System i

Sieciowy protokół FTP

Wersja 6 wydanie 1

System i

Sieciowy protokół FTP

Wersja 6 wydanie 1

Uwaga

Przed skorzystaniem z tych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje zawarte w sekcji “Uwagi”, na stronie 161.

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

Protokół FTP

Platformę IBM System i można skonfigurować tak, aby możliwe było wysyłanie, odbieranie i współużytkowanie plików w sieciach za pomocą protokołu FTP, który umożliwia także zmianę nazwy oraz dodawanie i usuwanie plików w sieci. Aby skonfigurować system do przesyłania plików, należy najpierw skonfigurować i uruchomić w systemie protokół TCP/IP.

Uwaga: Korzystając z przykładowego kodu, użytkownik akceptuje warunki opisane w sekcji Informacje dotyczące kodu.

Plik PDF z informacjami na temat protokołu FTP

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 FTP (około 1636 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 zainstalowany na komputerze. Bezpłatną kopię programu można pobrać z serwisu WWW firmy Adobe

(www.adobe.com/products/acrobat/readstep.html) .

Scenariusze: protokół FTP

Scenariusze protokołu FTP przedstawiają sposób konfigurowania protokołu FTP i korzystania z niego w środowisku i5/OS. Scenariusze te ułatwiają zrozumienie zasad działania protokołu FTP i sposobu wykorzystania środowiska FTP we własnej sieci.

Scenariusze te przedstawiają podstawowe koncepcje dotyczące FTP, z których po przystąpieniu do zadań planowania i konfigurowania mogą czerpać korzyści zarówno użytkownicy początkujący, jak i doświadczeni.

Scenariusz: przesyłanie pliku ze zdalnego hosta

Ten scenariusz opisuje, jak za pomocą podstawowych funkcji protokołu FTP pobrać pliki ze zdalnego hosta. W tym scenariuszu klient i serwer są systemami używającymi protokołu FTP i5/OS.

Sytuacja

Załóżmy, że współpracownik użytkownika utworzył pliki Java i umieścił je w systemie zdalnym. Użytkownik jako inżynier testujący system musi przesłać plik przykład.jar z systemu zdalnego do testowego systemu lokalnego.

Cele

Użyj protokołu FTP, aby wysłać plik przez sieć TCP/IP.

Informacje szczegółowe

Do przesłania pliku wykorzystywane są dwa połączenia: połączenie sterujące i połączenie dla danych. Połączenie sterujące używane jest do wysyłania podkomend od klienta do serwera i otrzymywania odpowiedzi na te komendy. Klient wysyła komendy FTP do serwera FTP. Połączenie dla danych wykorzystywane jest do przesyłania plików. Zarówno klient, jak i interfejs serwera łączy się z systemem plików i5/OS.

Aby przesłać pliki, potrzebny jest w obu systemach identyfikator użytkownika. Wymagania systemowe są następujące:

- system operacyjny i5/OS,
- program narzędziowy IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1),
- skonfigurowany serwer FTP.

Aby przesyłać pliki, wymagane są również następujące informacje:

- nazwa hosta zdalnego systemu,
- nazwa i hasło użytkownika w zdalnym systemie,
- nazwa pliku do przesłania,
- lokalizacja pliku,
- format pliku (format, w jakim plik ma zostać przesłany, np. binarny lub ASCII).

Zadania konfiguracyjne

Aby zrealizować proste przesyłanie pliku, wykonaj następujące czynności:

Uwaga: Można również przesyłać pliki automatycznie za pomocą zadania wsadowego FTP.

1. Uruchom sesję klienta FTP. W tym scenariuszu w interfejsie znakowym wpisz komendę STRTCPFTP i naciśnij klawisz Enter.
2. Podaj nazwę zdalnego systemu, do którego chcesz wysłać plik.

   W tym scenariuszu: theirco.com.
3. Podaj swoją nazwę użytkownika w systemie zdalnym.

   ```
   Wpisz identyfikator logowania (twój_identyfikator):
   ===>twój_identyfikator
   ```
4. Podaj swoje hasło w systemie zdalnym.

   ```
   Wpisz hasło:
   ===>twoje_hasło
   ```
5. Odszukaj w systemie IchFirmy katalog, z którego chcesz przesłać plik. Dotyczy niniejszego scenariusza: ===>cd /qibm/userdata/os400/dirserv/usrtools/windows
6. Przejdź do katalogu w systemie lokalnym, do którego chcesz przesłać plik. Dotyczy niniejszego scenariusza: ===>lcd /qibm/userdata/os400/dirserv/usrtools/windows
7. Określ typu pliku ASCII lub BINARY. Domyślnym typem jest ASCII. Dla pliku .jar trzeba zmienić typ przesyłanego pliku na binarny.

   W tym scenariuszu: ===> BINARY
8. Zażądaj przesłania pliku ze zdalnego serwera do systemu klienta.

   Dotyczy niniejszego scenariusza: ===> get example.jar
9. Po zakończeniu zamknij program FTP.

   Dotyczy niniejszego scenariusza: ===> QUIT

   Zadania pokrewne

   “Przesyłanie plików za pomocą protokołu FTP” na stronie 31
   Protokół FTP umożliwia wysyłanie i odbieranie plików.

   Odsyłacze pokrewne

“Korzystanie z protokołu FTP w trybie nienadzorowanym za pomocą zadania wsadowego” na stronie 33
Klient FTP może być uruchamiany interaktywnie lub w trybie nienadzorowanym. Ten temat zawiera jeden prosty i jeden zaawansowany przykład użycia metody zadania wsadowego protokołu FTP.

“Uruchamianie i zatrzymywanie sesji klienta” na stronie 28
Po uzyskaniu identyfikatora logowania i hasła do zdalnego serwera FTP można uruchomić sesję klienta z tym serwerem FTP. Sesję klienta można zakończyć przy użyciu podkomendy QUIT serwera FTP.

“ASCII (Zmiana typu pliku na ASCII - Change File Type to ASCII)” na stronie 63
Podkomenda ASCII klienta FTP i5/OS służy doustawiania typu przesyłania plików na format ASCII.

“BINARY (Ustawienie typu przesyłania dla obrazu - Set Transfer Type to Image)” na stronie 64
Podkomenda BINARY klienta FTP i5/OS służy do ustawiania typu przesyłania plików na format BINARY.

Scenariusz: zabezpieczanie protokołu FTP za pomocą protokołu SSL

W tym scenariuszu pokazano, jak przesyłać dane do przedsiębiorstwa partnerskiego przy użyciu protokołu SSL. Korzystając z protokołu SSL, aplikacje klienta i serwera FTP na platformach System i mogą komunikować się ze sobą w sposób umożliwiający zablokowanie podsłuchiwania komunikatów, manipulowania przy nich i ich fałszowania.

Sytuacja

Pracownicy MojejFirmy wyszukują powstające przedsiębiorstwa i sprzedają wyniki poszukiwań firmom planującym inwestycje. Jedno z przedsiębiorstw planujących inwestycje, IchFirma, potrzebuje usług MojejFirmy i chciałoby otrzymywać raporty poszukiwań za pomocą protokołu FTP. MojaFirma zawsze dba o prywatność i bezpieczeństwo danych rozprowadzanych do jej klientów bez względu na ich format. W tym przypadku MojaFirma musi nawiązać z IchFirmą sesje FTP chronione za pomocą SSL.

Cele

W ramach niniejszego scenariusza określone zostały następujące cele:

- Utworzenie i prowadzenie lokalnego ośrodka certyfikacji w systemie MojejFirmy.
- Włączenie protokołu SSL na serwerze FTP MojejFirmy.
- Eksportowanie kopii certyfikatu lokalnego ośrodka certyfikacji (CA) MojejFirmy do pliku.
- Utworzenie bazy certyfikatów *SYSTEM w systemie IchFirmy.
- Importowanie certyfikatu lokalnego ośrodka CA MojejFirmy do bazy certyfikatów *SYSTEM IchFirmy.
- Określenie lokalnego ośrodka CA MojejFirmy jako zaufanego ośrodka CA dla klienta FTP IchFirmy.

Wymagania wstępne

MojaFirma

- Platforma System i ma uruchomiony system operacyjny i5/OS.
- W systemie jest zainstalowany program narzędziowyIBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1).
- W systemie jest zainstalowany program IBM Digital Certificate Manager (DCM) (5761-SS1 opcja 34).
- W systemie jest zainstalowany serwer IBM HTTP (5761-DG1).
- Dostęp do aplikacji i zasobów publicznych w systemie jest zabezpieczony za pomocą certyfikatów.

IchFirma

- Platforma System i ma uruchomiony system operacyjny i5/OS.
- W systemie jest zainstalowany program narzędziowy TCP/IP Connectivity Utilities for i5/OS (5761-TC1).
- W systemie jest zainstalowany program IBM Digital Certificate Manager (5761-SS1 opcja 34).
- W systemie jest zainstalowany serwer IBM HTTP (5761-DG1).
- Do obsługi sesji FTP w systemie jest wykorzystywany system operacyjny i5/OS z klientem FTP TCP/IP.

Informacje szczegółowe

IchFirma korzysta z systemu operacyjnego i5/OS z klientem FTP, aby żądać bezpiecznego przesyłania plików z serwera FTP MojejFirmy. Serwer jest uwierzytelniony. IchFirma otrzymuje raporty finansowe z MojejFirmy poprzez sesję FTP chronioną za pomocą warstwy SSL.

Pojęcia pokrewne

"Zabezpieczanie klientów FTP za pomocą protokołu TLS lub SSL" na stronie 22
Dane przesyłane za pomocą połączeń sterujących i połączeń danych protokołu FTP można szyfrować, korzystając z połączeń TLS lub SSL.

Zadania pokrewne

Zarządzanie publicznymi certyfikatami internetowymi dla sesji komunikacyjnych SSL

Uruchamianie programu Digital Certificate Manager

Informacje pokrewne

Scenariusz: używanie certyfikatów do uwierzytelniania zewnętrznego

Szczegóły konfiguracji

Aby zabezpieczyć protokół FTP za pomocą protokołu SSL, należy skonfigurować systemy korzystające z protokołu FTP, w tym współpracę z ośrodkiem certyfikacji, aktywowanie protokołu SSL itp.

W tym scenariuszu MojaFirma i IchFirma wykonują szereg czynności w celu zabezpieczenia sesji FTP za pomocą protokołu SSL.

Tworzenie i prowadzenie lokalnego ośrodka certyfikacji w systemie MojaFirma:

Scenariusz zakłada, że MojaFirma nie używała wcześniej programu Digital Certificate Manager do konfigurowania certyfikatów w swoim systemie. Zgodnie z celami tego scenariusza MojaFirma zdecydowała się na utworzenie i prowadzenie lokalnego ośrodka certyfikacji (CA) w celu wystawienia certyfikatu serwerowi FTP.

Uwaga: Zamiast tworzyć i prowadzić lokalny ośrodek CA, MojaFirma mogłaby również korzystać z certyfikatu publicznego dla protokołu SSL, konfigurując serwer FTP przy użyciu programu DCM.

Program DCM tak kieruje procesem tworzenia lokalnego ośrodka CA, aby zostały skonfigurowane wszystkie elementy niezbędne do aktywowania protokołu SSL.

Aby utworzyć i prowadzić w systemie MojaFirma lokalny ośrodek CA przy użyciu programu DCM, wykonaj następujące czynności:

1. Uruchom program IBM DCM. Jeśli jest konieczne uzyskanie lub utworzenie certyfikatów albo skonfigurowanie lub zmiana systemu certyfikatów, należy zrobić to w tym momencie.
2. W ramce nawigacji programu DCM wybierz **Tworzenie ośrodka certyfikacji**, aby wyświetlić szereg formularzy. Formularze te prowadzą przez proces tworzenia lokalnego ośrodka CA i wykonywania innych czynności niezbędnych do rozpoczęcia korzystania z certyfikatów cyfrowych dla protokołu SSL, podpisywania obiektów i weryfikowania podpisów.
3. Uzupełnij wszystkie wyświetlane formularze. Dla każdego zadania, które musi być wykonane w celu utworzenia i prowadzenia lokalnego ośrodka CA w systemie, istnieje oddzielny formularz.
   a. Wybierz, w jaki sposób ma być przechowywany klucz prywatny certyfikatu lokalnego CA. Ta czynność wymagana jest tylko wtedy, jeśli w systemie zainstalowany jest koprocesor szyfrujący IBM 4758-023 PCI. Jeśli w systemie nie ma takiego koprocesora, program DCM automatycznie składuje certyfikat i jego klucz prywatny w bazie certyfikatów lokalnego ośrodka certyfikacji.
   b. Wprowadź informacje identyfikujące lokalny ośrodek CA.
   c. Zainstaluj lokalny certyfikat CA na komputerze PC lub w przeglądarce. Dzięki temu oprogramowanie będzie mogło rozpoznać lokalny ośrodek certyfikacji (CA) oraz wydawane przez niego certyfikaty.
   d. Wybierz dane strategii dla lokalnego ośrodka CA.

e. Użyj nowego lokalnego ośrodka CA do wystawienia certyfikatu klienta lub serwera, z którego aplikacja będzie mogła skorzystać do nawiązywania połączeń z użyciem protokołu SSL. Jeśli w systemie zainstalowano koprocesor szyfrujący IBM 4758-023 PCI, można wybrać metodę przechowywania klucza prywatnego dla certyfikatu serwera lub klienta. Jeśli w systemie nie ma tego koprocesora, program DCM automatycznie umieszcza certyfikat i jego klucz prywatny w bazie certyfikatów *SYSTEM. Program DCM tworzy bazę certyfikatów *SYSTEM jako część tego zadania.

f. Wybierz aplikacje, które będą mogły używać certyfikatu serwera lub klienta w połączeniach SSL.

   Uwaga: Należy wybrać ID aplikacji serwera TCP/IP FTP i5/OS (QIBM_QTMF_FTP_SERVER).

g. Użyj nowego lokalnego ośrodka CA do wystawienia certyfikatu podpisującego obiekt, z którego aplikacje będą mogły korzystać do cyfrowego podpisywania obiektów. Zadanie to tworzy bazę certyfikatów *OBJECTSIGNING, której można używać do zarządzania certyfikatami do podpisywania obiektów.

   Uwaga: Mimo że w tym scenariuszu nie są używane certyfikaty do podpisywania obiektów, ten krok należy wykonać. Anulowanie zadania w tym momencie spowoduje konieczność wykonania odrębnych zadań, które umożliwią zakończenie konfigurowania certyfikatu dla protokołu SSL.

h. Wybierz aplikacje ufające lokalnemu ośrodkowi CA.

   Uwaga: Należy wybrać ID aplikacji serwera TCP/IP FTP i5/OS (QIBM_QTMF_FTP_SERVER).

Aktywowanie protokołu SSL na serwerze FTP MojejFirmy:

Teraz, gdy do serwera FTP jest przypisany certyfikat, należy skonfigurować serwer FTP MojejFirmy w celu korzystania z protokołu SSL.

Aby skonfigurować serwer FTP przy użyciu programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Kliknij prawym przyciskiem **FTP**.
3. Wybierz opcję **Właściwości** (Properties).
4. Wybierz zakładkę **Ogólne** (General).
5. Aby włączyć obsługę warstwy SSL, wybierz następującą opcję: **Tylko połączenia chronione**. Wybierz tę opcję, aby zezwolić na nawiązywanie z serwerem FTP jedynie sesji SSL. Połączenia mogą być nawiązywane z niechronionym portem FTP, ale klient FTP musi wynegocjować sesję SSL, zanim użytkownik będzie mógł się zalogować.

Po zakończeniu tego zadania serwer FTP może używać warstwy SSL do szyfrowania sesji komunikacyjnych i chronienia prywatności danych przesyłanych podczas tych sesji. Jednak aby skonfigurować klienta FTP do uczestnictwa w sesji SSL z serwerem FTP, MojaFirma musi udostępnić klientowi IchFirmy kopię certyfikatu lokalnego CA. W tym celu MojaFirma musi wyeksportować kopię certyfikatu lokalnego CA do pliku i udostępnić go IchFirmie. Kiedy IchFirma otrzyma już ten plik, może skorzystać z programu DCM, aby zaimportować certyfikat lokalnego ośrodka CA do bazy certyfikatów *SYSTEM i skonfigurować klienta FTP i5/OS tak, aby korzystał z protokołu SSL.

Eksportowanie kopii certyfikatu lokalnego ośrodka certyfikacji MojejFirmy do pliku:

Aby aktywować bezpieczne połączenie FTP pomiędzy dwoma systemami, MojaFirma musi udostępnić IchFirmie kopię certyfikatu lokalnego ośrodka certyfikacji. Aplikacja klienta IchFirmy musi ufać certyfikatowi ośrodka CA, aby mogła uczestniczyć w sesji SSL.

Wykonaj poniższe czynności, aby wyeksportować kopię certyfikatu lokalnego ośrodka CA do pliku:

1. Uruchom program IBM Digital Certificate Manager (DCM). Jeśli jest konieczne uzyskanie lub utworzenie certyfikatów albo skonfigurowanie lub zmiana systemu certyfikatów, należy zrobić to w tym momencie.
2. Kliknij **Wybór ośrodka certyfikacji**.

3. Wybierz ***SYSTEM**, aby otworzyć bazę certyfikatów, i kliknij przycisk **Kontynuuj**.
4. Kiedy pojawi się ekran Baza certyfikatów i hasło, wpisz hasło, które zostało podane dla bazy certyfikatów podczas jej tworzenia, a następnie kliknij przycisk **Kontynuuj**.
5. Kiedy ramka nawigacji zostanie odświeżona, wybierz **Zarządzanie certyfikatami**, a następnie zadanie **Eksportuj certyfikat**.
6. Wybierz **Ośrodek certyfikacji (CA)** i kliknij przycisk **Kontynuuj**, aby wyświetlić listę certyfikatów ośrodka certyfikacji.
7. Wybierz z listy certyfikat lokalnego ośrodka CA MojejFirmy i kliknij przycisk **Eksportuj**.
8. Jak miejsce docelowe eksportu podaj **Plik** i kliknij przycisk **Kontynuuj**.
9. Podaj pełną ścieżkę i nazwę dla pliku eksportowanego certyfikatu lokalnego CA i kliknij **Kontynuuj**, aby wyeksportować certyfikat.
10. Kliknij **OK**, aby opuścić stronę potwierdzenia eksportu.

Od tego momentu można przesyłać te pliki do systemów końcowych, na których mają być weryfikowane podpisy utworzone za pomocą certyfikatu. Do przesłania tych plików można użyć poczty elektronicznej lub protokołu FTP, ponieważ nie muszą one być przesyłane bezpiecznie.

Tworzenie bazy certyfikatów *SYSTEM w systemie IchFirmy:

Aby uczestniczyć w sesji SSL, klient FTP systemu IchFirmy musi być w stanie rozpoznawać i akceptować certyfikat przedstawiany przez serwer FTP MojejFirmy. Aby uwierzytelnić certyfikat, klient FTP IchFirmy musi mieć kopię certyfikatu ośrodka certyfikacji w bazie certyfikatów *SYSTEM.

W tym scenariuszu założono, że do tworzenia i zarządzania certyfikatami nie był wcześniej wykorzystywany program DCM. W takiej sytuacji w IchFirmie należy utworzyć bazę certyfikatów *SYSTEM. W tym celu wykonaj następujące czynności:

1. Uruchom program IBM DCM. Jeśli jest konieczne uzyskanie lub utworzenie certyfikatów albo skonfigurowanie lub zmiana systemu certyfikatów, należy zrobić to w tym momencie.
2. W ramce nawigacji programu DCM wybierz opcję **Tworzenie nowej bazy certyfikatów** (Create New Certificate Store), a następnie wybierz ***SYSTEM** jako bazę certyfikatów, która ma być utworzona, i kliknij przycisk **Kontynuuj**.
3. Wybierz **Nie**, aby utworzyć certyfikat podczas tworzenia bazy certyfikatów *SYSTEM, i kliknij przycisk **Kontynuuj**.
4. Podaj hasło dla nowej bazy certyfikatów i kliknij przycisk **Kontynuuj**, aby wyświetlić stronę z potwierdzeniem.
5. Kliknij przycisk **OK**.

Importowanie certyfikatu lokalnego ośrodka certyfikacji MojejFirmy do bazy certyfikatów *SYSTEM IchFirmy:

Baza certyfikatów *SYSTEM IchFirmy zawiera kopie certyfikatów większości publicznych ośrodków certyfikacji. Ponieważ serwer FTP MojejFirmy korzysta jednak z certyfikatu lokalnego ośrodka CA, klient FTP IchFirmy musi otrzymać kopię tego certyfikatu i zaimportować go do bazy certyfikatów *SYSTEM.

Aby zaimportować certyfikat lokalnego ośrodka certyfikacji do bazy certyfikatów *SYSTEM i określić, że ośrodek ten jest zaufanym źródłem certyfikatów, w systemie IchFirmy wykonaj następujące czynności:

1. W ramce nawigacji programu DCM kliknij **Wybór ośrodka certyfikacji** i wybierz ***SYSTEM**, aby otworzyć tę bazę certyfikatów.
2. Kiedy pojawi się ekran Baza certyfikatów i hasło, wpisz hasło, które zostało podane dla bazy certyfikatów podczas jej tworzenia, a następnie kliknij przycisk **Kontynuuj**.
3. Po odświeżeniu widoku ramki nawigacji wybierz opcję **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
4. Z listy zadań wybierz **Import certyfikatu**.
5. Jako typ certyfikatu wybierz **Ośrodek certyfikacji** i kliknij **Kontynuuj**.

6. Podaj pełną ścieżkę i nazwę dla pliku certyfikatu ośrodka CA i kliknij **Kontynuuj**. Pojawi się komunikat potwierdzający pomyślne zakończenie importu lub informacja o błędzie, jeśli proces nie powiódł się.

Określanie lokalnego ośrodka CA MojejFirmy jako zaufanego ośrodka CA dla klienta FTP IchFirmy:

Zanim IchFirma będzie mogła korzystać z klienta FTP do nawiązywania bezpiecznych połączeń z serwerem FTP MojejFirmy, musi za pomocą programu Digital Certificate Manager (DCM) określić, którym ośrodkom certyfikacji klient powinien ufać. Oznacza to, że IchFirma musi określić, że zaimportowany wcześniej certyfikat lokalnego ośrodka CA jest godny zaufania.

W systemie IchFirmy wykonaj poniższe czynności, aby określić, że klient FTP IchFirmy powinien ufać certyfikatowi lokalnego CA MojejFirmy:

1. Uruchom program DCM.
2. Kliknij **Wybór ośrodka certyfikacji** i wybierz *SYSTEM, aby otworzyć tę bazę certyfikatów.
3. Kiedy pojawi się ekran Baza certyfikatów i hasło, wpisz hasło, które zostało podane dla bazy certyfikatów podczas jej tworzenia, a następnie kliknij przycisk **Kontynuuj**.
4. W ramce nawigacji wybierz **Zarządzanie aplikacjami**, aby wyświetlić listę zadań.
5. Z listy zadań wybierz **Definiowanie listy zaufanych ośrodków certyfikacji (CA)**.
6. Jako typ aplikacji, dla której chcesz zdefiniować listę, wybierz **Klient** i kliknij przycisk **Kontynuuj**.
7. Wybierz z listy aplikację klienta FTP TCP/IP systemu i5/OS (QIBM_QTMF_FTP_CLIENT) i kliknij przycisk **Kontynuuj**, aby wyświetlić listę certyfikatów ośrodków CA.
8. Wybierz certyfikat lokalnego ośrodka CA MojejFirmy, który był wcześniej zaimportowany, i kliknij przycisk **OK**. Program DCM wyświetli komunikat potwierdzający wybór listy zaufanych certyfikatów.

Po zakończeniu tych działań serwer FTP MojejFirmy może ustanowić sesję SSL z klientem lub serwerem FTP IchFirmy.

Pojęcia pokrewne

"Zabezpieczanie klientów FTP za pomocą protokołu TLS lub SSL" na stronie 22
Dane przesyłane za pomocą połączeń sterujących i połączeń danych protokołu FTP można szyfrować, korzystając z połączeń TLS lub SSL.

Konfigurowanie serwera FTP

Serwer FTP można skonfigurować tak, aby współpracował z klientami FTP z interfejsem graficznym, przeglądarkami WWW oraz narzędziami WWW.

Licencjonowany program narzędziowy TCP/IP Connectivity Utilities dostarczany jest razem ze skonfigurowanymi serwerami FTP TCP/IP. Kiedy uruchamiany jest protokół TCP/IP, uruchamia się jednocześnie serwer FTP. Przed skonfigurowaniem połączenia serwera FTP z siecią Internet należy zabezpieczyć dane. W tym celu należy:

- używać zapory firewall między systemem a siecią Internet,
- używać systemu innego niż produkcyjny jako serwera FTP,
- nie przyłączać serwera FTP do pozostałych sieci lokalnych (LAN) lub rozległych (WAN) należących do firmy,
- wykorzystać programy obsługi wyjścia FTP, aby zabezpieczyć dostęp do serwera FTP,
- raz w miesiącu przetestować programy obsługi wyjścia FTP, aby upewnić się, że nie zawierają one żadnych luk w systemie ochrony,
- nie nadawać anonimowym użytkownikom FTP praw odczytu i zapisu do tego samego katalogu; pozbawia to anonimowych użytkowników możliwości stania się nieuchwytnym w sieci Internet,
- protokołować wszystkie operacje dostępu do serwera FTP i codziennie lub co tydzień przeglądać protokoły w poszukiwaniu ewentualnych prób włamania,
- raz na miesiąc sprawdzać, czy dla serwera FTP są zarejestrowane prawidłowe programy obsługi wyjścia,

- zapoznać się z tematem Zabezpieczenie serwera FTP w celu uzyskania informacji na temat zabezpieczania serwera FTP.

Odsyłacze pokrewne

"Zabezpieczanie protokołu FTP" na stronie 16
Dane przesyłane przez protokół FTP można zabezpieczyć za pomocą protokołu SSL, jak również monitorując użytkowników protokołu FTP i zarządzając dostępem użytkowników do funkcji protokołu FTP.

Konfigurowanie serwera FTP za pomocą programu System i Navigator

System i Navigator udostępnia graficzny interfejs użytkownika (GUI), za pomocą którego można skonfigurować serwer FTP i5/OS i zarządzać nim.

Aby uzyskać dostęp do interfejsu GUI serwera FTP w programie System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **TCP/IP** (*system* > Network > Servers > TCP/IP).
2. W prawym panelu kliknij prawym przyciskiem myszy **FTP** i wybierz **Właściwości**.
3. W tym miejscu można zmieniać właściwości serwera FTP. Pomoc elektroniczną można przejrzeć, klikając przycisk pomocy. Aby wyświetlić pomoc dla określonego pola, należy kliknąć przycisk ze znakiem zapytania, a następnie żądane pole.

Zadania pokrewne

"Uruchamianie i zatrzymywanie serwera FTP" na stronie 26
Serwer FTP można uruchamiać i zatrzymywać za pomocą programu System i Navigator.

Konfigurowanie serwerów FTP w celu współpracy z klientami FTP z interfejsem graficznym oraz narzędziami WWW

Serwery FTP w systemie operacyjnym i5/OS obsługują klienty FTP z interfejsem graficznym, przeglądarki WWW oraz narzędzia WWW. Ponieważ większość klientów FTP z interfejsem graficznym używa formatu listingu przypominającego system UNIX oraz pliku ścieżek jako formatu nazw plików, serwer FTP musi być tak skonfigurowany, aby obsługiwał te formaty.

Aby korzystać z obsługiwanych formatów, wykonaj następujące instrukcje w celu ustawienia właściwości serwera FTP:

1. W programie System i Navigator rozwiń ***system*** → **Sieć** → **Serwery** → **TCP/IP** (*system* > Network > Servers > TCP/IP).
2. W prawym panelu kliknij prawym przyciskiem myszy **FTP** i wybierz **Właściwości**.
3. Na stronie **Właściwości** kliknij zakładkę **Formaty**.
   - Dla Formatu nazw zbiorów wybierz opcję **Ścieżki**.
   - Dla Formatu listingu plików wybierz **Format listingu obiektów UNIX**.

   Uwaga: W poszczególnych sesjach FTP można sterować ustawieniami LISTFMT i NAMEFMT za pomocą programu obsługi wyjścia dla formatu TCPL0200 lub TCPL0300 punktu wyjścia logowania do serwera FTP.

Można także zmienić format listingu *po* uruchomieniu sesji FTP za pomocą opcji podkomendy SITE (Wysłanie informacji używanych przez serwer - Send Information Used by a Server System) serwera FTP. Te ustawienia sterują wynikami zwracanymi przez komendy LIST (Lista zbiorów - File List) i NLST (Lista nazw - Name List) serwera FTP.

Odsyłacze pokrewne

"Format TCPL0200 punktu wyjścia" na stronie 125
Punktem wyjścia logowania do serwera FTP jest QIBM_QTMF_SVR_LOGON. Jednym z interfejsów sterujących formatem parametrów dla tych punktów wyjścia jest TCPL0200. W tym temacie opisano parametry formatu punktu wyjścia TCPL0200.

"Format TCPL0300 punktu wyjścia" na stronie 129
Punktem wyjścia logowania do serwera FTP jest QIBM_QTMF_SVR_LOGON. Punktem wyjścia logowania do serwera REXEC jest QIBM_QTMX_SVR_LOGON. Jednym z interfejsów sterujących formatem parametrów dla tych punktów wyjścia jest TCPL0300. W tym temacie opisano parametry formatu punktu wyjścia TCPL0300.

"SITE (Wysłanie informacji używanych przez serwer - Send Information Used by a Server System)" na stronie 55
Podkomenda SITE serwera FTP i5/OS służy do wysyłania informacji lub udostępniania usług wykorzystywanych przez serwer FTP.

"LIST (Lista zbiorów - File List)" na stronie 48
Podkomenda LIST serwera FTP i5/OS służy do wyświetlania listy pozycji katalogu, zawartości biblioteki lub zbiorów w grupie zbiorów.

"NLST (Lista nazw - Name List)" na stronie 50
Podkomenda NLST serwera FTP i5/OS służy do wyświetlania nazw wielu zbiorów, grupy zbiorów, katalogu lub biblioteki.

Pozycje pliku i katalogu w formacie i5/OS

Klienty platformy System i umożliwiają listing plików na serwerze FTP zarówno w formacie systemu i5/OS, jak i w formacie właściwym dla systemu UNIX. W tym temacie omówiono format systemu i5/OS.

Oryginalny format stylu systemu i5/OS dla podkomendy LIST jest następujący (gdy LISTFMT=0):

```
właściciel wielkość data godzina typ nazwa
```

Pola rozdzielone są znakiem odstępu.

Opis poszczególnych pól:

owner (właściciel)
Łańcuch 10 znaków reprezentujący profil użytkownika będącego właścicielem obiektu. Łańcuch ten jest wyrównywany w lewo i zawiera znaki puste. Dla sesji anonimowej FTP pole to pozostaje puste.

size (wielkość)
10-znakowy numer reprezentujący wielkość obiektu. Numer ten jest wyrównywany w prawo i zawiera znaki puste. Pole to jest puste, jeśli obiekt nie ma przypisanej wielkości.

date (data)
8-znakowa data modyfikacji w formacie zdefiniowanym dla danego zadania serwera. W typ polu wykorzystywane są separatory daty zdefiniowane dla danego zadania serwera. Data modyfikacji jest wyrównywana w lewo i zawiera znaki puste.

time (godzina)
8-znakowa godzina modyfikacji wykorzystująca separator godziny zdefiniowany przez zadanie serwera.

type (typ)
10-znakowy typ obiektu i5/OS.

name (nazwa)
Nazwa obiektu, o zmiennej długości, występująca po znaku CRLF (powrót karetki, nowy wiersz). Nazwa może zawierać znaki puste.

Przykładowa pozycja pliku w oryginalnym formacie stylu systemu i5/OS:

```
BAILEYSE     5263360 06/11/97 12:27:39 *FILE     BPTFSAVF
```

Odsyłacze pokrewne

"Pozycje pliku i katalogu w formacie systemu UNIX" na stronie 10
Klienty platformy System i umożliwiają listing plików i katalogów na serwerze FTP zarówno w formacie systemu i5/OS, jak i w formacie systemu UNIX. W tym temacie omówiono format systemu UNIX.

"SITE (Wysłanie informacji używanych przez serwer - Send Information Used by a Server System)" na stronie 55
Podkomenda SITE serwera FTP i5/OS służy do wysyłania informacji lub udostępniania usług wykorzystywanych przez serwer FTP.

“LIST (Lista zbiorów - File List)” na stronie 48
Podkomenda LIST serwera FTP i5/OS służy do wyświetlania listy pozycji katalogu, zawartości biblioteki lub zbiorów w grupie zbiorów.

“NLST (Lista nazw - Name List)” na stronie 50
Podkomenda NLST serwera FTP i5/OS służy do wyświetlania nazw wielu zbiorów, grupy zbiorów, katalogu lub biblioteki.

Pozycje pliku i katalogu w formacie systemu UNIX

Klienty platformy System i umożliwiają listing plików i katalogów na serwerze FTP zarówno w formacie systemu i5/OS, jak i w formacie systemu UNIX. W tym temacie omówiono format systemu UNIX.

Format systemu UNIX podkomendy LIST jest następujący (gdy LISTFMT=1):

```
tryb dowiązania właściciel grupa wielkość data godzina nazwa
```

Pola rozdzielone są znakiem odstępu.

Poszczególne pola formatu systemu UNIX są opisane poniżej.

mode (tryb)
Pole to może zawierać do 10 znaków. Każdy znak ma konkretne znaczenie.

Pierwszy znak	Znaczenie
d	Obiekt jest katalogiem.
b	Obiekt jest blokiem pliku specjalnego.
c	Obiekt jest znakiem pliku specjalnego.
l	Obiekt jest dowiązaniem symbolicznym. została ustawiona flaga -N lub dowiązanie symboliczne nie wskazuje na istniejący plik
p	Obiekt jest plikiem specjalnym typu FIFO.
s	Obiekt jest gniazdem lokalnym.
-	Obiekt jest zwykłym plikiem.

Następne 9 znaków jest podzielone na trzy zestawy po 3 znaki każdy. Te trzy znaki w każdym zestawie oznaczają odpowiednio uprawnienia do odczytu, zapisu i wykonywania pliku. Uprawnienia do wykonywania w odniesieniu do katalogu oznaczają prawo do przeszukiwania danego katalogu. Uprawnienia te mają następujące znaczenie: pierwszy zestaw znaków pokazuje uprawnienia właściciela obiektu. Drugi zestaw znaków pokazuje uprawnienia grupy. Ostatni zestaw znaków pokazuje uprawnienia pozostałych użytkowników do tego pliku.

Pierwszy znak	Funkcja
r	read (odczyt)
w	write (edit) (zapis - edycja)
x	execute (search) (wykonanie - przeszukiwanie)
-	brak uprawnienia

odsyłacze
Liczba dowiązań do obiektu. Minimalna liczba znaków wynosi 3. Maksymalna liczba znaków wynosi 5. Pole jest wyrównywane w prawo i zawiera znaki puste.

owner (właściciel)
Właściciel obiektu. Minimalna liczba znaków wynosi 8. Maksymalna liczba znaków wynosi 10. Pole jest wyrównywane w lewo i zawiera znaki puste. Pole to zawiera nazwę profilu właściciela obiektu. Dla sesji anonimowych FTP pole to zawiera numer identyfikacyjny właściciela.

group (grupa)

Właściciel obiektu. Minimalna liczba znaków wynosi 8. Maksymalna liczba znaków wynosi 10. Pole jest wyrównywane w lewo i zawiera znaki puste. Pole to zawiera nazwę profilu grupy. Jeśli nie ma grupy, pole zawiera numer identyfikacyjny grupy. Dla sesji anonimowych w tym polu znajduje się numer identyfikacyjny grupy.

size (wielkość)

Wielkość obiektu. Minimalna liczba znaków wynosi 7. Maksymalna liczba znaków wynosi 10. Pole jest wyrównane w prawo i zawiera znaki puste. Jeśli obiekt nie ma żadnej wielkości, podana zostaje domyślna wartość 0.

datetime (data/godzina)

12-znakowa data/godzina modyfikacji. Pole jest wyrównywane w lewo i zawiera znaki puste. Jeśli modyfikacja nastąpiła podczas ostatnich 180 dni, to format pola jest następujący:

```
Mmm dd gg:mm
```

Jeśli modyfikacja wystąpiła wcześniej, to format pola jest następujący:

```
Mmm dd rrrr
```

Opis poszczególnych pól:

Znaki	Znaczenie
Mmm	Skrócony miesiąc.
dd	Dwa znaki dnia miesiąca. Pole jest wyrównywane w prawo i dopełniane znakami pustymi.
gg	Dwie cyfry godziny (00-23). Pole jest wyrównywane w prawo i dopełniane zerami.
mm	Dwie cyfry minuty (00-59). Pole jest wyrównywane w prawo i dopełniane zerami.
rrrr	Cztery cyfry roku.

name (nazwa)

Nazwa obiektu o zmiennej długości, po której występują znaki CR/LF (powrót karetki, nowy wiersz). Nazwa może zawierać znaki puste.

Poniżej przedstawiony jest przykład formatu stylu dla systemu UNIX:

```
drwxrwxrwx   4 QSYS           0    51200 Feb  9 21:28 home
```

Poniższa informacja jest ważna, jeśli podkomenda LIST zwraca dane w formacie systemu UNIX : jeśli LISTFMT=1, dane zwracane przez komendę LIST są inne dla zbiorów QSYS.LIB w zależności od ustawienia NAMEFMT:

- Jeśli NAMEFMT=1, wyświetlone zostaną tylko nazwy zbiorów QSYS.LIB.
- Jeśli NAMEFMT=0, wyświetlone zostaną zarówno nazwy zbiorów QSYS.LIB, jak i nazwy ich podzbiorów.

Odsyłacze pokrewne

“Pozycje pliku i katalogu w formacie i5/OS” na stronie 9
Klienty platformy System i umożliwiają listing plików na serwerze FTP zarówno w formacie systemu i5/OS, jak i w formacie właściwym dla systemu UNIX. W tym temacie omówiono format systemu i5/OS.

“SITE (Wysłanie informacji używanych przez serwer - Send Information Used by a Server System)” na stronie 55
Podkomenda SITE serwera FTP i5/OS służy do wysyłania informacji lub udostępniania usług wykorzystywanych przez serwer FTP.

“LIST (Lista zbiorów - File List)” na stronie 48
Podkomenda LIST serwera FTP i5/OS służy do wyświetlania listy pozycji katalogu, zawartości biblioteki lub zbiorów w grupie zbiorów.

“NLST (Lista nazw - Name List)” na stronie 50
Podkomenda NLST serwera FTP i5/OS służy do wyświetlania nazw wielu zbiorów, grupy zbiorów, katalogu lub biblioteki.

Konfigurowanie anonimowego serwera FTP

Anonimowy serwer FTP umożliwia zdalnym użytkownikom korzystanie z serwera FTP bez przypisanego ID użytkownika i hasła.

Anonimowy FTP umożliwia niezabezpieczony dostęp (bez hasła) do wybranych informacji w systemie zdalnym. System zdalny określa, które informacje mają być ogólnie dostępne. Takie informacje są dostępne publicznie i mogą być przeczytane przez kogokolwiek. Jedynie właściciel informacji i systemu jest odpowiedzialny za to, że udostępniane są wyłącznie odpowiednie informacje.

Aby uzyskać dostęp do tych informacji, użytkownik musi zalogować się do hosta z identyfikatorem użytkownika anonimowego. Użytkownik anonimowy ma ograniczone prawo dostępu do plików na serwerze FTP oraz ograniczony zakres czynności, które może wykonywać. Poniższe operacje są zwykle jedynymi dozwolonymi operacjami.

- zalogowanie się za pomocą FTP,
- wyświetlenie zawartości ograniczonego zbioru katalogów,
- pobranie plików z tych katalogów.

Najczęściej użytkownicy anonimowi nie mają uprawnień do przesyłania plików do serwera FTP. Niektóre systemy udostępniają użytkownikom anonimowym katalog wejściowy, do którego mogą wysyłać dane. Tradycyjnie specjalne konto użytkownika anonimowego akceptuje dowolny ciąg znaków jako hasło, ale powszechnie używa się hasła *guest* (gość) lub adresu e-mail tego użytkownika. Niektóre serwisy archiwalne pytają wprost o adres poczty elektronicznej użytkownika i nie pozwolą na zalogowanie się za pomocą hasła ″guest″ (gość). Podawanie adresu poczty elektronicznej jest uprzejmością wyświadczaną operatorom serwisów archiwalnych, która umożliwia im zorientowanie się, kto korzysta z ich serwisów.

Anonimowy serwer FTP w systemie operacyjnym i5/OS

Serwer FTP nie obsługuje anonimowego logowania do FTP. Aby skonfigurować anonimowy serwer FTP w systemie operacyjnym i5/OS, należy udostępnić programy obsługi wyjścia dla punktu wyjścia logowania do serwera FTP i punktu wyjścia potwierdzenia żądania protokołu FTP.

Anonimowy serwer FTP jest wygodną i często potrzebną usługą. Stosowanie anonimowego serwera FTP może jednak powodować problemy związane z bezpieczeństwem systemu.

Pojęcia pokrewne

“Zarządzanie dostępem za pomocą programów obsługi wyjścia FTP” na stronie 23
Dodatkowe bezpieczeństwo można zapewnić, dodając programy obsługi wyjścia FTP do punktów wyjścia serwera i klienta FTP, które oferują więcej możliwości ograniczenia dostępu do systemu.

“Kontrolowanie dostępu do serwera FTP” na stronie 17
Jeśli protokół FTP jest używany, istnieje potrzeba zachowania kontroli nad użytkownikami w celu ochrony danych i sieci. Sekcja ta zawiera wskazówki i uwagi dotyczące ochrony.

Odsyłacze pokrewne

“Punkt wyjścia logowania do serwera FTP” na stronie 106
Uwierzytelnianiem logowania do serwera aplikacji TCP/IP można sterować za pomocą punktu wyjścia logowania do serwera aplikacji TCP/IP. Ten punkt wyjścia umożliwia dostęp do serwera FTP na podstawie adresu systemu, który nawiązał sesję. Dzięki temu można określić początkowy katalog roboczy inny od tego, który znajduje się w profilu użytkownika.

Przygotowanie do konfigurowania anonimowego serwera FTP

Aby skonfigurować anonimowy serwer FTP, należy uwzględnić następujące kwestie związane z bezpieczeństwem.

Wymagane umiejętności

Aby skonfigurować anonimowy serwer FTP, wymagane są następujące umiejętności:

- znajomość interfejsu znakowego i komend systemu i5/OS z wieloma parametrami i słowami kluczowymi;

- umiejętność tworzenia bibliotek, podzbiorów i źródłowych zbiorów fizycznych w systemie (należy posiadać uprawnienie przynajmniej na poziomie *SECOF);
- umiejętność przypisywania uprawnień do bibliotek, zbiorów, podzbiorów i programów;
- umiejętność pisania, zmiany, kompilowania i testowania programów w systemie.

Kwestie związane z bezpieczeństwem

Pierwszym krokiem podczas implementacji anonimowego serwera FTP jest zdefiniowanie jego strategii. Ten plan definiuje ochronę serwera FTP i określa sposób kodowania programów obsługi wyjścia. Ponieważ serwer FTP będzie umożliwiał wszystkim użytkownikom uzyskanie dostępu do przechowywanych na nim danych, należy dokładnie rozważyć, w jaki sposób będzie on wykorzystywany i jakie dane muszą być chronione.

W celu ustalenia planu strategii serwera FTP należy:

- używać zapory firewall między systemem a siecią Internet,
- używać systemu innego niż produkcyjny jako serwera FTP,
- nie przyłączać serwera FTP do sieci lokalnych (LAN) lub rozległych (WAN) należących do własnej firmy,
- wykorzystać programy obsługi wyjścia FTP, aby zabezpieczyć dostęp do serwera FTP,
- przetestować programy obsługi wyjścia FTP w celu upewnienia się, że nie zawierają one żadnych luk w systemie ochrony,
- nie nadawać anonimowym użytkownikom FTP praw odczytu i zapisu do tego samego katalogu; pozbawia to anonimowych użytkowników możliwości stania się nieuchwytnym w sieci Internet,
- umożliwić dostęp tylko użytkownikom anonimowym; nie pozwolić żadnym innym identyfikatorom użytkownika na uzyskanie dostępu i nie przeprowadzać uwierzytelniania haseł,
- ograniczyć dostęp użytkowników anonimowych tylko do jednej publicznej biblioteki lub jednego katalogu; (Gdzie to będzie? Jak to zostanie wywołane?),
- umieścić w publicznej bibliotece lub katalogu tylko publicznie dostępne pliki,
- ograniczyć komendy użytkowników anonimowych tylko do komend ″przeglądania″ i ″pobierania″ (get, mget); **pod żadnym pozorem nie należy udostępniać użytkownikom anonimowym komend CL,**
- protokołować wszystkie operacje dostępu do serwera FTP,
- przeglądać protokoły serwera FTP raz dziennie lub co najmniej raz w tygodniu, szukając prób włamania,
- sprawdzić raz w miesiącu, czy serwer FTP rejestruje poprawne programy obsługi wyjścia,
- raz w miesiącu testować serwer FTP w poszukiwaniu luk w systemie ochrony.

Pisanie programów obsługi wyjścia dla anonimowego serwera FTP

Aby korzystać z anonimowego serwera FTP w systemie operacyjnym i5/OS, należy napisać dwa programy obsługi wyjścia: program obsługi wyjścia logowania do serwera FTP i program obsługi wyjścia potwierdzenia żądania protokołu FTP.

Pierwszy z nich udostępnia użytkownikom anonimowym identyfikator i wymusza skierowanie ich do publicznej biblioteki lub katalogu. Program obsługi wyjścia potwierdzenia żądania serwera FTP ogranicza dostęp użytkownika anonimowego do komend, plików i bibliotek lub katalogów.

Punkty wyjścia i formaty punktów wyjścia

Serwer FTP komunikuje się z każdym programem obsługi wyjścia za pomocą określonego punktu wyjścia. Parametry przekazywane są pomiędzy serwerem a programem obsługi wyjścia. Format wymienianych informacji określony jest przez format punktu wyjścia.

Program	Punkt wyjścia	Format
Logowanie do serwera	QIBM_QTMF_SVR_LOGON	TCPL0100, TCPL0200 lub TCPL0300. [1]
Potwierdzenie żądań	QIBM_QTMF_SERVER_REQ	VLRQ0100

Program	Punkt wyjścia	Format
[1] Punkt wyjścia może mieć kilka formatów, ale program obsługi wyjścia może być zarejestrowany tylko dla jednego formatu punktu wyjścia. Należy rozważyć każdy z wymienionych formatów, a następnie wybrać najodpowiedniejszy dla posiadanego systemu.		

Przykładowe programy

Dostępne są przykładowe programy ułatwiające konfigurowanie anonimowego serwera FTP w systemie. Przykłady te mogą posłużyć jako wzór do pisania własnych programów. Kopiując fragmenty kodu z tych przykładów, można je dodać do własnych programów. Zalecane jest uruchamianie programów przykładowych na systemie innym niż produkcyjny.

Uwaga: Poniższe programy przykładowe przedstawione są jedynie jako ilustracja. Zawierają one za mało opcji, aby można je było uruchomić na maszynie produkcyjnej. Można ich używać jako podstawy do tworzenia własnego kodu lub wykorzystywać ich części przy pisaniu własnych programów.

Pojęcia pokrewne

Podstawowe informacje o programie System i Navigator

"Punkt wyjścia potwierdzenia żądania: klient i serwer" na stronie 95
Za pomocą punktów wyjścia potwierdzenia żądania można ograniczyć zakres operacji, jakie mogą wykonywać użytkownicy protokołu FTP.

Odsyłacze pokrewne

"Programy obsługi wyjścia FTP" na stronie 94
Istnieje możliwość użycia programów obsługi wyjścia w celu ochrony protokołu FTP. Serwer FTP komunikuje się z każdym programem obsługi wyjścia za pomocą określonego punktu wyjścia. Sekcja zawiera opisy parametrów oraz kody przykładowych programów.

"Punkt wyjścia logowania do serwera FTP" na stronie 106
Uwierzytelnianiem logowania do serwera aplikacji TCP/IP można sterować za pomocą punktu wyjścia logowania do serwera aplikacji TCP/IP. Ten punkt wyjścia umożliwia dostęp do serwera FTP na podstawie adresu systemu, który nawiązał sesję. Dzięki temu można określić początkowy katalog roboczy inny od tego, który znajduje się w profilu użytkownika.

Tworzenie profilu użytkownika ANONYMOUS w systemie i5/OS

Aby nikt nie mógł wpisać się bezpośrednio do systemu operacyjnego i5/OS, korzystając z profilu użytkownika ANONYMOUS, należy utworzyć profil użytkownika ANONYMOUS i przypisać mu hasło *NONE.

Aby utworzyć ten profil przy użyciu programu System i Navigator, wykonaj następujące czynności:

1. W programie **System i Navigator** rozwiń **Użytkownicy i grupy** (Users and Groups).
2. Kliknij prawym przyciskiem myszy **Wszyscy użytkownicy** i wybierz **Nowy użytkownik**.
3. Na panelu Nowi użytkownicy wprowadź następujące informacje:

   Nazwa użytkownika = ANONYMOUS i

   Hasło = Bez hasła.
4. Kliknij przycisk **Zadania** i wybierz zakładkę Ogólne.
5. Na zakładce Ogólne przypisz bibliotekę bieżącą oraz katalog osobisty, z których użytkownik anonymous ma korzystać.
6. Kliknij przycisk **OK** i dokończ inne ustawienia.
7. Kliknij przycisk **Dodaj**, aby utworzyć profil.

Tworzenie publicznej biblioteki lub katalogu

Po utworzeniu anonimowych użytkowników można utworzyć publiczną bibliotekę lub katalog, z którego będą mogli korzystać. Zazwyczaj anonimowi użytkownicy powinni mieć dostęp jedynie do plików publicznych.

Zaleca się, aby użytkownicy ci mieli dostęp tylko do jednej biblioteki lub jednego drzewa katalogów, które zawierają tylko pliki publiczne.

1. Utwórz biblioteki publiczne lub katalogi zawierające pliki dostępne dla anonimowego użytkownika FTP.
2. Załaduj do publicznych bibliotek lub katalogów pliki o dostępie publicznym.
3. Ustaw uprawnienia publicznych bibliotek lub katalogów oraz plików na PUBLIC *USE.

Instalowanie i rejestrowanie programów obsługi wyjścia

Istnieje możliwość utworzenia bibliotek zawierających programy obsługi wyjścia i ich protokoły, a następnie skompilowania i zarejestrowania tych programów jako programów używanych przez serwer FTP.

Pojęcia pokrewne

"Zarządzanie dostępem za pomocą programów obsługi wyjścia FTP" na stronie 23
Dodatkowe bezpieczeństwo można zapewnić, dodając programy obsługi wyjścia FTP do punktów wyjścia serwera i klienta FTP, które oferują więcej możliwości ograniczenia dostępu do systemu.

Zadania pokrewne

"Usuwanie programu obsługi wyjścia" na stronie 133
Kiedy program obsługi wyjścia nie jest już dłużej potrzebny, można go usunąć za pomocą ekranu Praca z programem obsługi wyjścia (Work with Exit Program).

Odsyłacze pokrewne

"Programy obsługi wyjścia FTP" na stronie 94
Istnieje możliwość użycia programów obsługi wyjścia w celu ochrony protokołu FTP. Serwer FTP komunikuje się z każdym programem obsługi wyjścia za pomocą określonego punktu wyjścia. Sekcja zawiera opisy parametrów oraz kody przykładowych programów.

Instalowanie programów obsługi wyjścia:

Aby zainstalować programy obsługi wyjścia dla protokołu FTP w systemie i5/OS, niezbędne jest utworzenie biblioteki zawierającej programy obsługi wyjścia i ich pliki protokołu, skompilowanie programów obsługi wyjścia w bibliotece oraz nadanie obiektom biblioteki, programu i pliku uprawnienia PUBLIC *EXCLUDE.

Serwer aplikacji FTP zaadaptuje uprawnienia, jeśli będzie to konieczne, do określenia i wywołania programu obsługi wyjścia.

Rejestrowanie programów obsługi wyjścia:

Programy obsługi wyjścia nie będą działać, dopóki nie zostaną zarejestrowane. W celu zarejestrowania programów obsługi wyjścia na serwerze FTP systemu i5/OS należy użyć komendy Praca z informacjami rejestracyjnymi (Work with Registration Information - WRKREGINF).

Aby zarejestrować programy obsługi wyjścia, wykonaj następujące czynności:

1. W interfejsie znakowym wprowadź komendę WRKREGINF.
2. Przejdź na następną stronę do punktu wyjścia logowania do serwera FTP:

```
QIBM_QTMF_SVR_LOGON   TCPL0100
QIBM_QTMF_SVR_LOGON   TCPL0200
QIBM_QTMF_SVR_LOGON   TCPL0300
QIBM_QTMF_SERVER_REQ  VLRQ0100
```

3. Wprowadź 8 w polu opcji (Opt) z lewej strony wpisu punktu wyjścia i naciśnij klawisz Enter.
4. Na ekranie Praca z programami obsługi wyjścia wprowadź 1 (dodaj).
5. Wpisz nazwę programu obsługi wyjścia w polu Program obsługi wyjścia.
6. W polu Biblioteka wpisz nazwę biblioteki zawierającej program obsługi wyjścia.
7. Naciśnij klawisz Enter.
8. Zakończ i zrestartuj serwer FTP, aby upewnić się, że wszystkie instancje serwera FTP używają programów obsługi wyjścia.

9. Przetestuj dokładnie programy obsługi wyjścia.

Uwaga: Programy obsługi wyjścia zaczną działać, gdy tylko nastąpi żądanie nowej sesji FTP. Sesje już uruchomione nie zostaną nimi objęte.

Zabezpieczanie protokołu FTP

Dane przesyłane przez protokół FTP można zabezpieczyć za pomocą protokołu SSL, jak również monitorując użytkowników protokołu FTP i zarządzając dostępem użytkowników do funkcji protokołu FTP.

System używany w Internecie jako serwer FTP jest dostępny dla dowolnego użytkownika na świecie. Dlatego też należy zapewnić odpowiednie bezpieczeństwo protokołu FTP, aby przechowywane w systemie istotne dane firmowe nie były zagrożone.

Pojęcia pokrewne

"Konfigurowanie serwera FTP" na stronie 7
Serwer FTP można skonfigurować tak, aby współpracował z klientami FTP z interfejsem graficznym, przeglądarkami WWW oraz narzędziami WWW.

Blokowanie dostępu do serwera FTP

W celu uniemożliwienia jakiegokolwiek dostępu do systemu użytkownika za pomocą protokołu FTP można zablokować port protokołu FTP. Aby nikt nie mógł uzyskać dostępu do systemu użytkownika za pomocą protokołu FTP, należy uniemożliwić uruchamianie serwera FTP.

Blokowanie automatycznego uruchamiania serwera FTP

Jednym ze sposobów zabezpieczenia protokołu FTP jest zablokowanie automatycznego uruchamiania serwera FTP.

Aby zablokować automatyczne uruchamianie zadań serwera FTP przy uruchamianiu protokołu TCP/IP, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Kliknij prawym przyciskiem **FTP** i wybierz **Właściwości**.
3. Anuluj wybór **Uruchom wraz z TCP/IP**.

Blokowanie dostępu do portów FTP

Jednym ze sposobów zabezpieczenia protokołu FTP jest zablokowanie dostępu do portów FTP.

Aby zablokować uruchamianie serwera FTP oraz uniemożliwić innym użytkownikom przypisanie aplikacji użytkownika (na przykład aplikacji używającej gniazd) do portu używanego zwykle przez system do obsługi protokołu FTP, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***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 **Właściwości - Konfiguracja TCP/IP** kliknij zakładkę **Ograniczenia dla portów**.
4. Na stronie **Ograniczenia dla portów** kliknij przycisk **Dodaj**.
5. Na stronie **Dodawanie ograniczeń dla portów** podaj następujące informacje:
   - **Nazwa użytkownika** (User name): podaj nazwę profilu użytkownika, który jest chroniony w systemie. (*profil użytkownika chronionego* to taki, który nie ma 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**: 20
   - **Port końcowy**: 21
   - **Protokół**: TCP

6. Kliknij przycisk **OK**, aby dodać ograniczenie.
7. Na stronie **Ograniczenia dla portów** kliknij przycisk **Dodaj**, a następnie powtórz całą procedurę dla protokołu UDP.
8. Kliknij przycisk **OK**, aby zapisać ograniczenia dla portów i zamknąć okno **Właściwości - Konfiguracja TCP/IP**.

Uwagi:

- 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.
- Informacje o przypisanych numerach portów można znaleźć w serwisie WWW organizacji Internet Assigned Numbers Authority (IANA) pod adresem http://www.iana.org.
- Jeśli porty 20 lub 21 są zastrzeżone dla profilu użytkownika innego niż QTCP, próby uruchomienia serwera FTP spowodują jego natychmiastowe błędne zatrzymanie.
- Ta metoda działa tylko w razie całkowitego ograniczenia aplikacji takich jak serwer FTP. Nie działa w razie ograniczania określonych użytkowników. Kiedy użytkownik łączy się z serwerem FTP, żądanie początkowo korzysta z profilu QTCP. Po pomyślnym połączeniu system zmienia indywidualny profil użytkownika. Każdy użytkownik serwera FTP korzysta z uprawnień QTCP podczas dostępu do portu.

Kontrolowanie dostępu do serwera FTP

Jeśli protokół FTP jest używany, istnieje potrzeba zachowania kontroli nad użytkownikami w celu ochrony danych i sieci. Sekcja ta zawiera wskazówki i uwagi dotyczące ochrony.

Jeśli istnieje potrzeba zezwolenia klientom FTP na dostęp do systemu, trzeba być świadomym następujących zagadnień dotyczących ochrony:

- Schemat uprawnień do obiektu może nie zapewniać dostatecznego zabezpieczenia, jeśli FTP ma dostęp do serwera. Na przykład jeśli użytkownik ma uprawnienia do przeglądania pliku (uprawnienie *USE), może także go skopiować do komputera PC lub innego systemu, podczas gdy niektóre pliki powinny być zabezpieczone przed takim kopiowaniem.
- Programy obsługi wyjścia serwera FTP mogą być wykorzystane do ograniczenia zakresu operacji FTP wykonywanych przez użytkowników. Program obsługi wyjścia potwierdzenia żądania protokołu FTP umożliwia sprawowanie kontroli nad operacjami, które są dozwolone. Na przykład można odrzucać żądania komendy GET dla określonych plików bazy danych.
- Punkt wyjścia logowania do serwera umożliwia uwierzytelnianie użytkowników, którzy logują się na serwerze FTP. W sekcji Konfigurowanie serwera anonimowego FTP opisano, w jaki sposób używać programów obsługi wyjścia w celu zapewnienia obsługi serwera anonimowego FTP w systemie.
- Hasła do serwera FTP nie są szyfrowane podczas ich przesyłania pomiędzy systemem klienta a systemem serwera, chyba że jest używany protokół TLS/SSL. W zależności od metod łączenia, system może być podatny na kradzież haseł poprzez podsłuchiwanie linii.
- Jeśli wartość systemowa QMAXSGNACN jest ustawiona na 1, to wartość systemowa QMAXSIGN stosowana jest dla usługi TELNET, a nie dla usługi FTP. Jeśli QMAXSGNACN jest ustawiona na 2 lub 3 (wartości, które wyłączają profil, jeśli przekroczona jest maksymalna liczba wpisów), próby logowania do serwera FTP są zliczane. W takim wypadku haker może zaatakować, powodując odmowę wykonania usługi przez FTP powtarzając próby zalogowania się za pomocą nieprawidłowego hasła do czasu, aż profil użytkownika nie zostanie wyłączony.
- Po każdej nieudanej próbie logowania system zapisuje komunikat CPF2234 w protokole QHST. Można napisać program monitorujący protokół QHST w celu poszukiwania tego komunikatu. Jeśli program wykryje powtarzające się próby, może zakończyć działanie serwera FTP.
- Parametr limitu czasu bezczynności (INACTTIMO) można wykorzystać podczas konfigurowania FTP, aby zredukować ryzyko wystawienia serwera, kiedy użytkownik opuszcza sesję FTP nie nadzorując jej. Aby zrozumieć istotę współpracy parametru INACTTIMO z licznikiem czasu połączeń (dla uruchomień systemu), należy zapoznać się z dokumentacją lub pomocą elektroniczną.

Uwaga: Wartość systemowa limitu czasu dla zadań nieaktywnych (Time-out interval for inactive jobs - QINACTITV) nie wpływa na sesje FTP.

- W przypadku korzystania z obsługi FTP jako zadania wsadowego program musi wysłać do systemu serwera zarówno identyfikator użytkownika, jak i hasło. Identyfikator i hasło muszą być zakodowane w programie lub program musi odczytywać je z pliku. Opcje przechowywania haseł i identyfikatorów użytkowników mogą stanowić potencjalne ryzyko naruszenia bezpieczeństwa. Jeśli korzysta się z FTP jako zadania wsadowego, należy upewnić się, że do zabezpieczenia informacji o identyfikatorze użytkownika i haśle wykorzystywana jest ochrona obiektu. Zalecane jest także korzystanie z jednego identyfikatora użytkownika, który w systemie docelowym ma ograniczone uprawnienia. Powinien on mieć uprawnienia wystarczające tylko do wykonywania potrzebnych funkcji, takich jak przesyłanie pliku.
- Protokół FTP umożliwia korzystanie z komend zdalnych, podobnie jak zaawansowana komunikacja program-program (Advanced program-to-program communications - APPC) i produkt System i Access for Windows. Komenda serwera FTP RCMD (Komenda zdalna) jest równoważna dostępowi do wiersza komend w systemie. Zanim FTP zostanie udostępniony, należy upewnić się, że schemat ochrony obiektu jest odpowiedni. Do ograniczenia lub odrzucania wywołań komendy RCMD można użyć także programu obsługi wyjścia serwera FTP. W sekcji Programy obsługi wyjścia serwera FTP znajduje się opis tych punktów wyjścia oraz przykładowe programy.
- Użytkownik może mieć dostęp poprzez FTP do obiektów zintegrowanego systemu plików. Dlatego kiedy w systemie uruchamiany jest serwer FTP, należy się upewnić, że schemat uprawnień zintegrowanego systemu plików jest właściwy.
- Do częstych praktyk stosowanych przez hakerów należy ustawianie nie wzbudzających podejrzeń serwerów jako magazynów informacji. Czasami te informacje mogą być nielegalne lub mogą zawierać treści pornograficzne. Jeśli haker uzyska dostęp do serwera przez protokół FTP, ładuje te niepożądane informacje do systemu. Następnie informuje innych o adresie FTP tego serwera. Wtedy inni hakerzy uzyskują dostęp do systemu za pomocą protokołu FTP i pobierają te niepożądane informacje.

  Przed tego typu atakiem można się zabezpieczyć, korzystając z programów obsługi wyjścia serwera FTP. Na przykład można skierować wszystkie żądania przesłania informacji do katalogu, który jest tylko do odczytu. Niweczy to cel hakera, ponieważ jego znajomi nie będą mogli pobrać informacji z katalogu.

  Pojęcia pokrewne

  “Konfigurowanie anonimowego serwera FTP” na stronie 12
  Anonimowy serwer FTP umożliwia zdalnym użytkownikom korzystanie z serwera FTP bez przypisanego ID użytkownika i hasła.

  Odsyłacze pokrewne

  “Punkt wyjścia logowania do serwera FTP” na stronie 106
  Uwierzytelnianiem logowania do serwera aplikacji TCP/IP można sterować za pomocą punktu wyjścia logowania do serwera aplikacji TCP/IP. Ten punkt wyjścia umożliwia dostęp do serwera FTP na podstawie adresu systemu, który nawiązał sesję. Dzięki temu można określić początkowy katalog roboczy inny od tego, który znajduje się w profilu użytkownika.

  “Korzystanie z protokołu FTP w trybie nienadzorowanym za pomocą zadania wsadowego” na stronie 33
  Klient FTP może być uruchamiany interaktywnie lub w trybie nienadzorowanym. Ten temat zawiera jeden prosty i jeden zaawansowany przykład użycia metody zadania wsadowego protokołu FTP.

  “Programy obsługi wyjścia FTP” na stronie 94
  Istnieje możliwość użycia programów obsługi wyjścia w celu ochrony protokołu FTP. Serwer FTP komunikuje się z każdym programem obsługi wyjścia za pomocą określonego punktu wyjścia. Sekcja zawiera opisy parametrów oraz kody przykładowych programów.

  Informacje pokrewne

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

Używanie protokołu SSL do zabezpieczania serwera FTP

Protokół SSL pozwala uniknąć jawnego przesyłania haseł i danych podczas używania serwera FTP z klientem FTP, który również korzysta z protokołu SSL.

Serwer FTP zapewnia zaawansowaną ochronę podczas wysyłania i otrzymywania plików poprzez sieć niezaufaną. Serwer FTP używa warstwy SSL do zabezpieczenia haseł i innych wrażliwych danych podczas wymiany informacji. Serwer FTP obsługuje chronione sesje SSL lub TLS, w tym uwierzytelnianie klienta oraz automatyczne logowanie.

Większość aplikacji obsługujących SSL łączy klienta z oddzielnymi portami TCP, innym dla sesji niechronionych, a innym dla sesji chronionych. Jednak ochrona FTP jest bardziej elastyczna. Klient może połączyć się z nieszyfrowanym portem TCP (zazwyczaj jest to port 21), a następnie negocjować opcje uwierzytelniania i szyfrowania. Klient może także wybrać chroniony port FTP (zazwyczaj jest to port 990), który domyślnie przyjmuje połączenia SSL. Obie te opcje są dostępne na serwerze FTP.

Przed skonfigurowaniem serwera FTP w celu korzystania z protokołu SSL należy w systemie zainstalować wstępnie wymagane programy i skonfigurować certyfikaty cyfrowe.

Uwaga: Należy utworzyć lokalny ośrodek certyfikacji lub skonfigurować na serwerze FTP certyfikat publiczny protokołu SSL, korzystając z programu Digital Certificate Manager (DCM).

Pojęcia pokrewne

Protokół SSL

Pojęcia związane z protokołem SSL

Wymaganie wstępne - programy

“Zabezpieczanie klientów FTP za pomocą protokołu TLS lub SSL” na stronie 22
Dane przesyłane za pomocą połączeń sterujących i połączeń danych protokołu FTP można szyfrować, korzystając z połączeń TLS lub SSL.

Zadania pokrewne

Konfigurowanie certyfikatów cyfrowych

Używanie certyfikatu publicznego

Tworzenie lokalnego ośrodka certyfikacji

Lokalny ośrodek certyfikacji można utworzyć i prowadzić w systemie przy użyciu programu IBM Digital Certificate Manager (DCM). Lokalny ośrodek CA umożliwia wystawianie prywatnych certyfikatów dla aplikacji uruchamianych w systemie.

Aby utworzyć i prowadzić lokalny ośrodek CA w systemie za pomocą programu DCM, wykonaj następujące czynności:

1. Uruchom program IBM Digital Certificate Manager. Jeśli jest konieczne uzyskanie lub utworzenie certyfikatów albo skonfigurowanie lub zmiana systemu certyfikatów, należy zrobić to w tym momencie.
2. W ramce nawigacji programu DCM wybierz **Tworzenie ośrodka certyfikacji**, aby wyświetlić szereg formularzy. Formularze te prowadzą przez proces tworzenia lokalnego ośrodka CA i wykonywania innych czynności niezbędnych do rozpoczęcia korzystania z certyfikatów cyfrowych dla protokołu SSL, podpisywania obiektów i weryfikowania podpisów.
3. Uzupełnij wszystkie wyświetlane formularze. Każdej czynności, która musi być wykonana w celu utworzenia i prowadzenia lokalnego ośrodka CA w systemie, odpowiada oddzielny formularz. Wypełniając te formularze, wykonaj następujące czynności:
   a. Wybierz, w jaki sposób ma być przechowywany klucz prywatny certyfikatu lokalnego CA. Ta czynność wymagana jest tylko wtedy, jeśli w systemie zainstalowany jest koprocesor szyfrujący IBM 4758-023 PCI. Jeśli w systemie nie ma takiego koprocesora, program DCM automatycznie składuje certyfikat i jego klucz prywatny w bazie certyfikatów lokalnego ośrodka certyfikacji.
   b. Wprowadź informacje identyfikujące lokalny ośrodek CA.
   c. Zainstaluj lokalny certyfikat CA na komputerze PC lub w przeglądarce. Dzięki temu oprogramowanie będzie mogło rozpoznać lokalny ośrodek certyfikacji (CA) oraz wydawane przez niego certyfikaty.
   d. Wybierz dane strategii dla lokalnego ośrodka CA.
   e. Użyj nowego lokalnego ośrodka CA do wystawienia certyfikatu klienta lub serwera, z którego aplikacja będzie mogła skorzystać do nawiązywania połączeń z użyciem protokołu SSL. Jeśli w systemie jest zainstalowany

koprocesor szyfrujący IBM 4758-023 PCI, ten krok umożliwia wybór metody przechowywania klucza prywatnego dla certyfikatu serwera lub klienta. Jeśli w systemie nie ma tego koprocesora, program DCM automatycznie umieszcza certyfikat i jego klucz prywatny w bazie certyfikatów *SYSTEM. Program DCM tworzy bazę certyfikatów *SYSTEM jako część tego zadania.

f. Wybierz aplikacje, które będą mogły używać certyfikatu serwera lub klienta w połączeniach SSL.

   Uwaga: Wybierz ID aplikacji serwera FTP i5/OS (QIBM_QTMF_FTP_SERVER).

g. Użyj nowego lokalnego ośrodka CA do wystawienia certyfikatu podpisującego obiekt, z którego aplikacje będą mogły korzystać do cyfrowego podpisywania obiektów. Zadanie to tworzy bazę certyfikatów *OBJECTSIGNING, której można używać do zarządzania certyfikatami do podpisywania obiektów.

   Uwaga: Mimo że w tym scenariuszu nie są używane certyfikaty do podpisywania obiektów, ten krok należy wykonać. Jeśli w tym miejscu przerwane zostanie wykonywanie zadania, należy wykonać inne zadania, które umożliwią zakończenie konfigurowania certyfikatów SSL.

h. Wybierz aplikacje ufające lokalnemu ośrodkowi CA.

   Uwaga: Wybierz ID aplikacji serwera FTP i5/OS (QIBM_QTMF_FTP_SERVER).

Zadania pokrewne

Uruchamianie programu Digital Certificate Manager

Zarządzanie certyfikatami użytkowników

Używanie interfejsów API do programowego wystawiania certyfikatów użytkownikom serwerów innych niż System i

Uzyskiwanie kopii certyfikatu prywatnego ośrodka CA

Wiązanie certyfikatu z serwerem FTP

Jeśli podczas tworzenia lokalnego ośrodka certyfikacji nie przypisano certyfikatu do aplikacji serwera FTP lub jeśli system został skonfigurowany tak, aby żądał certyfikatu z publicznego ośrodka CA, należy powiązać certyfikat z serwerem FTP.

Aby powiązać certyfikat z serwerem FTP, wykonaj następujące czynności:

1. Uruchom program IBM Digital Certificate Manager. Jeśli jest konieczne uzyskanie lub utworzenie certyfikatów albo skonfigurowanie lub zmiana systemu certyfikatów, należy zrobić to w tym momencie. Informacje na temat konfigurowania systemu certyfikatów zawiera sekcja Konfigurowanie programu DCM.
2. Kliknij przycisk **Wybierz bazę certyfikatów**.
3. Wybierz ***SYSTEM**. Kliknij przycisk **Kontynuuj**.
4. Wpisz hasło bazy certyfikatów *SYSTEM. Kliknij przycisk **Kontynuuj**.
5. Po odświeżeniu menu nawigacji po lewej stronie, rozwiń pozycję **Zarządzanie aplikacjami**.
6. Kliknij **Aktualizacja przypisania certyfikatów**.
7. Na następnym ekranie wybierz aplikację **Serwer**. Kliknij przycisk **Kontynuuj**.
8. Kliknij element **Serwer TCP/IP FTP systemu i5/OS**.
9. Kliknij element **Aktualizuj przypisania certyfikatów**, aby przypisać certyfikat do serwera FTP.
10. Z listy wybierz certyfikat, aby przypisać go do serwera.
11. Kliknij **Przypisanie nowego certyfikatu**.
12. Program DCM przejdzie do strony **Aktualizuj przypisania certyfikatów**, pokazując komunikat potwierdzający. Kiedy zakończysz konfigurację certyfikatów dla serwera FTP, kliknij przycisk **Gotowe**.

Zadania pokrewne

Uruchamianie programu Digital Certificate Manager

“Aktywowanie protokołu SSL na serwerze FTP” na stronie 21
Aktywowanie protokołu SSL na serwerze FTP udostępnia więcej opcji zabezpieczających dla tego serwera.

Wymaganie uwierzytelniania klienta przez serwer FTP

Jeśli serwer FTP jest potrzebny do uwierzytelniania klientów, można zmienić specyfikację aplikacji w programie IBM Digital Certificate Manager (DCM). Czynność ta jest opcjonalna.

Uwaga: Za pomocą serwera FTP można uwierzytelniać klientów, nie można jednak uwierzytelnić klienta FTP systemu i5/OS. Może być wymagane uwierzytelnienie klienta, nie będzie ono jednak obejmowało połączeń dla klientów FTP systemu i5/OS.

Jeśli klient FTP nawiązuje połączenie z serwerem FTP, na którym jest włączona opcja uwierzytelniania klienta, musi wysłać podkomendę USER. Po wysłaniu podkomendy USER wraz z odpowiednimi informacjami serwer FTP sprawdzi, czy użytkownik jest zgodny z profilem powiązanym z certyfikatem klienta, który klient wysłał w trakcie uzgadniania połączenia SSL. Jeśli użytkownik i certyfikat są zgodne, nie jest potrzebne hasło, a serwer FTP loguje użytkownika do systemu. Podkomenda USER jest wymagana, ponieważ w protokole FTP nie ma mechanizmu informującego klienta o jego zalogowaniu bez użycia tej komendy.

1. Uruchom program IBM Digital Certificate Manager. Jeśli jest konieczne uzyskanie lub utworzenie certyfikatów albo skonfigurowanie lub zmiana systemu certyfikatów, należy zrobić to w tym momencie. Informacje dotyczące konfigurowania ośrodka certyfikacji zawiera sekcja Konfigurowanie programu DCM.
2. Kliknij przycisk **Wybierz bazę certyfikatów**.
3. Wybierz ***SYSTEM**. Kliknij przycisk **Kontynuuj**.
4. Wpisz hasło bazy certyfikatów *SYSTEM. Kliknij przycisk **Kontynuuj**.
5. Po odświeżeniu menu nawigacji po lewej stronie, rozwiń pozycję **Zarządzanie aplikacjami**.
6. Kliknij **Aktualizuj definicję aplikacji**.
7. Na następnym ekranie wybierz aplikację **Serwer**. Kliknij przycisk **Kontynuuj**.
8. Kliknij element **Serwer TCP/IP FTP systemu i5/OS**.
9. Kliknij **Aktualizuj definicję aplikacji**.
10. W tabeli, która się pojawi, wybierz **Tak**, aby żądać uwierzytelniania klienta.
11. Kliknij przycisk **Zastosuj**.
12. Program DCM przejdzie do strony **Aktualizuj definicję aplikacji**, pokazując komunikat potwierdzający. Kiedy zakończysz aktualizację definicji aplikacji dla serwera FTP, kliknij przycisk **Gotowe**.

Zadania pokrewne

Uruchamianie programu Digital Certificate Manager

Aktywowanie protokołu SSL na serwerze FTP

Aktywowanie protokołu SSL na serwerze FTP udostępnia więcej opcji zabezpieczających dla tego serwera.

Aby aktywować protokół SSL na serwerze FTP, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system* → Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Kliknij prawym przyciskiem **FTP**.
3. Wybierz opcję **Właściwości** (Properties).
4. Wybierz zakładkę **Ogólne** (General).
5. Wybierz jedną z następujących opcji do obsługi SSL:
   - **Tylko połączenia chronione**

     Wybierz tę opcję, aby zezwolić na nawiązywanie z serwerem FTP tylko sesji SSL. Połączenia mogą być nawiązywane z niechronionym portem FTP, ale klient FTP musi wynegocjować sesję SSL, zanim użytkownik będzie mógł się zalogować.
   - **Tylko połączenia niechronione**

     Wybierz tę opcję, aby zabronić nawiązywania sesji chronionych. Próby połączenia z portem SSL będą blokowane.
   - **Połączenia chronione i niechronione**

Wybór zezwala na sesje zarówno chronione, jak i niechronione.

Uwaga: Nie trzeba restartować serwera FTP. Wykryje on dynamicznie, że został przypisany do niego certyfikat. Jeśli tego nie zrobi, należy sprawdzić, czy w systemie są zainstalowane najnowsze poprawki PTF.

Zadania pokrewne

"Wiązanie certyfikatu z serwerem FTP" na stronie 20
Jeśli podczas tworzenia lokalnego ośrodka certyfikacji nie przypisano certyfikatu do aplikacji serwera FTP lub jeśli system został skonfigurowany tak, aby żądał certyfikatu z publicznego ośrodka CA, należy powiązać certyfikat z serwerem FTP.

Zabezpieczanie klientów FTP za pomocą protokołu TLS lub SSL

Dane przesyłane za pomocą połączeń sterujących i połączeń danych protokołu FTP można szyfrować, korzystając z połączeń TLS lub SSL.

Podstawową przyczyną szyfrowania połączenia sterującego jest chęć ukrycia hasła podczas logowania do serwera FTP.

Aby klient FTP mógł nawiązywać bezpieczne połączenia z serwerami FTP, należy za pomocą programu DCM skonfigurować zaufane ośrodki certyfikacji dla tego klienta. Należy także dodać wszystkie ośrodki certyfikacji użyte do utworzenia certyfikatów przypisanych do serwerów FTP, z którymi będzie nawiązywane połączenie. W zależności od używanych ośrodków CA może być wymagane wyeksportowanie lub zaimportowanie certyfikatów ośrodka certyfikacji.

Jeśli dla połączenia sterującego wybrane zostanie szyfrowanie TLS/SSL, klient FTP domyślnie zaszyfruje także dane przesyłane przez połączenie dla danych. Protokół FTP nie pozwala na istnienie chronionego połączenia dla danych, gdy nie ma chronionego połączenia sterującego.

Szyfrowanie może istotnie wpłynąć na wydajność, ale może zostać pominięte w przypadku połączenia dla danych. Pozwala to na przesyłanie mniej ważnych plików bez zmniejszania wydajności oraz na zabezpieczenie ochrony systemu przez nieujawnianie haseł.

Klient FTP używa specyficznych parametrów komendy CL STRTCPFTP oraz podkomend, które są wykorzystywane jako część obsługi TLS/SSL (SECOpen i SECData).

Określanie poziomu ochrony protokołu TLS/SSL klienta FTP systemu i5/OS

Połączenie sterujące

Ochrona TLS/SSL może być ustawiona za pomocą komendy STRTCPFTP i SECOPEN.

Dla komendy STRTCPFTP (FTP) należy podać *SSL dla parametru SECCNN ochrony połączenia, aby zażądać chronionego połączenia sterującego. Można także określić opcję *IMPLICIT, aby uzyskać połączenie chronione przez wcześniej zdefiniowany numer portu serwera.

Do uzyskania chronionego połączenia sterującego można podczas sesji użyć komendy klienta FTP SECOPEN.

Połączenie dla danych

Dla komendy STRTCPFTP (FTP) należy podać *PRIVATE dla parametru DTAPROT ochrony danych, aby określić chronione połączenie dla danych. Aby dane były wysyłane bez szyfrowania, należy podać *CLEAR dla parametru DTAPROT ochrony danych.

Po nawiązaniu chronionego połączenia sterującego, do zmiany poziomu ochrony połączenia dla danych można użyć komendy SECDATA.

Niejawne połączenie SSL

Niektóre serwery FTP obsługują połączenia zwane niejawnymi połączeniami SSL. Takie połączenie oferuje te same zabezpieczenie szyfrujące, jak opcja *SSL, ale może być nawiązywane tylko przez wcześniej określony port serwera, zazwyczaj 990, dla którego serwer musi być skonfigurowany w celu oczekiwania na negocjację połączenia SSL/TLS.

Metodę tę udostępniono, aby umożliwić połączenia chronione dla tych implementacji FTP, które nie obsługują standardowego protokołu zapewniającego ochronę TLS/SSL.

Wiele wczesnych implementacji obsługi SSL korzysta z połączeń niejawnych, obecnie jednak grupa IETF uznała je za nieaktualne.

Uwaga:

Standardowy protokół konfigurowania połączenia TLS/SSL wymaga, aby podczas łączenia się z serwerem FTP została użyta podkomenda AUTH (Autoryzacja - Authorization). Do określenia poziomu ochrony używane są komendy serwera PBSZ i PROT.

Jednak w przypadku niejawnych połączeń SSL podkomendy serwera AUTH, PBSZ i PROT nie są wysyłane do serwera FTP. Zamiast tego serwer działa tak, jakby klient przesłał te podkomendy z następującymi parametrami:

- AUTH SSL
- PBSZ 0
- PROT P

Pojęcia pokrewne

"Używanie protokołu SSL do zabezpieczania serwera FTP" na stronie 18
Protokół SSL pozwala uniknąć jawnego przesyłania haseł i danych podczas używania serwera FTP z klientem FTP, który również korzysta z protokołu SSL.

Zadania pokrewne

Definiowanie listy zaufanych ośrodków CA dla aplikacji

"Określanie lokalnego ośrodka CA MojejFirmy jako zaufanego ośrodka CA dla klienta FTP IchFirmy" na stronie 7
Zanim IchFirma będzie mogła korzystać z klienta FTP do nawiązywania bezpiecznych połączeń z serwerem FTP MojejFirmy, musi za pomocą programu Digital Certificate Manager (DCM) określić, którym ośrodkom certyfikacji klient powinien ufać. Oznacza to, że IchFirma musi określić, że zaimportowany wcześniej certyfikat lokalnego ośrodka CA jest godny zaufania.

Odsyłacze pokrewne

"Scenariusz: zabezpieczanie protokołu FTP za pomocą protokołu SSL" na stronie 3
W tym scenariuszu pokazano, jak przesyłać dane do przedsiębiorstwa partnerskiego przy użyciu protokołu SSL. Korzystając z protokołu SSL, aplikacje klienta i serwera FTP na platformach System i mogą komunikować się ze sobą w sposób umożliwiający zablokowanie podsłuchiwania komunikatów, manipulowania przy nich i ich fałszowania.

"Uruchamianie i zatrzymywanie sesji klienta" na stronie 28
Po uzyskaniu identyfikatora logowania i hasła do zdalnego serwera FTP można uruchomić sesję klienta z tym serwerem FTP. Sesję klienta można zakończyć przy użyciu podkomendy QUIT serwera FTP.

"SECOpen (Konfigurowanie ochrony danych - Setting data security protection)" na stronie 86
Podkomenda SECOPEN klienta FTP i5/OS służy do otwierania chronionego połączenia sterującego z serwerem FTP przy użyciu określonej opcji ochrony.

"SECData (Konfigurowanie ochrony danych - Setting data security protection)" na stronie 85
Podkomenda SECData klienta FTP i5/OS służy do określania poziomu ochrony, który ma być stosowany dla połączeń danych, gdy z systemem zdalnym jest już nawiązane chronione połączenie sterujące.

Zarządzanie dostępem za pomocą programów obsługi wyjścia FTP

Dodatkowe bezpieczeństwo można zapewnić, dodając programy obsługi wyjścia FTP do punktów wyjścia serwera i klienta FTP, które oferują więcej możliwości ograniczenia dostępu do systemu.

Aby ograniczyć dostęp użytkowników do komend CL i podkomend FTP, można napisać program obsługi wyjścia potwierdzania żądań serwera FTP.

Uwierzytelnianiem użytkowników serwera aplikacji TCP/IP można sterować za pomocą programu obsługi wyjścia dla punktu wyjścia logowania do serwera.

Program obsługi wyjścia potwierdzania żądań klienta FTP można napisać dla punktu wyjścia klienta: potwierdzanie żądań. Decyduje to o tym, z jakich funkcji klienta FTP może korzystać użytkownik.

W zależności od sytuacji, zamiast pisania programów obsługi wyjścia potwierdzania żądań serwera FTP oraz punktów wyjścia potwierdzania żądań klienta FTP, można rozważyć ograniczenie dostępu do podkomend FTP za pomocą funkcji ograniczania dostępu Administrowanie aplikacjami (Application Administration).

Aby zapewnić poprawność działania programów obsługi wyjścia, należy zainstalować i zarejestrować programy obsługi wyjścia. Jeśli programy obsługi wyjścia nie są już potrzebne, należy je prawidłowo usunąć, aby zapobiec ich uruchamianiu w przyszłości.

Pojęcia pokrewne

"Konfigurowanie anonimowego serwera FTP" na stronie 12
Anonimowy serwer FTP umożliwia zdalnym użytkownikom korzystanie z serwera FTP bez przypisanego ID użytkownika i hasła.

"Punkt wyjścia potwierdzenia żądania: klient i serwer" na stronie 95
Za pomocą punktów wyjścia potwierdzenia żądania można ograniczyć zakres operacji, jakie mogą wykonywać użytkownicy protokołu FTP.

Zadania pokrewne

"Zarządzanie dostępem za pomocą programu System i Navigator"
Dostęp do serwera lub klienta FTP można ograniczyć za pomocą opcji Administrowanie aplikacjami (Application Administration) w programie System i Navigator. Opcja Administrowanie aplikacjami jest komponentem programu System i Navigator, który użytkownik może wybrać do zainstalowania.

"Instalowanie i rejestrowanie programów obsługi wyjścia" na stronie 15
Istnieje możliwość utworzenia bibliotek zawierających programy obsługi wyjścia i ich protokoły, a następnie skompilowania i zarejestrowania tych programów jako programów używanych przez serwer FTP.

"Usuwanie programu obsługi wyjścia" na stronie 133
Kiedy program obsługi wyjścia nie jest już dłużej potrzebny, można go usunąć za pomocą ekranu Praca z programem obsługi wyjścia (Work with Exit Program).

Odsyłacze pokrewne

"Programy obsługi wyjścia FTP" na stronie 94
Istnieje możliwość użycia programów obsługi wyjścia w celu ochrony protokołu FTP. Serwer FTP komunikuje się z każdym programem obsługi wyjścia za pomocą określonego punktu wyjścia. Sekcja zawiera opisy parametrów oraz kody przykładowych programów.

"Punkt wyjścia logowania do serwera FTP" na stronie 106
Uwierzytelnianiem logowania do serwera aplikacji TCP/IP można sterować za pomocą punktu wyjścia logowania do serwera aplikacji TCP/IP. Ten punkt wyjścia umożliwia dostęp do serwera FTP na podstawie adresu systemu, który nawiązał sesję. Dzięki temu można określić początkowy katalog roboczy inny od tego, który znajduje się w profilu użytkownika.

"Format punktu wyjścia VLRQ0100" na stronie 103
Punktem wyjścia potwierdzenia żądania aplikacji serwera FTP jest QIBM_QTMF_SERVER_REQ. Punktem wyjścia potwierdzenia żądania aplikacji klienta FTP jest QIBM_QTMF_CLIENT_REQ. Interfejs sterujący formatem parametru dla tego punktu wyjścia to VLRQ0100. Interfejs punktu wyjścia VLRQ0100 zawiera określone parametry.

Zarządzanie dostępem za pomocą programu System i Navigator

Dostęp do serwera lub klienta FTP można ograniczyć za pomocą opcji Administrowanie aplikacjami (Application Administration) w programie System i Navigator. Opcja Administrowanie aplikacjami jest komponentem programu System i Navigator, który użytkownik może wybrać do zainstalowania.

Program System i Navigator umożliwia ograniczenie dostępu użytkownikom do funkcji serwera i klienta FTP. Za pomocą opcji Administrowanie aplikacjami można nadawać poszczególnym użytkownikom lub grupom użytkowników uprawnienia dostępu do poszczególnych funkcji lub odmawiać im tego dostępu. Dostępem do funkcji protokołu FTP można także zarządzać, pisząc programy obsługi wyjścia FTP dla punktów wyjścia potwierdzenia żądania FTP.

Aby zarządzać dostępem użytkowników do funkcji przy użyciu programu System i Navigator, wykonaj następujące czynności:

1. W programie System i Navigator kliknij prawym przyciskiem myszy pozycję ***system*** (*system*) i wybierz opcję **Administrowanie aplikacjami** (Application Administration).
2. Wybierz zakładkę **Aplikacje hosta**.
3. Rozwiń pozycję **Narzędzia protokołu TCP/IP dla i5/OS → Protokół FTP** (TCP/IP Utilities for i5/OS > File Transfer Protocol (FTP)).
4. Rozwiń **Klient FTP** lub **Serwer FTP**.
5. Wybierz funkcję, do której chcesz umożliwić lub zablokować dostęp.
6. Kliknij **Dostosuj**.
7. Za pomocą okna dialogowego **Dostosowanie dostępu** zmień listę użytkowników i grup, które mają dostęp do danej funkcji lub nie.
8. Kliknij przycisk **OK**, aby zapisać zmiany na stronie **Dostosowanie dostępu**.
9. Kliknij przycisk **OK**, aby opuścić stronę **Administracja aplikacji**.

Dostępem określonego użytkownika lub grupy użytkowników do zarejestrowanych funkcji FTP można także zarządzać za pomocą narzędzia Zarządzanie użytkownikami i grupami (Users and Groups management) w programie System i Navigator. Aby to zrobić, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń ***system*** **→ Użytkownicy i grupy** (*system* > Users and Groups).
2. Wybierz **Wszyscy użytkownicy** lub **Grupy**.
3. Kliknij prawym przyciskiem myszy grupę, a następnie wybierz opcję **Właściwości** (Properties).
4. Kliknij **Możliwości**.
5. Kliknij **Aplikacje**.

   W tym miejscu można zmieniać ustawienia użytkownika lub grupy dla wyświetlonej funkcji. Można także zmieniać ustawienia dla wszystkich funkcji w hierarchii, zmieniając ustawienia funkcji wyższego poziomu.

   Pojęcia pokrewne

   “Zarządzanie dostępem za pomocą programów obsługi wyjścia FTP” na stronie 23
   Dodatkowe bezpieczeństwo można zapewnić, dodając programy obsługi wyjścia FTP do punktów wyjścia serwera i klienta FTP, które oferują więcej możliwości ograniczenia dostępu do systemu.

Monitorowanie przyłączających się użytkowników FTP

W celu monitorowania aktywności i sprawdzania, czy nie miały miejsca ataki z zewnątrz, należy protokołować użycie protokołu FTP i przeglądać pliki protokołów.

Aby monitorować przyłączających się użytkowników FTP, wykonaj poniższe czynności:

1. W programie System i Navigator rozwiń **serwer → Sieć → Serwery → TCP/IP** (server > Network > Servers > TCP/IP).
2. W prawym panelu kliknij prawym przyciskiem myszy **FTP** i wybierz **Zadania serwera**.
3. Zostanie otwarty panel zadań serwera FTP. W kolumnie Aktualny użytkownik (Current user) zostanie wyświetlony użytkownik zalogowany w zadaniu serwera. Jeśli nie będzie zalogowany żaden użytkownik, zostanie wyświetlona pozycja Qtcp. Aby odświeżyć ekran, naciśnij klawisz F5 lub wybierz kolejno polecenia **Widok → Odśwież**.

Format nazw tych zadań ma postać *QTFTPnnnnn*, gdzie *nnnnn* jest liczbą losową.

Zadania pokrewne

"Uruchamianie i zatrzymywanie serwera FTP"
Serwer FTP można uruchamiać i zatrzymywać za pomocą programu System i Navigator.

Zarządzanie serwerem FTP

Zarządzanie serwerem FTP obejmuje uruchamianie i zatrzymywanie serwera, zarządzanie bezpieczeństwem FTP i korzystanie z protokołu SSL.

System można skonfigurować tak, aby możliwe było wysyłanie, odbieranie i współużytkowanie plików w sieciach za pomocą protokołu FTP. Protokół FTP składa się z dwóch części: klienta FTP i serwera FTP. Użytkownik pracuje z klientem FTP. Klient FTP komunikuje się z serwerem FTP. Bezpośrednia współpraca z serwerem FTP nie jest zazwyczaj wymagana.

Uruchamianie i zatrzymywanie serwera FTP

Serwer FTP można uruchamiać i zatrzymywać za pomocą programu System i Navigator.

Instrukcje dotyczące uzyskiwania dostępu do serwera FTP znajdują się w sekcji "Konfigurowanie serwera FTP za pomocą programu System i Navigator" na stronie 8.

Aby uruchomić serwer FTP, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. W prawym panelu kliknij prawym przyciskiem myszy **FTP** i wybierz **Uruchom**.

Aby zatrzymać serwer FTP, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. W prawym panelu kliknij prawym przyciskiem myszy **FTP** i wybierz **Zatrzymaj**.

Pojęcia pokrewne

"Określanie problemów związanych z protokołem FTP" na stronie 152
Jeśli podczas korzystania z protokołu FTP wystąpi problem, należy za pomocą schematu oraz list przyczyn, które są zawarte w poniższym temacie, zidentyfikować przyczynę tego problemu.

Zadania pokrewne

"Monitorowanie przyłączających się użytkowników FTP" na stronie 25
W celu monitorowania aktywności i sprawdzania, czy nie miały miejsca ataki z zewnątrz, należy protokołować użycie protokołu FTP i przeglądać pliki protokołów.

"Konfigurowanie serwera FTP za pomocą programu System i Navigator" na stronie 8
System i Navigator udostępnia graficzny interfejs użytkownika (GUI), za pomocą którego można skonfigurować serwer FTP i5/OS i zarządzać nim.

"Usuwanie programu obsługi wyjścia" na stronie 133
Kiedy program obsługi wyjścia nie jest już dłużej potrzebny, można go usunąć za pomocą ekranu Praca z programem obsługi wyjścia (Work with Exit Program).

Ustawianie liczby dostępnych serwerów FTP

W systemie można określić minimalną liczbę dostępnych serwerów dla przyszłych połączeń klientów.

Określenie wartości 1 opóźnia połączenia przychodzące do serwera FTP. Zalecaną wartością jest 3.

Aby ustawić tę wartość, należy przejść na stronę **Właściwości FTP** i podać liczbę z zakresu od 1 do 20 dla **Początkowej liczby serwerów do uruchomienia**.

Kiedy klient łączy się z serwerem FTP i5/OS, serwer FTP sprawdza liczbę aktywnych serwerów FTP, które nie są połączone z żadnym klientem, oraz wartość podaną jako początkowa liczba serwerów FTP do uruchomienia. Jeśli ta wartość jest większa niż liczba dostępnych serwerów FTP, uruchamiane są dodatkowe serwery FTP, dopóki te liczby nie będą równe. Jeśli natomiast wartość początkowa jest mniejsza niż liczba dostępnych serwerów FTP, nie jest podejmowane żadne działanie. Zmiana początkowej liczby serwerów FTP ma miejsce podczas następnego połączenia z klientem po aktywowaniu powyższego procesu.

Jeśli na przykład w tym samym czasie jest uruchomionych pięć sesji klienta FTP, a początkowa liczba serwerów FTP jest ustawiona na 10, będzie działało 15 serwerów FTP. Te 15 serwerów obejmuje pięć serwerów FTP dla pięciu aktywnych sesji klientów oraz dziesięć dostępnych serwerów FTP. Liczba dostępnych serwerów może być większa niż ich liczba początkowa. Jeśli w tym samym przykładzie pięciu klientów zakończy swoje sesje, a inne sesje nie zostaną uruchomione, dostępnych będzie 15 serwerów FTP.

Zwiększanie wydajności serwera FTP dzięki obsłudze konfigurowalnego podsystemu

Domyślny podsystem (QSYS/QSYSWRK) jest używany do wielu zadań serwerów firmy IBM. Korzystanie z podsystemu innego niż domyślny może wpłynąć korzystnie na wydajność protokołu FTP, ponieważ nie ma wtedy konieczności współużytkowania zasobów.

Aby skonfigurować podsystem dla serwera FTP, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. Kliknij prawym przyciskiem **FTP** i wybierz **Właściwości**.
3. Na stronie **Właściwości FTP** wybierz **Opis podsystemu**.
4. Określ opis podsystemu i predefiniowaną bibliotekę.

Jeśli podany podsystem nie istnieje, wtedy serwer FTP utworzy go razem z pozycjami tabeli routingu i opisami zadań. Podczas uruchamiania zadania uruchamiania dla serwera FTP zostaną określone parametry dla nowo utworzonego podsystemu, a następnie wprowadzone zostaną zadania serwera dla wsadowych zadań uruchamiania w podsystemie.

Korzystanie z klienta FTP na platformie System i

Jeśli w systemie jest uruchomiony klient FTP, można uruchamiać i zatrzymywać sesje klienta, przesyłać i odbierać pliki oraz konfigurować zadania wsadowe FTP.

Za pomocą klienta FTP można przesyłać pliki znajdujące się w systemie, w tym pliki znajdujące się w systemach plików Root, QSYS.Lib, QOpenSys, QOPT i QFileSvr.400. Możliwe jest również przesyłanie folderów i dokumentów znajdujących się w systemie plików usług biblioteki dokumentów (QDLS). Klienta FTP można uruchomić interaktywnie w nienadzorowanym trybie wsadowym, w którym komendy są czytane z pliku, a odpowiedzi na nie zapisywane do pliku. Zapewnia on także inne funkcje umożliwiające przetwarzanie plików w systemie, na którym działa.

Klient ma interfejs użytkownika, z którego można wprowadzać komendy klienta, umożliwiające wysyłanie żądań do serwera FTP. Wyniki tych żądań są następnie wyświetlane.

Do przesyłania plików między klientem i serwerem ustanawiane są dwa połączenia. Połączenie sterujące służy do wysyłania żądań do serwera za pomocą komend serwera FTP. Serwer wysyła do klienta odpowiedzi informujące o tym, jak żądania będą przetwarzane. Drugie połączenie, nazywane połączeniem danych, służy do przesyłania list plików i właściwych danych w plikach.

Zarówno klient, jak i serwer używają funkcji przesyłania danych, które komunikują się z lokalnymi systemami plików. Funkcje te czytają lub zapisują dane w lokalnych systemach plików oraz odbierają i wysyłają dane przez połączenie danych.

Uruchamianie i zatrzymywanie sesji klienta

Po uzyskaniu identyfikatora logowania i hasła do zdalnego serwera FTP można uruchomić sesję klienta z tym serwerem FTP. Sesję klienta można zakończyć przy użyciu podkomendy QUIT serwera FTP.

Ten temat zawiera szczegółowe informacje na temat korzystania z klienta FTP w systemie operacyjnym i5/OS.

"Uruchamianie sesji klienta FTP"
"Zatrzymywanie sesji klienta FTP" na stronie 31

Uruchamianie sesji klienta FTP

Przed uruchomieniem funkcji klienta FTP, należy zebrać następujące informacje:

- nazwę lub adres internetowy systemu, do którego pliki są wysyłane lub z którego są otrzymywane,
- identyfikator logowania oraz hasło (jeśli jest wymagane) dla zdalnego systemu, do lub z którego nastąpi przesyłanie plików,
- nazwa pliku lub plików, z którymi będzie się pracowało (na przykład wysyłało je lub otrzymywało).

Komenda Start TCP/IP File Transfer Protocol (STRTCPFTP *system_zdalny*) służy do uruchamiania sesji klienta w systemie lokalnym, a następnie otwierania połączenia z serwerem FTP w podanym systemie zdalnym. Na przykład wpisanie komendy FTP myserver.com spowoduje uruchomienie sesji klienta w systemie lokalnym, a następnie otwarcie połączenia z serwerem FTP w systemie zdalnym myserver.com. Wpisując komendę STRTCPFTP bez określenia systemu zdalnego, można podać dodatkowe parametry lub poczekać, aż zostanie wyświetlone zapytanie o te parametry.

```
                      Uruchomienie przesyłania plików TCP/IP (FTP)
                      (Start TCP/IP File Transfer (FTP))

Wpisz opcje i naciśnij klawisz Enter.

System zdalny  . . . . . . . . . > MYSERVER.COM



Identyfikator kodowanego zestawu znaków     *DFT          1-65533, *DFT
Port . . . . . . . . . . . . . . . >          *SECURE       1-65535, *DFT, *SECURE
Połączenie chronione . . . . . .            *DFT          *DFT, *NONE, *SSL, *IMPLICIT
Połączenie dla danych. . . . . .            *DFT          *DFT, *CLEAR, *PRIVATE
```

Po podaniu nazwy systemu zdalnego, system zapyta o dodatkowe informacje. Poniżej znajduje się podsumowanie dostępnych opcji; dodatkowe szczegóły są dostępne w pomocy dla tych pól:

Nazwa systemu zdalnego (RMTSYS)

Nazwa zdalnego systemu, do lub z którego mają być przesyłane pliki. Poniższe elementy stanowią możliwe wartości:

***INTNETADR**
System pyta o podanie parametru Adres internetowy (Internet address - INTNETADR). Adres internetowy ma postać nnn.nnn.nnn.nnn, gdzie nnn jest liczbą dziesiętną z zakresu od 0 do 255.

system_zdalny
Nazwa zdalnego systemu, do lub z którego mają być przesyłane pliki.

Identyfikator kodowanego zestawu znaków (CCSID)

Identyfikator kodowanego zestawu znaków ASCII, który jest używany do przesyłania plików ASCII SBCS (zestaw znaków jednobajtowych), kiedy ustawiony jest tryb FTP ASCII. Możliwymi wartościami są:

***DFT** Używana wartość identyfikatora CCSID to 00819 (ISO 8859-1 8-bitowy kod ASCII).

wartość_CCSID
Używana jest żądana wartość CCSID. Ta wartość jest zatwierdzana dla uzyskania pewności, że żądany identyfikator CCSID ASCII SBCS jest prawidłowy.

Port (PORT)

Numer portu używanego do łączenia się z serwerem FTP. Do łączenia z serwerem FTP używany jest zazwyczaj ogólnie znany port 21. W niektórych sytuacjach połączenie z serwerem FTP może jednak zostać nawiązane za pomocą portu innego niż 21. W takich sytuacjach parametr port może zostać użyty do podania portu serwera. Możliwymi wartościami są:

***DFT** Używana jest wartość 00021.

***SECURE**
Używana jest wartość 00990. Port 990 jest zarezerwowany dla serwerów FTP, które korzystają bezpośrednio z protokołów TLS lub SSL (do szyfrowania danych).

wartość_portu
Używana jest żądana wartość portu. Ta wartość jest zatwierdzana dla uzyskania pewności, że pochodzi z właściwego zakresu.

Uwaga: Jeśli podany został port 990, klient FTP wykonuje te same funkcje, jak w przypadku określenia opcji *SECURE.

Ochrona połączenia (Secure connection - SECCNN)

Określa typ mechanizmu ochrony, który ma być używany do zabezpieczenia informacji przesyłanych połączeniem sterującym FTP (w tym hasło używane do uwierzytelniania sesji z serwerem FTP). Protokoły TLS i SSL są kompatybilnymi protokołami, używającymi szyfrowania do ochrony danych przed przeglądaniem podczas przesyłania i weryfikującymi, czy nie nastąpiła utrata lub zniekształcenie danych.

Uwaga: Podkomenda klienta FTP SECOPEN może być wykorzystana w celu nawiązania chronionego połączenia FTP podczas sesji klienta FTP.

Możliwymi wartościami są:

***DFT** Jeśli w parametrze PORT podano *SECURE lub 990, używana jest opcja *IMPLICIT; w przeciwnym razie *NONE.

***IMPLICIT**
Klient FTP już podczas łączenia z określonym serwerem FTP rozpoczyna korzystanie z warstwy TLS/SSL (bez wysyłania do serwera komendy AUTH). Jeśli serwer FTP nie obsługuje niejawnego protokołu TLS/SSL na określonym porcie lub negocjacja TLS/SSL nie powiodła się z jakiegokolwiek powodu, połączenie zostanie zamknięte.

***SSL** Po połączeniu z określonym serwerem FTP klient FTP wysyła podkomendę AUTH (Autoryzacja - Authorization), która żąda sesji zabezpieczonej protokołem TLS/SSL. Jeśli serwer FTP obsługuje protokół TLS lub SSL, odbędzie się negocjacja TLS lub SSL. Jeśli serwer FTP nie obsługuje protokołu TLS/SSL lub negocjacja nie powiodła się, połączenie zostanie zamknięte.

***NONE**
Klient FTP nie korzysta z szyfrowania dla połączenia sterującego z określonym serwerem FTP.

Ochrona danych (Data protection - DTAPROT)

Określa rodzaj zabezpieczenia danych, który ma być wykorzystywany dla informacji przesyłanych połączeniem dla danych. To połączenie jest używane do przesyłania plików z danymi i listingów katalogów. Protokół FTP nie zezwala na zabezpieczenie połączenia dla danych, jeśli nie jest chronione połączenie sterujące.

Uwaga: Komenda klienta FTP SECData może być później wykorzystana do zmiany poziomu ochrony danych. Klient FTP używa komendy serwera FTP PROT, aby zażądać określonej ochrony danych po nawiązaniu chronionego połączenia sterującego.

Możliwymi wartościami są:

***DFT** Jeśli parametr SECCNN określa chronione połączenie sterujące, używany jest parametr *PRIVATE; w pozostałych przypadkach jest używany parametr *CLEAR.

***PRIVATE**
Informacje wysyłane przez połączenie FTP dla danych są szyfrowane. Jeśli parametr SECCNN określa, że połączenie sterujące nie jest szyfrowane, nie można użyć parametru *PRIVATE.

***CLEAR**
Informacje wysyłane przez połączenie FTP dla danych nie są szyfrowane.

Tabela wychodzących danych ASCII/EBCDIC (TBLFTPOUT)

Określa obiekt tabeli, który jest używany do odwzorowywania wszystkich danych wychodzących klienta FTP. Dane wychodzące są odwzorowywane z EBCDIC na ASCII. Jeśli dla parametru TBLFTPOUT nie określono żadnej tabeli, do określenia odwzorowania wychodzącego, używany jest parametr CCSID. Możliwymi wartościami są:

***CCSID**
Parametr CCSID używany jest do określania odwzorowania danych wychodzących.

***DFT** Parametr CCSID używany jest do określania odwzorowania danych wychodzących.

Nazwa odwzorowania wychodzącego może być kwalifikowana za pomocą jednej z poniższych wartości biblioteki:

***LIBL** Przeszukiwane są wszystkie biblioteki w częściach dotyczących listy biblioteki zadania użytkownika i systemu, dopóki nie zostanie znalezione pierwsze odwzorowanie o takiej nazwie.

***CURLIB**
Przeszukiwana jest bieżąca biblioteka zadania. Jeśli jako bieżąca biblioteka zadania nie została podana żadna biblioteka, używana jest biblioteka QGPL.

nazwa_biblioteki
Nazwa biblioteki do przeszukania.

tabela_odwzorowania_wychodzącego
Obiekt tabeli, który ma być użyty przez klienta FTP w celu odwzorowania danych wychodzących.

Tabela przychodzących danych ASCII/EBCDIC (TBLFTPIN)

Obiekt tabeli, który jest używany do odwzorowywania wszystkich danych przychodzących klienta FTP. Dane przychodzące są odwzorowywane z ASCII na EBCDIC. Jeśli w parametrze TBLFTPIN nie podano żadnej tabeli, do określenia odwzorowania przychodzącego używany jest parametr CCSID. Poniższe elementy stanowią możliwe wartości:

***CCSID**
Parametr CCSID używany jest do określania odwzorowania danych przychodzących.

***DFT** Parametr CCSID używany jest do określania odwzorowania danych przychodzących.

Nazwa odwzorowania przychodzącego może być kwalifikowana za pomocą jednej z poniższych wartości biblioteki:

***LIBL** Przeszukiwane są wszystkie biblioteki w częściach dotyczących listy biblioteki zadania użytkownika i systemu, dopóki nie zostanie znalezione pierwsze odwzorowanie o takiej nazwie.

***CURLIB**
Przeszukiwana jest bieżąca biblioteka zadania. Jeśli jako bieżąca biblioteka zadania nie została podana żadna biblioteka, używana jest biblioteka QGPL.

nazwa_biblioteki
Nazwa biblioteki do przeszukania.

tabela_odwzorowania_przychodzącego
Obiekt tabeli, który ma być użyty przez klienta FTP w celu odwzorowania danych przychodzących.

Zatrzymywanie sesji klienta FTP

Użyj podkomendy QUIT, aby zakończyć sesję FTP.

Zamyka ona połączenie ze zdalnym hostem i kończy sesję FTP w systemie. W tym celu można także nacisnąć klawisz F3 (Wyjście), a następnie potwierdzić zakończenie sesji FTP.

Pojęcia pokrewne

"Zabezpieczanie klientów FTP za pomocą protokołu TLS lub SSL" na stronie 22
Dane przesyłane za pomocą połączeń sterujących i połączeń danych protokołu FTP można szyfrować, korzystając z połączeń TLS lub SSL.

Zadania pokrewne

"Przesyłanie plików za pomocą protokołu FTP"
Protokół FTP umożliwia wysyłanie i odbieranie plików.

Odsyłacze pokrewne

"Scenariusz: przesyłanie pliku ze zdalnego hosta" na stronie 1
Ten scenariusz opisuje, jak za pomocą podstawowych funkcji protokołu FTP pobrać pliki ze zdalnego hosta. W tym scenariuszu klient i serwer są systemami używającymi protokołu FTP i5/OS.

Uwagi na temat przekroczenia limitu czasu przez serwer

Wartość limitu czasu nieaktywności to liczony w sekundach czas braku aktywności serwera FTP, po którym zamyka on sesję. Połączenie FTP można podtrzymywać, aby nie zostało zamknięte wskutek przekroczenia tego limitu czasu.

Niektóre systemy zdalne pozwalają klientom na zmianę tej wartości. Na przykład platforma System i obsługuje podkomendę TIME serwera FTP, którą można wysłać do serwera za pomocą podkomendy QUOTE klienta FTP. Serwery systemu UNIX często obsługują podkomendę SITE IDLE.

Podczas stosowania lokalnych podkomend FTP i5/OS w połączeniu z podkomendą SYSCMD lub naciskaniem klawisza F21 nie występuje żadna interakcja między klientem a serwerem FTP. Jeśli zatem wykonywanie tych lokalnych komend FTP przekracza limit czasu nieaktywności serwera, połączenie zostanie zamknięte przez serwer. Jeśli połączenie zostanie utracone, należy ponownie zalogować się do serwera FTP za pomocą komendy OPEN (OPEN <*nazwa systemu zdalnego*>) i komendy USER.

Odsyłacze pokrewne

"QUOTE (Wysłanie komendy do serwera FTP - Send a Subcommand to an FTP Server)" na stronie 83
Podkomenda QUOTE klienta FTP i5/OS służy do wysyłania podkomendy do serwera FTP.

Przesyłanie plików za pomocą protokołu FTP

Protokół FTP umożliwia wysyłanie i odbieranie plików.

Aby przesłać pliki za pomocą protokołu FTP i5/OS, wykonaj następujące czynności:

1. Należy przygotować następujące informacje:
   - nazwę TCP/IP lub adres IP zdalnego komputera,
   - nazwę i hasło użytkownika zdalnego komputera (jeśli komputer zdalny nie obsługuje anonimowego FTP),
   - nazwę i miejsce położenia pliku, który ma zostać przesłany,

- docelowe położenie pliku,
- format przesyłanego pliku: ASCII, EBCDIC lub BINARY,
- czy połączenie ma być chronione za pomocą ochrony TLS (Transport Layer Security), czy SSL (Secure Sockets Layer).

2. W wierszu komend wpisz FTP i naciśnij klawisz Enter.
3. Następnie wprowadź nazwę TCP/IP lub adres IP zdalnego komputera i naciśnij klawisz Enter. Możesz użyć nazwy lub adresu IP, takich jak:

   zdalna.nazwa_systemu.com
   lub
   110.25.9.13
4. Wpisz identyfikator CCSID (Coded Character Set Identifier). Użyj wartości domyślnej (*DFT), chyba że wiesz, jaki konkretny identyfikator CCSID jest potrzebny.
5. Jeśli chcesz użyć bezpiecznego połączenia w celu zabezpieczenia haseł i danych, podaj wartość *SECURE jako wartość portu.
6. Naciśnij klawisz Enter, aby nawiązać połączenie. Klient FTP wyświetli komunikaty, które powiadomią o pomyślnym nawiązaniu połączenia z systemem zdalnym.

   Uwaga: Jeśli jako port określono wartość *SECURE, a serwer FTP nie obsługuje niejawnego protokołu TLS/SSL na określonym porcie lub negocjacja TLS/SSL nie powiodła się z jakiegokolwiek powodu, połączenie zostanie zamknięte.
7. Aby zmienić typ przesyłanego pliku, wykonaj następujące czynności:
   a. Aby zmienić typ na EBCDIC, wpisz EBCDIC i naciśnij klawisz Enter przed wysłaniem pliku.
   b. Aby zmienić typ na BINARY, wpisz BINARY i naciśnij klawisz Enter przed wysłaniem pliku.
   c. Aby powrócić do domyślnego typu ASCII, wpisz ASCII i naciśnij klawisz Enter przed wysłaniem pliku.
8. Od tego momentu można już przesyłać pliki:
   a. Wpisz CD i nazwę katalogu. Naciśnij klawisz Enter.
   b. Wykonaj jedną z poniższych czynności:
      - Aby przesłać plik z systemu serwera do systemu klienta, wprowadź komendę GET wraz z nazwą pliku:
        ```
        GET mojplik.txt
        ```
      - Aby przesłać plik znajdujący się na systemie klienta do systemu serwera, wprowadź komendę PUT wraz z nazwą pliku:
        ```
        PUT mojplik.txt
        ```
9. Wprowadź podkomendę FTP QUIT, aby zakończyć sesję klienta FTP i powrócić do wiersza komend.

Pojęcia pokrewne

“Metody przesyłania danych” na stronie 133
Przed rozpoczęciem przesyłania plików należy wybrać właściwy format ich przesyłania. Można użyć domyślnego formatu ASCII lub podać inny format, na przykład EBDCIC lub BINARY.

Odsyłacze pokrewne

“Scenariusz: przesyłanie pliku ze zdalnego hosta” na stronie 1
Ten scenariusz opisuje, jak za pomocą podstawowych funkcji protokołu FTP pobrać pliki ze zdalnego hosta. W tym scenariuszu klient i serwer są systemami używającymi protokołu FTP i5/OS.

“Uruchamianie i zatrzymywanie sesji klienta” na stronie 28
Po uzyskaniu identyfikatora logowania i hasła do zdalnego serwera FTP można uruchomić sesję klienta z tym serwerem FTP. Sesję klienta można zakończyć przy użyciu podkomendy QUIT serwera FTP.

Korzystanie z protokołu FTP w trybie nienadzorowanym za pomocą zadania wsadowego

Klient FTP może być uruchamiany interaktywnie lub w trybie nienadzorowanym. Ten temat zawiera jeden prosty i jeden zaawansowany przykład użycia metody zadania wsadowego protokołu FTP.

Pojęcia pokrewne

"Kontrolowanie dostępu do serwera FTP" na stronie 17
Jeśli protokół FTP jest używany, istnieje potrzeba zachowania kontroli nad użytkownikami w celu ochrony danych i sieci. Sekcja ta zawiera wskazówki i uwagi dotyczące ochrony.

Odsyłacze pokrewne

"Scenariusz: przesyłanie pliku ze zdalnego hosta" na stronie 1
Ten scenariusz opisuje, jak za pomocą podstawowych funkcji protokołu FTP pobrać pliki ze zdalnego hosta. W tym scenariuszu klient i serwer są systemami używającymi protokołu FTP i5/OS.

Informacje pokrewne

V4 TCP/IP for AS/400: More Cool Things Than Ever

Przykład prosty: zadania wsadowe FTP

Ten prosty przykład demonstruje przesyłanie danych za pomocą pliku wsadowego. W przykładzie opisano przesłanie jednego pliku z systemu zdalnego.

Komponenty:

- program w języku CL,
- plik wejściowy zawierający komendy FTP,
- plik wyjściowy zawierający komunikaty FTP.

Program w języku CL

```
************************************************************
   ITSOLIB1/QCLSRC BATCHFTP:
   ---------------------
       PGM
       OVRDBF   FILE(INPUT) TOFILE(ITSOLIB1/QCLSRC) MBR(FTPCMDS)
       OVRDBF   FILE(OUTPUT) TOFILE(ITSOLIB1/QCLSRC) MBR(OUT)
       FTP      RMTSYS(SYSxxx)
       ENDPGM
************************************************************
```

Uwaga: Jeśli powyższy przykładowy program jest pisany w środowisku ILECL, to aby działał, do komendy OVRDBF należy dodać parametr OVRSCOPE(*CALLLVL).

Program BATCHFTP przepisuje parametr INPUT do źródłowego zbioru fizycznego ITSOLIB1/QCLSRC MBR(FTPCMDS). Dane wyjściowe są przesyłane do MBR(OUT).

Plik wejściowy zawierający komendy FTP

```
************************************************************
ITSOLIB1/QCLSRC FTPCMDS:
---------------------
ITSO ITSO
CD ITSOLIB1
SYSCMD CHGCURLIB ITSOLIB2
GET QCLSRC.BATCHFTP QCLSRC.BATCHFTP (REPLACE
QUIT
************************************************************
```

Wymagania dotyczące komend FTP znajdują się w pliku FTPCMDS.

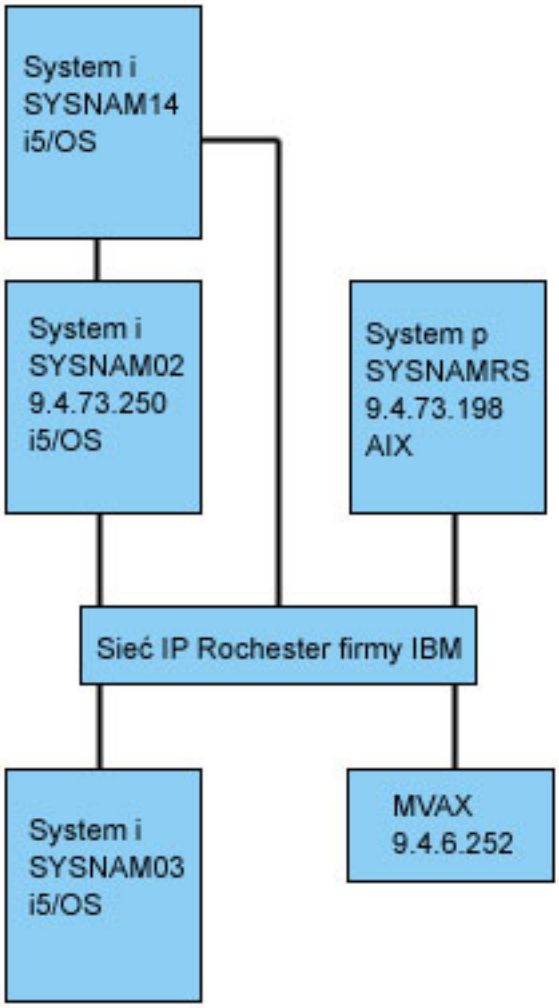
Plik wyjściowy zawierający komunikaty FTP

```
     ************************************************************
     FTP Output Redirected to a File
     FTP Input from Overridden File
     Connecting to host name SYSxxx
     at address x.xxx.xx.xxx using port 21.
     220-QTCP at SYSxxx.sysnam123.ibm.com.
     220 Connection will close if idle more than 5 minutes.
     Enter login ID (itso):
     > ITSO ITSO
     331 Enter password.
     230 ITSO logged on.
      Zdalnym systemem operacyjnym jest system i5/OS.  Wersja protokołu
TCP/IP: "V3R1M0".
     250  Używany obecnie format nazewnictwa: "0".
     257 Biblioteka bieżąca: "QGPL".
     Enter an FTP subcommand.
     > CD ITSOLIB1
     Enter an FTP subcommand.
     250 Current library changed to ITSOLIB1.
     > SYSCMD CHGCURLIB ITSOLIB2
     Enter an FTP subcommand.
     > GET QCLSRC.BATCHFTP QCLSRC.BATCHFTP (REPLACE
     200 PORT subcommand request successful.
     150 Retrieving member BATCHFTP in file QCLSRC in library ITSOLIB1.
     250 File transfer completed successfully.
     147 bytes transferred in 0.487 seconds. Transfer rate 0.302 KB/sec.
     Enter an FTP subcommand.
     > QUIT
     221 QUIT subcommand received.
     ************************************************************
```

Powyżej pokazany został wyjściowy plik komunikatów. Napisanie programu przetwarzającego ten plik i wyświetlającego komunikat o błędzie w QSYSOPR, jeśli pojawiły się jakieś komunikaty o błędach, nie powinno być problemem. Komunikaty FTP o błędach mają numery zaczynające się od cyfry 4 lub 5.

Przykład zaawansowany: zadania wsadowe FTP

W tym przykładzie pokazano sposób pobierania plików z kilku hostów zdalnych do systemu centralnego w trybie wsadowym.



Użytkownik GWIL systemu SYSNAM03 chce wykonać następujące czynności:

1. Pobrać pliki z hostów SYSNAMRS (RS/6000) i MVAX (VAX).
2. Po pobraniu pliku z hosta SYSNAMRS przesłać plik do systemu SYSNAM02 (kolejnego systemu) za pomocą protokołu FTP.
3. Z systemu SYSNAM02 wysłać plik do systemu SYSNAM14 za pomocą protokołu TCP/IP.

Przykład: tworzenie programu CL uruchamiającego usługę FTP:

To jest przykładowy program CL, który uruchamia usługę FTP w trybie wsadowym. Ten program CL zawiera komendy nadpisujące wejście komendy oraz wyjście komunikatu, uruchamiające usługę FTP i usuwające nadpisania po zamknięciu połączenia FTP.

1. Jak widać w prostym przykładzie, klient FTP używa terminalu do WEJŚCIA komendy i WYJŚCIA komunikatu, co musi zostać nadpisane w celu pracy w trybie wsadowym. W tym przykładzie pliki te są zastępowane nowymi, które będą używane w zadaniu wsadowym, za pomocą komendy OVRDBF:

   ```
   OVRDBF FILE(INPUT) TOFILE(GERRYLIB/QCLSRC) MBR(FTPCMDS)
   OVRDBF FILE(OUTPUT) TOFILE(GERRYLIB/QCLSRC) MBR(FTPLOG)
   ```

2. Komenda STRTCPFTP zawarta w pliku programu CL wymaga podania jako parametru nazwy hosta lub adresu internetowego. Jeśli jednak system zdalny ma zostać określony w wejściowym pliku komend, a nie w pliku programu CL, w komendzie STRTCPFTP musi zostać podana fikcyjna nazwa hosta w celu zachowania wymaganej składni komendy. Nazwa fikcyjna może być nazwą wyimaginowanego lub istniejącego hosta. Jeśli podana zostanie nazwa rzeczywistego hosta, jako pierwszą pozycję wejściowego pliku komend należy podać identyfikator

użytkownika i hasło, a jako drugą pozycję - komendę CLOSE. Jeśli podana zostanie nazwa wyimaginowanego hosta, powyższe pozycje nie są wymagane, a pierwszą pozycją musi być podkomenda OPEN, aby nawiązane zostało połączenie z wymaganym serwerem FTP.

```
FTP RMTSYS(LOOPBACK)
```

Klient FTP przetwarza plik wejściowy i zapisuje komunikaty do pliku wyjściowego (FTPLOG).

3. Po zakończeniu aplikacji FTP należy usunąć nadpisania:

```
DLTOVR     FILE(INPUT OUTPUT)
```

W systemie SYSNAM01 program CL dla klienta FTP w trybie wsadowym może wyglądać jak program przedstawiony w poniższym przykładzie na ilustracji nr 1:

Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki zapisane w sekcji “Licencja na kod oraz Informacje dotyczące kodu” na stronie 159.

```
 Kolumny . . . :    1  71           Przeglądaj                      GERRYLIB/QCLSRC
 SEU==>                                                                FTPBATCH
 FMT **  ...+... 1 ...+... 2 ...+... 3 ...+... 4 ...+... 5 ...+... 6 ...+... 7
        *************** Początek danych  ************************************
0001.00 PGM
0002.00              OVRDBF     FILE(INPUT) TOFILE(GERRYLIB/QCLSRC) +
0003.00                           MBR(FTPCMDS)
0004.00              OVRDBF     FILE(OUTPUT) TOFILE(GERRYLIB/QCLSRC) +
0005.00                           MBR(FTPLOG)
0006.00              FTP        RMTSYS(LOOPBACK) /* (FTP CL Program) */
0007.00              DLTOVR     FILE(INPUT OUTPUT)
0008.00 ENDPGM
        ****************** Koniec danych ***************************************


 F3=Wyjście   F5=Odśwież   F9=Poprzednie komendy   F10=Kursor   F12=Anuluj
 F16=Powtórz szukanie        F24=Inne klawisze
                                      (C) COPYRIGHT IBM CORP. 1981, 1994.
```

Rysunek 1. Program FTPBATCH w języku CL dla klienta FTP w trybie wsadowym

Przykład: tworzenie pliku wejściowego FTP (FTCPDMS):

Plik wejściowy FTP musi zawierać wszystkie podkomendy klienta FTP niezbędne do połączenia się z serwerem FTP, zalogowania się do niego, skonfigurowania i wykonania przesyłania plików, zamknięcia połączenia z serwerem oraz zakończenia sesji klienta. W tym przykładzie pokazane są podkomendy służące do przesyłania plików do dwóch różnych systemów zdalnych.

Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki zapisane w sekcji “Licencja na kod oraz Informacje dotyczące kodu” na stronie 159.

```
 Kolumny . . . :    1  71          Przeglądaj                     GERRYLIB/QCLSRC
 SEU==>                                                           FTPCMDS
 FMT **  ...+... 1 ...+... 2 ...+... 3 ...+... 4 ...+... 5...+... 6 ...+... 7
        *************** Początek danych  ************************************
0001.00 gwil ****
0002.00 close
0003.00 open sysnamrs
0004.00 user root root
0005.00 ascii
0006.00 syscmd dltf file(gerrylib/rs6)
0007.00 get /Itsotest gerrylib/rs6.rs6
0008.00 close
0009.00 open mvax
0010.00 user tester tester
0011.00 get screen1.file gerrylib/vax.vax (replace
0012.00 close
0013.00 open sysnam02
0014.00 user gwil ****
0015.00 ebcdic
0016.00 put gerrylib/rs6.rs6 gerrylib/rs6.rs6
0017.00 quote rcmd sndnetf file(gerrylib/rs6) tousrid((gwilsysnam14))
0018.00 close
0019.00 quit
        ****************** Koniec danych ***************************************
 F3=Wyjście   F5=Odśwież   F9=Poprzednie komendy   F10=Kursor   F12=Anuluj
 F16=Powtórz szukanie        F24=Inne klawisze
```

Rysunek 2. Przesyłanie plików do dwóch systemów zdalnych

Poniższe objaśnienia pomogą zrozumieć podkomendy klienta FTP przedstawione na Rys. 2. Numery wierszy na ekranie odpowiadają numerom w poniższym zestawieniu.

0001 Identyfikator użytkownika i hasło dla fikcyjnego połączenia z systemem klienta SYSNAM03.

0002 Zamknięcie fikcyjnego połączenia w systemie SYSNAM03.

0003 Otworzenie połączenia sterującego do hosta RISC System/6000 SYSNAMRS.

0004 Komenda USER z identyfikatorem użytkownika i hasłem dla hosta SYSNAMRS.

Uwaga: Podczas uruchamiania klienta FTP w trybie wsadowym, po komendzie OPEN musi nastąpić komenda USER. Komenda USER powinna mieć następujące parametry: identyfikator użytkownika do zalogowania się oraz hasło. Inaczej jest, gdy FTP działa interaktywnie. Gdy usługa FTP zostanie uruchomiona interaktywnie, klient automatycznie uruchomi podkomendę USER i podpowie identyfikator do zalogowania się. Jeśli usługa FTP została uruchomiona w trybie wsadowym, komenda USER nie jest uruchamiana automatycznie.

0005 Przesłanie danych ASCII (w systemie zostanie dokonana ich konwersja do/z kodu EBCDIC).

0006 Komenda CL uruchamiana w systemie klienta w celu usunięcia pliku (zamiast niej można użyć parametru REPLACE w następnej instrukcji get).

0007 Pobranie pliku z systemu RISC System/6000.

0008 Zamknięcie połączenia sterującego do hosta RISC System/6000 SYSNAMRS.

0009 Otwarcie połączenia do hosta VAX MVAX.

0010 Komenda USER z identyfikatorem użytkownika i hasłem dla hosta MVAX.

0011 Pobranie pliku z hosta VAX i zastąpienie istniejącego pliku systemu i5/OS.

0012 Zamknięcie połączenia sterującego z hostem VAX MVAX.

0013 Otwarcie połączenia sterującego z systemem zdalnym SYSNAM02.

0014 Komenda USER z identyfikatorem użytkownika i hasłem dla hosta SYSNAM02.

0015 Przesłanie danych EBCDIC (na takiej samej zasadzie, jak z platformy System i na platformę System i).

0016 Wysłanie plików systemu i5/OS do systemu SYSNAM02 za pomocą protokołu TCP/IP.

0017 Wysłanie tego pliku z systemu SYSNAM03 do zdalnego systemu SYSNAM14 przez sieć TCP/IP.

0018 Zamknięcie połączenia sterującego z systemem SYSNAM02.

0019 Zakończenie aplikacji FTP.

Przykład: program CL do wprowadzania zadania FTPBATCH:

Utworzenie programu CL wprowadzającego zadanie FTPBATCH pozwala na ustalenie harmonogramu przesyłania plików oraz uruchamianie przesyłania w trybie nienadzorowanym. W tym przykładzie przesyłanie plików ma zostać uruchomione w następny piątek o godzinie 17:00 w trybie nienadzorowanym.

Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki zapisane w sekcji “Licencja na kod oraz Informacje dotyczące kodu” na stronie 159.

```
Kolumny . . . :    1  71           Przeglądaj                      GERRYLIB/QCLSRC
SEU==>                                                              FTPSUBMIT
FMT **  ...+... 1 ...+... 2 ...+... 3 ...+... 4 ...+... 5...+... 6 ...+... 7
       *************** Początek danych  ************************************
0001.00 PGM
0002.00              SBMJOB     CMD(CALLPGM(GERRYLIB/FTPBATCH)) +
0003.00                           JOB(FTPFRIDAY)OUTQ(QUSRSYS/GERRYQ)    +
0004.00                           SCDDATE(*FRI)SCDTIME(170000) /* FTP for +
0005.00                           Friday, 5:00 in theafternoon */
0006.00 ENDPGM
       ****************** Koniec danych ***************************************

F3=Wyjście   F5=Odśwież   F9=Poprzednie komendy   F10=Kursor   F12=Anuluj
F16=Powtórz szukanie        F24=Inne klawisze
                                    (C) COPYRIGHT IBMCORP. 1981, 1994.
```

Rysunek 3. Program w języku CL wprowadzający zadanie dla klienta FTP w trybie wsadowym

Przykład: sprawdzanie, czy plik wyjściowy FTP nie zawiera błędów:

Po każdym uruchomieniu o zaplanowanej godzinie klient FTP tworzy dane w podzbiorze zbioru FTPLOG. Dane w podzbiorze zbioru FTPLOG odpowiadają rzeczywistym instrukcjom występującym w obu przykładach. Należy przejrzeć te dane wyjściowe (FTPLOG), aby sprawdzić, czy podczas przetwarzania FTP nie pojawiły się błędy.

Przykładowy plik wyjściowy jest następujący:

Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki zapisane w sekcji “Licencja na kod oraz Informacje dotyczące kodu” na stronie 159.

```
       Łączenie z hostem LOOPBACK pod adresem 127.0.0.1 za pomocą portu 21.
220-QTCP w hoście lokalnym.
220 Połączenie zostanie zamknięte po 5 minutach pracy jałowej.
Wpisz ID użytkownika (gwil):

>>>GWIL ****
331 Enter password.
230 Zarejestrowanie się jako GWIL.
Zdalnym systemem operacyjnym jest system i5/OS.  Wersja prot. TCP/IP: "V4R2M0".
250  Używany obecnie format nazewnictwa: "0".
257 Biblioteka bieżąca: "QGPL".
Enter an FTP subcommand.

> CLOSE
221 QUIT subcommand received.
Enter an FTP subcommand.

> OPEN SYSNAMRS
Łączenie z hostem SYSNAMRS pod adresem 9.4.73.198 za pomocą portu 21.
220 Serwer FTP sysnamrs.sysnam123.ibm.com (wersja 4.9 czw 2 wrz 20:35:07 CDT
    1993) jest gotowy.
Enter an FTP subcommand.
```

Rysunek 4. Dane wyjściowe klienta FTP (FTPLOG) po uruchomieniu programu FTPBATCH (część 1/5)

```
> USER root ****
331 Wymagane hasło dla użytkownika root.
230 Zarejestrowanie się jako użytkownik root.
UNIX Typ: L8 Wersja: BSD-44
Enter an FTP subcommand.

> ASCII
200 Typ ustawiony na A; formularz ustawiony na N.
Enter an FTP subcommand.

> SYSCMD DLTF FILE(GERRYLIB/RS6)
Enter an FTP subcommand.

> GET /Itsotest GERRYLIB/RS6/RS7
200 Komenda PORT powiodła się.
150 Otwieranie połączenia danych dla /Itsotest (467 bajtów).
226 Przesyłanie zakończone.
Wysłano 467 bajtów przez 2,845 s. Szybkość przesyłania 0,167kB/s.
Enter an FTP subcommand.
```

Rysunek 5. Dane wyjściowe klienta FTP (FTPLOG) po uruchomieniu programu FTPBATCH (część 2/5)

```
> CLOSE
221 Goodbye.
Enter an FTP subcommand.

> OPEN MVAX
Łączenie z hostem mvax pod adresem 9.4.6.252 za pomocą portu 21.
220 Usługa FTP gotowa
Enter an FTP subcommand.

> USER TESTER ******
331 Otrzymano nazwę użytkownika TESTER, proszę podać hasło
230 Użytkownik TESTER zalogowany, katalog $DISK1:[TESTER]
Enter an FTP subcommand.

GET SCREEN1.FILE GERRYLIB/VAX.VAX (REPLACE
200 Komenda PORT powiodła się.
125 Rozpoczęto przesyłanie ASCII dla $DISK1:[TESTERSCREEN1.FILE;1(266586 bajtów)
226 Przesyłanie plików zakończone powodzeniem.
Przesłano 265037 bajtów w ciągu 8,635 s. Szybkość przesyłania 30,694 kB/s.
Enter an FTP subcommand.

> CLOSE
221 Goodbye.
Enter an FTP subcommand.

OPEN SYSNAM02
Łączenie z hostem SYSNAM02 pod adresem 9.4.73.250 za pomocą portu 21.
220-QTCP w SYSNAM02.sysnam123.ibm.com.
220 Connection will close if idle more than 5 minutes.
       Enter an FTP subcommand.
```

Rysunek 6. Dane wyjściowe klienta FTP (FTPLOG) po uruchomieniu programu FTPBATCH (część 3/5)

```
> USER GWIL ****
331 Enter password.
230 Zarejestrowanie się jako GWIL.
 Zdalnym systemem operacyjnym jest system i5/OS.  Wersja protokołu TCP/IP: "V4R2M0".
250  Używany obecnie format nazewnictwa: "0".
257 Biblioteka bieżąca: "QGPL".
Enter an FTP subcommand.

> EBCDIC
200 Typ reprezentacji to niedrukowalny EBCDIC.
Enter an FTP subcommand.

> PUT GERRYLIB/RS6.RS6 GERRYLIB/RS6.RS6
200 PORT subcommand request successful.
150 Wysyłanie zbioru do podzbioru RS6 w zbiorze RS6 w bibliotece GERRYLIB.
250 File transfer completed successfully.
Wysłano 467 bajtów przez 0,148 s. Szybkość przesyłania 3,146 kB/s.
Enter an FTP subcommand.

> RCMD SNDNETF FILE(GERRYLIB/RS6) TOUSRID((GERRYLIB SYSNAM14))
250 Command SNDNETF FILE(GERRYLIB/RS6) TOUSRID((GWIL SYSNAM14))
    successful.
Enter an FTP subcommand.
```

Rysunek 7. Dane wyjściowe klienta FTP (FTPLOG) po uruchomieniu programu FTPBATCH (część 4/5)

```
> CLOSE
221 QUIT subcommand received.
Enter an FTP subcommand.
> QUIT
(To kończy działanie aplikacji FTP)
```

Rysunek 8. Dane wyjściowe klienta FTP (FTPLOG) po uruchomieniu programu FTPBATCH (część 5/5)

Można to zrobić, przeglądając dane lub uruchomić program testujący pojawienie się kodów błędu odpowiedzi. Trzycyfrowe kody błędów FTP zaczynają się od cyfr 4 lub 5. Należy unikać komunikatów takich jak 'Przesłano 467 bajty...'.

Przykładowa procedura: przykładowa procedura REXX i przykładowy podzbiór zbioru fizycznego są dostarczane jako część produktu TCP/IP. Zbiór QATMPINC w bibliotece QTCP zawiera następujące dwa podzbiory:

- BATCHFTP, który zawiera kod źródłowy REXX określający wejścia i wyjścia plików wsadowych oraz uruchamiający FTP.
- BFTPFILE, który zawiera komendy oraz dane niezbędne do zalogowania się i uruchomienia FTP.

Informacje dotyczące protokołu FTP

Informacje uzupełniające dotyczące protokołu FTP zawierają informacje o podkomendach klienta i serwera FTP i5/OS, programach obsługi wyjścia FTP oraz metodzie przesyłania danych.

Podkomendy serwera FTP

Poniższe podkomendy przedstawiają komunikację pomiędzy klientem FTP a serwerem FTP. W tym temacie opisano podkomendy odpowiadające komendom CL w systemie i5/OS, które są unikalne dla serwera FTP i5/OS.

Klienci FTP komunikują się z serwerem za pomocą komend serwera. W tym rozdziale przedstawiono poszczególne komendy serwera, opisy ich działania, konwencje składni i komunikaty statusu odpowiedzi FTP.

Serwer FTP i5/OS używa podkomend wymienionych w poniższej tabeli.

Podkomenda	**Do czego służy**
ABOR	Anuluje poprzednią podkomendę
ADDM	Dodaje podzbiór do zbioru fizycznego
ADDV	Dodaje podzbiór o zmiennej długości do zbioru fizycznego
APPE	Dopisuje dane do podanego zbioru
AUTH	Definiuje mechanizm uwierzytelniania używany dla bieżącej sesji FTP
"CCC (Kanał komendy usuwania zawartości - Clear Command Channel)" na stronie 45	Zmienia tryb transmisji danych przez połączenie sterujące z trybu zaszyfrowanego na tryb jawnego tekstu
CDUP	Zmienia katalog na katalog nadrzędny
CRTL	Tworzy bibliotekę
CRTP	Tworzy zbiór fizyczny
CRTS	Tworzy źródłowy zbiór fizyczny
CWD	Zmienia katalog roboczy lub bibliotekę
DBUG	Uruchamia lub zatrzymuje śledzenie serwera
DELE	Usuwa plik, podzbiór lub dokument
DLTF	Usuwa zbiór
DLTL	Usuwa bibliotekę

Podkomenda	Do czego służy
HELP	Pobiera informacje o podkomendach serwera FTP
LIST	Wyświetla listę pozycji katalogu i plików
MKD	Tworzy katalog
MODE	Określa format transmisji danych
NLST	Wyświetla listę nazw plików lub katalogów
NOOP	Sprawdza, czy serwer odpowiada
PASS	Wysyła hasło do serwera
PASV	Nakazuje serwerowi pasywne otwarcie kolejnego połączenia danych
PBSZ	Definiuje maksymalną wielkość buforu dla danych zakodowanych na poziomie aplikacji, które są wysyłane lub odbierane przez połączenie danych
PORT	Określa port danych, na którym klient będzie nasłuchiwał połączenia
PROT	Określa ochronę używaną dla połączeń danych w protokole FTP
PWD	Wyświetla bieżący katalog roboczy
QUIT	Wylogowuje użytkownika; zamyka połączenie
RCMD	Wysyła komendę CL do serwera FTP
REIN	Ponownie uruchamia sesję na serwerze
RETR	Wczytuje dane z serwera
RMD	Usuwa katalog
RNFR	Określa plik, który ma mieć zmienioną nazwę
RNTO	Określa nową nazwę pliku
SITE	Wysyła informacje, które mogą być użyte przez serwer
STAT	Pobiera z serwera informacje o statusie
STOR	Składuje dane na serwerze i zastępuje istniejący plik
STOU	Składuje dane na serwerze, ale nie zastępuje istniejącego pliku
STRU	Określa strukturę pliku
SYST	Wyświetla nazwę systemu operacyjnego serwera
TIME	Określa wartość limitu czasu dla serwera FTP
TYPE	Określa typ przesyłania plików
USER	Wysyła identyfikator logowania użytkownika do serwera
XCUP	Przechodzi do katalogu nadrzędnego
XCWD	Przechodzi do katalogu roboczego
XMKD	Tworzy katalog
XPWD	Wyświetla bieżący katalog lub bibliotekę
XRMD	Usuwa katalog

Podkomendy unikalne dla serwera FTP i5/OS

Podkomendy serwera FTP i5/OS obejmują specjalny zestaw komend, które są skróconymi nazwami odpowiadających im, lecz dłuższych komend CL systemu i5/OS.

Nazwy specjalnych podkomend serwera muszą być skrócone do 4 znaków, aby spełniały ograniczenia architektury FTP. Gdy serwer FTP otrzymuje te podkomendy, interpretuje je następująco:

- ADDM = ADDPFM (Add Physical File Member - Dodanie podzbioru zbioru fizycznego)
- ADDV = ADDPVLM (Add Physical File Variable Length Member - Dodanie podzbioru zbioru fizycznego o zmiennej długości)
- CRTL = CRTLIB (Create Library - Utworzenie biblioteki)
- CRTP = CRTPF (Create Physical File - Utworzenie zbioru fizycznego)
- CRTS = CRTSRCPF (Create Source Physical File - Utworzenie źródłowego zbioru fizycznego)
- DLTF = DLTF (Delete File - Usunięcie pliku)
- DLTL = DLTLIB (Delete Library - Usunięcie biblioteki)

Oprócz powyższych podkomend można użyć podkomendy RCMD serwera FTP w celu wysłania dowolnej komendy CL do serwera FTP.

Odsyłacze pokrewne

"Konwencje składni komend serwera FTP" na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

"Komunikaty o statusie z serwera FTP" na stronie 144
Po wpisaniu podkomendy podczas trwania sesji klienta FTP komunikaty o statusie zwracane są przez serwer za pomocą 3-cyfrowego kodu: *xyz*. Do każdej cyfry przypisane są pewne wartości wskazujące różne statusy.

"Podkomendy klienta FTP" na stronie 60
Za pomocą podkomend klienta FTP można nawiązywać połączenia ze zdalnymi serwerami FTP, przechodzić do bibliotek i katalogów oraz tworzyć, usuwać i przesyłać pliki.

ADDM (Dodanie podzbioru zbioru fizycznego - Add Physical File Member)

Podkomenda ADDM serwera FTP i5/OS służy do dodawania podzbioru do zbioru fizycznego.

Podkomenda serwera FTP

ADDM parametry

parametry

Parametry tej komendy są takie same, jak komendy ADDPFM języka CL.

Aby na przykład dodać podzbiór BANANA do zbioru fizycznego GEORGE w bibliotece RLKAYS, należy wpisać:

```
ADDM FILE(RLKAYS/GEORGE) MBR(BANANA)
```

Odsyłacze pokrewne

"Konwencje składni komend serwera FTP" na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

ADDV (Dodanie podzbioru zbioru fizycznego o zmiennej długości - Add Physical File Variable Length)

Podkomenda ADDV serwera FTP i5/OS służy do dodawania podzbioru o zmiennej długości do zbioru fizycznego.

Podkomenda serwera FTP

ADDV parametry

parametry

Parametry tej komendy są takie same, jak komendy ADDPVLM języka CL.

Aby na przykład dodać podzbiór POLEBEAN do zbioru fizycznego GEORGE w bibliotece RLKAYS, należy wpisać:
`ADDV FILE(RLKAYS/GEORGE) MBR(POLEBEAN)`

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

APPE (Dopisanie do istniejącego pliku - Append to Existing File)

Podkomenda APPE serwera FTP służy do akceptowania przesłanych danych i zapisywania ich w pliku na serwerze FTP. Jeśli podany plik istnieje, podkomenda dopisuje dane do tego pliku. W przeciwnym razie podkomenda tworzy taki plik.

Podkomenda serwera FTP

APPE *nazwa_pliku*

nazwa_pliku
Plik, w którym pobrane dane zostaną zapisane na serwerze FTP.

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

AUTH (Autoryzacja - Authorization)

Podkomenda AUTH serwera FTP i5/OS służy do określania mechanizmu uwierzytelniania i bezpieczeństwa, który jest używany dla bieżącej sesji FTP.

Podkomenda serwera FTP

Składnia tej komendy jest następująca:

AUTH [TLS-C | TLS-P | TLS | SSL]

Tabela 1. Wartości parametrów:

Wartość parametru	Definicja
TLS-C	Zastosowanie protokołu Transport Layer Security (TLS) jako mechanizmu ochrony. Ustawienia ochrony dla połączeń danych przyjmują domyślnie wartości RFC2228; oznacza to brak niejawnego zabezpieczenia połączeń danych.
TLS-P	Jako mechanizm ochrony wykorzystywany jest protokół TLS. Połączenie danych jest zabezpieczane niejawnie (taki sam efekt dają wywołane po kolei komendy: AUTH TLC-C, PBSZ 0, PROT P).
TLS	Patrz termin preferowany TLS-C.
SSL	Patrz termin preferowany TLS-P.

TLS-C	Zastosowanie protokołu Transport Layer Security (TLS) jako mechanizmu ochrony. Ustawienia ochrony dla połączeń danych przyjmują domyślnie wartości RFC2228; oznacza to brak niejawnego zabezpieczenia połączeń danych.
TLS-P	Jako mechanizm ochrony wykorzystywany jest protokół TLS. Połączenia danych zabezpieczane są niejawnie (taki sam efekt dają wywołane po kolei komendy: AUTH TLC-C, PBSZ 0, PROT P)

TLS	Patrz termin preferowany TLS-C.
SSL	Patrz termin preferowany TLS-P.

Uwaga: Protokół TLS jest kompatybilny z protokołem SSL (Secure Sockets Layer).

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

CCC (Kanał komendy usuwania zawartości - Clear Command Channel)

Podkomenda CCC serwera FTP i5/OS służy do zmiany trybu transmisji danych przez połączenie sterujące z trybu zaszyfrowanego na tryb jawnego tekstu.

Podkomenda serwera FTP

CCC

Kiedy serwer FTP otrzymuje podkomendę CCC (Kanał komendy usuwania zawartości - Clear Command Channel), sprawdza najpierw, czy bieżący użytkownik posiada uprawnienie do jej wykonania. Jeśli użytkownik posiada uprawnienie, serwer akceptuje tę komendę przez odesłanie do klienta FTP komunikatu potwierdzającego. Następnie serwer FTP zmienia tryb transmisji danych przez połączenie sterujące z trybu zaszyfrowanego na tryb jawnego tekstu.

Pozwala to zabezpieczyć poufne informacje, w tym nazwę użytkownika i hasło, wysyłając je w trybie zaszyfrowanym przez połączenie sterujące. Następnie przy użyciu podkomendy CCC można zmienić tryb transmisji na tryb jawnego tekstu i wysłać informacje o porcie i adresie IP.

W porównaniu z pełnym szyfrowaniem połączenia sterującego korzystanie z podkomendy CCC wiąże się z pewnym zagrożeniem dla bezpieczeństwa i integralności:

- Podczas korzystania z podkomendy CCC istnieje ryzyko przechwycenia nazw plików i katalogów na serwerze FTP. Same te nazwy mogą zawierać informacje poufne lub zastrzeżone.
- Hakerzy mogą z łatwością przechwycić adres IP i informacje o porcie przesyłane przez połączenie sterujące.
- Niebezpieczeństwo innych bezpośrednich ataków TCP na serwer FTP lub wykorzystania serwera FTP do ataku na inne systemy można całkowicie wyeliminować, stosując protokół TLS. Po przywróceniu trybu jawnego tekstu dla połączenia sterującego niektóre z tych ataków stają się ponownie możliwe.

Ze względu na te zagrożenia korzystanie z podkomendy CCC podlega kontroli przy użyciu interfejsu używania funkcji systemu i5/OS. Ustawienie domyślne podkomendy CCC dla serwera FTP to *DENIED.

Aby je zmienić, należy określić ustawienie *ALLOWED dla funkcji QIBM_QTMF_SERVER_REQ_10 za pomocą folderu Administrowanie aplikacjami (Application Administration) w programie System i Navigator lub komendy Zmiana użycia funkcji (Change Function Usage - CHGFCNUSG). W ten sposób można zezwolić danemu użytkownikowi zalogowanemu do serwera FTP na użycie podkomendy CCC i zakończenie ochrony połączenia sterującego.

Przykładowe użycie komendy CHGFCNUSG jest następujące:

```
CHGFCNUSG FCNID(QIBM_QTMF_SERVER_REQ_10) USER(user) USAGE(*ALLOWED)
```

Informacje pokrewne

Zabezpieczanie protokołu FTP za pomocą protokołu TLS

CRTL (Utworzenie biblioteki - Create Library)

Podkomenda CRTL serwera FTP i5/OS służy do tworzenia biblioteki.

Podkomenda serwera FTP

CRTL parametry

parametry
Parametry tej komendy są takie same, jak komendy CRTLIB języka CL.

Aby na przykład utworzyć bibliotekę o nazwie TESTTCP, należy wpisać:

```
CRTL TESTTCP
```

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

CRTP (Utworzenie zbioru fizycznego - Create Physical File)

Podkomenda CRTP serwera FTP i5/OS służy do tworzenia zbioru fizycznego.

Podkomenda serwera FTP

CRTP parametry

parametry
Parametry tej komendy są takie same, jak komendy CRTPF języka CL.

Na przykład, aby utworzyć zbiór fizyczny o nazwie MYFILE o długości rekordu 80 i bez ograniczeń liczby podzbiorów, należy wpisać:

```
CRTP FILE(RLKAYS/MYFILE) RCDLEN(80) MAXMBRS(*NOMAX)
```

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

CRTS (Utworzenie źródłowego zbioru fizycznego - Create Source Physical File)

Podkomenda CRTS serwera FTP i5/OS służy do tworzenia źródłowego zbioru fizycznego.

Podkomenda serwera FTP

CRTS parametry

parametry
Parametry tej komendy są takie same, jak komendy CRTSRCPF języka CL.

Na przykład, aby utworzyć źródłowy zbiór fizyczny o nazwie GEORGE w bibliotece RLKAYS, należy wpisać:

```
CRTS FILE(RLKAYS/GEORGE)
```

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

CWD (Zmiana katalogu roboczego lub biblioteki - Change Working Directory or Library)

Podkomenda CWD serwera FTP i5/OS służy do zmiany katalogu roboczego, biblioteki lub grupy plików.

Podkomenda serwera FTP

CWD *katalog*

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

DBUG (Włączenie śledzenia serwera FTP - Turn on the FTP Server Trace)

Podkomenda DBUG serwera FTP i5/OS służy do uruchamiania lub zatrzymywania śledzenia serwera.

Podkomenda serwera FTP

Uwaga: Śledzenie serwera FTP powinno być używane tylko w celu raportowania firmie IBM problemów z oprogramowaniem. Korzystanie z tej funkcji może niekorzystnie wpływać na wydajność systemu.

DBUG

Jeśli śledzenie serwera FTP nie jest aktywne, zostanie ono uruchomione. Serwer FTP kontynuuje śledzenie, dopóki nie odbierze innej podkomendy DBUG lub podkomendy QUIT. Formatowanie wyników śledzenia przez podkomendę DBUG po zakończeniu śledzenia przez serwer FTP może zająć dużo czasu.

Pojęcia pokrewne

“Śledzenie serwera FTP” na stronie 154
Serwer FTP można śledzić z dowolnego systemu używającego protokołu TCP/IP.

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

DELE (Usunięcie pliku lub dokumentu - Delete file or document)

Podkomenda DELE serwera FTP i5/OS służy do usuwania pliku, podzbioru lub dokumentu.

Podkomenda serwera FTP

DELE *plik_zdalny*

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

DLTF (Usunięcie zbioru - Delete File)

Podkomenda DLTF serwera FTP i5/OS usuwa zbiór.

Podkomenda serwera FTP

DLTF parametry

parametry

Parametry tej komendy są takie same, jak komendy DLTF języka CL.

Na przykład, aby usunąć zbiór MYFILE z biblioteki RLKAYS, należy wpisać:

```
DLTF FILE(RLKAYS/MYFILE)
```

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

DLTL (Usunięcie biblioteki - Delete Library)

Podkomenda DLTL serwera FTP i5/OS służy do usuwania biblioteki.

Podkomenda serwera FTP

DLTL parametry

parametry

Parametry tej komendy są takie same, jak komendy DLTLIB języka CL.

Na przykład, aby usunąć bibliotekę, należy wpisać:

```
DLTL nazwa_biblioteki
```

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

HELP (Uzyskiwanie pomocy z systemu zdalnego - Getting Help from a Remote System)

Podkomenda HELP serwera FTP i5/OS służy do wyświetlania informacji o podkomendach serwera FTP.

Podkomenda serwera FTP

HELP [*podkomenda*]

podkomenda

Nazwa podkomendy serwera, dla której mają zostać wyświetlone informacje. Na przykład podkomenda HELP ADDM spowoduje wyświetlenie informacji dotyczących dodawania podzbioru do zbioru fizycznego w systemie operacyjnym i5/OS.

Aby określić składnię podkomendy ADDV używanej przez system, należy użyć następującej podkomendy serwera:

```
HELP ADDV
```

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

LIST (Lista zbiorów - File List)

Podkomenda LIST serwera FTP i5/OS służy do wyświetlania listy pozycji katalogu, zawartości biblioteki lub zbiorów w grupie zbiorów.

Podkomenda serwera FTP

LIST [katalog | nazwa]

Wyświetlone zostaną tylko te pliki, które mogą być przesłane przez protokół FTP.

Zadania pokrewne

"Konfigurowanie serwerów FTP w celu współpracy z klientami FTP z interfejsem graficznym oraz narzędziami WWW" na stronie 8
Serwery FTP w systemie operacyjnym i5/OS obsługują klienty FTP z interfejsem graficznym, przeglądarki WWW oraz narzędzia WWW. Ponieważ większość klientów FTP z interfejsem graficznym używa formatu listingu przypominającego system UNIX oraz pliku ścieżek jako formatu nazw plików, serwer FTP musi być tak skonfigurowany, aby obsługiwał te formaty.

Odsyłacze pokrewne

"Pozycje pliku i katalogu w formacie i5/OS" na stronie 9
Klienty platformy System i umożliwiają listing plików na serwerze FTP zarówno w formacie systemu i5/OS, jak i w formacie właściwym dla systemu UNIX. W tym temacie omówiono format systemu i5/OS.

"Pozycje pliku i katalogu w formacie systemu UNIX" na stronie 10
Klienty platformy System i umożliwiają listing plików i katalogów na serwerze FTP zarówno w formacie systemu i5/OS, jak i w formacie systemu UNIX. W tym temacie omówiono format systemu UNIX.

"Konwencje składni komend serwera FTP" na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

"SITE (Wysłanie informacji używanych przez serwer - Send Information Used by a Server System)" na stronie 55
Podkomenda SITE serwera FTP i5/OS służy do wysyłania informacji lub udostępniania usług wykorzystywanych przez serwer FTP.

MKD (Utworzenie katalogu - Make Directory)

Podkomenda MKD serwera FTP i5/OS służy do tworzenia katalogu.

Podkomenda serwera FTP

MKD *nazwa_katalogu*

Odsyłacze pokrewne

"Konwencje składni komend serwera FTP" na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

MODE (Ustawienie trybu przesyłania danych - Set Transfer Mode)

Podkomenda MODE klienta FTP i5/OS służy do określania trybu lub formatu, w którym mają być przesyłane dane.

Podkomenda serwera FTP

MODE [B | S]

B Tryb blokowy. W tym trybie dane przesyłane są jako serie bloków danych zaopatrzonych w jeden lub więcej bajtów nagłówka.

S Tryb strumieniowy. W trybie tym dane są strumieniem bajtów. W trybie strumieniowym można użyć dowolnego typu reprezentacji. Ten tryb przesyłania jest bardziej wydajny, ponieważ serwer FTP nie przekazuje żadnych informacji o blokach danych.

Uwagi:

1. Tryb strumieniowy jest domyślnym trybem przesyłania używanym przez system. Jest to tryb preferowany.
2. Jeśli nie podano żadnych parametrów, serwer FTP zwraca odpowiedź wskazującą aktualne ustawienie podkomendy MODE.

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

NLST (Lista nazw - Name List)

Podkomenda NLST serwera FTP i5/OS służy do wyświetlania nazw wielu zbiorów, grupy zbiorów, katalogu lub biblioteki.

Podkomenda serwera FTP

```
NLST [katalog | nazwa]
```

Wyświetlone zostaną tylko te pliki, które mogą być przekazane przez protokół FTP.

Zadania pokrewne

“Konfigurowanie serwerów FTP w celu współpracy z klientami FTP z interfejsem graficznym oraz narzędziami WWW” na stronie 8
Serwery FTP w systemie operacyjnym i5/OS obsługują klienty FTP z interfejsem graficznym, przeglądarki WWW oraz narzędzia WWW. Ponieważ większość klientów FTP z interfejsem graficznym używa formatu listingu przypominającego system UNIX oraz pliku ścieżek jako formatu nazw plików, serwer FTP musi być tak skonfigurowany, aby obsługiwał te formaty.

Odsyłacze pokrewne

“Pozycje pliku i katalogu w formacie i5/OS” na stronie 9
Klienty platformy System i umożliwiają listing plików na serwerze FTP zarówno w formacie systemu i5/OS, jak i w formacie właściwym dla systemu UNIX. W tym temacie omówiono format systemu i5/OS.

“Pozycje pliku i katalogu w formacie systemu UNIX” na stronie 10
Klienty platformy System i umożliwiają listing plików i katalogów na serwerze FTP zarówno w formacie systemu i5/OS, jak i w formacie systemu UNIX. W tym temacie omówiono format systemu UNIX.

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

NOOP (Uzyskanie odpowiedzi serwera - Obtain Server Response)

Podkomenda NOOP serwera FTP i5/OS sprawdza, czy serwer FTP jest podłączony i reaguje na żądania. Jeśli serwer reaguje, wysyła do klienta odpowiedź OK. Podkomenda ta nie wpływa w żaden sposób na przetwarzanie danych przez serwer.

Podkomenda serwera FTP

```
NOOP
```

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

PASS (Hasło -Password)

Podkomenda PASS serwera FTP i5/OS służy do wysyłania hasła do serwera FTP.

Podkomenda serwera FTP

```
PASS hasło
```

hasło Łańcuch tekstu, który określa hasło w systemie serwera.

Uwaga: Podkomenda serwera USER musi być uruchomiona bezpośrednio przed uruchomieniem podkomendy serwera PASS.

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

PASV (Użycie pasywnego połączenia danych - Use Passive Data Connection)

Podkomenda PASV serwera FTP i5/OS służy do wydawania serwerowi FTP polecenia pasywnego otwarcia następnego połączenia danych.

Podkomenda serwera FTP

PASV

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

PBSZ (Zabezpieczenie wielkości buforu - Protection Buffer Size)

Podkomenda PBSZ serwera FTP i5/OS służy do definiowania maksymalnej wielkości buforu dla danych zakodowanych na poziomie aplikacji, które są wysyłane lub odbierane przez połączenie danych.

Podkomenda serwera FTP

PBSZ *wartość*

gdzie *wartość* jest ciągiem znaków ASCII odpowiadającym liczbie dziesiętnej.

Uwaga: Dla tego parametru należy określić wartość ’0’.

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

PORT (Port danych - Data Port)

Podkomenda PORT serwera FTP i5/OS służy do określania portu danych, na którym klient będzie nasłuchiwał połączenia.

Podkomenda serwera FTP

PORT h1,h2,h3,h4,p1,p2

h *n* Reprezentuje adres IP systemu i jest łańcuchem znaków oznaczającym wartość dziesiętną między 0 a 255.

p *n* Reprezentuje numer portu TCP systemu i jest łańcuchem znaków oznaczającym wartość dziesiętną między 0 a 255.

Aby przekształcić wartości p1 i p2 na numer portu TCP, należy użyć następującej formuły:

```
port = ( p1 * 256 ) + p2
```

Na przykład w tej komendzie PORT:

```
PORT 9,180,128,180,4,8
```

numer portu to 1032, a adres IP to 9.180.128.180.

Uwaga: Jak określono w dokumencie Request for Comments (RFC) 1122 protokołu TCP/IP, serwer FTP po zamknięciu połączenia nie może połączyć się z tym samym adresem IP klienta i numerem portu, dopóki nie upłynie czas opóźnienia wynoszący dwie minuty. Serwer FTP może nawiązać połączenie z tym samym adresem IP klienta bez powyższego ograniczenia, korzystając z innego numeru portu.

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

PROT (Poziom ochrony kanału danych - Data Channel Protection Level)

Podkomenda PROT serwera FTP i5/OS służy do definiowania ochrony używanej dla połączeń danych w protokole FTP, które są używane do przesyłania listingów katalogów i danych plików.

Podkomenda serwera FTP

```
PROT [ C | P ]
```

Tabela 2. Wartości parametrów:

Wartość parametru	Definicja
C	Jawne. Za pomocą połączenia danych przesyłane są ″dane surowe″ bez ochrony.
P	Poufne. Połączenie danych będzie korzystać z protokołów TLS lub SSL, które zapewniają ochronę integralności i poufności.

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

PWD (Wyświetlenie katalogu roboczego lub biblioteki - Display Working Directory or Library)

Podkomenda PWD serwera FTP i5/OS służy do wyświetlania nazwy katalogu bieżącego lub biblioteki bieżącej.

Podkomenda serwera FTP

```
PWD
```

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

QUIT (Zakończenie sesji serwera FTP - End an FTP Server Session)

Podkomenda QUIT serwera FTP i5/OS służy do wylogowywania się z użytkownika klienta i zamykania połączenia sterującego. Jeśli trwa przesyłanie plików, połączenie jest utrzymywane do momentu zakończenia przesyłania, a następnie serwer je zamyka.

Podkomenda serwera FTP

```
QUIT
```

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

RCMD (Wysłanie komendy języka CL do serwera FTP - Send a CL Command to an FTP Server System)

Podkomenda serwera RCMD służy do wykonywania komend CL systemu i5/OS na serwerze FTP. Łańcuch komendy RCMD ma długość do 1000 znaków. Ponieważ dla podkomendy RCMD nie jest dostępny żaden wiersz komend, łańcuch podkomendy RCMD musi zawierać wszystkie parametry niezbędne do uruchomienia komendy CL.

Podkomenda serwera FTP

Jeśli komenda CL wywołana przez podkomendę RCMD zostanie zakończona powodzeniem, wyświetlony zostanie komunikat informujący o jej pomyślnym wykonaniu. W przypadku wystąpienia błędu zostanie wyświetlony komunikat o błędzie. Komunikat ten nie podaje przyczyn wystąpienia błędu, chyba że błąd powstał z powodu podania niewłaściwej biblioteki, zbioru lub podzbioru.

Oto przykład użycia komendy RCMD w celu uruchomienia komendy Usunięcie pliku (Delete File - DLTF):

```
QUOte RCMD DLTF FILE(mojabib/mojzbior)
```

mojabib jest nazwą biblioteki, z której zbiór ma być usunięty. mojzbior jest nazwą zbioru, który ma być usunięty.

Warto także przeczytać informacje o serwerze REXEC, który udostępnia alternatywny sposób uruchamiania komend w języku CL w systemie zdalnym.

Pojęcia pokrewne

Serwer REXEC

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

“QUOTE (Wysłanie komendy do serwera FTP - Send a Subcommand to an FTP Server)” na stronie 83
Podkomenda QUOTE klienta FTP i5/OS służy do wysyłania podkomendy do serwera FTP.

REIN (Reinicjowanie sesji pomiędzy systemami - Reinitialize Session between Systems)

Podkomenda REIN serwera FTP i5/OS służy do ponownego uruchamiania sesji na serwerze FTP.

Podkomenda serwera FTP

REIN

Komenda REINITIALIZE:

1. Umożliwia zakończenie rozpoczętego procesu przesyłania.
2. Kończy sesję USER, usuwając wszystkie informacje wejścia/wyjścia i informacje o koncie.
3. Przywraca ustawienia domyślne wszystkim parametrom serwera FTP.
4. Pozostawia otwarte łącze sterujące.

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

RETR (Pobranie pliku - Retrieve file)

Podkomenda RETR serwera FTP i5/OS służy do wczytywania danych z serwera FTP.

Podkomenda serwera FTP

```
RETR plik_zdalny
```

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

RMD (Usuwanie katalogu - Remove Directory)

Podkomenda RMD serwera FTP i5/OS służy do usuwania katalogu.

Podkomenda serwera FTP

```
RMD nazwa_katalogu
```

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

RNFR (Zmiana nazwy z - Rename From)

Podkomenda RNFR serwera FTP i5/OS służy do zmiany nazw plików. Bezpośrednio po tej podkomendzie należy użyć podkomendy RNTO (Zmiana nazwy na - Rename To) serwera FTP.

Podkomenda serwera FTP

```
RNFR nazwa_pliku
```

nazwa_pliku
Nazwa pliku, która ma zostać zmieniona.

Uwaga: System operacyjny i5/OS nie może zmienić nazwy pliku na nazwę z innego systemu plików.

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

RNTO (Zmiana nazwy na - Rename To)

Podkomenda RNTO serwera FTP i5/OS służy do określania nowej nazwy pliku podczas zmiany nazw plików na serwerze FTP. Należy jej użyć bezpośrednio po komendzie RNFR określającej nazwę pliku, która ma zostać zmieniona.

Podkomenda serwera FTP

```
RNTO nazwa_pliku
```

nazwa_pliku
Nowa nazwa pliku, jaka ma być nadana.

Uwaga: System operacyjny i5/OS nie może zmienić nazwy pliku na nazwę z innego systemu plików.

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

SITE (Wysłanie informacji używanych przez serwer - Send Information Used by a Server System)

Podkomenda SITE serwera FTP i5/OS służy do wysyłania informacji lub udostępniania usług wykorzystywanych przez serwer FTP.

Podkomenda serwera FTP

```
SITE [parametry]
```

Serwer FTP i5/OS obsługuje następujące parametry podkomendy SITE:

LISTFMT 0
Serwer FTP zwraca informacje dla podkomendy LIST w formacie listingu systemu i5/OS. Klient na platformie System i obsługuje zarówno format systemu i5/OS, jak i format systemu UNIX.

LISTFMT 1
Serwer FTP zwraca informacje dla podkomendy LIST w formacie listingu w stylu systemu UNIX. Nazwa pliku jest ostatnią pozycją każdego zwróconego wiersza. Klient na platformie System i obsługuje zarówno format systemu i5/OS, jak i format w stylu systemu UNIX.

LISTFMT
Zwraca komunikat wskazujący bieżące ustawienia LISTFMT serwera FTP.

Uwagi:

Aby zmienić domyślne ustawienia parametru LISTFMT na serwerze, należy użyć opcji LISTFMT komendy Zmiana atrybutów FTP (Change FTP Attributes - CHGFTPA). Tę właściwość serwera FTP można również zmienić przy użyciu programu System i Navigator.

1. W programie System i Navigator rozwiń ***system*** **→ Sieć → Serwery → TCP/IP** (*system* > Network > Servers > TCP/IP).
2. W prawym panelu kliknij prawym przyciskiem myszy **FTP** i wybierz **Właściwości**.
3. Kliknij zakładkę **Formaty**.
4. Pod nagłówkiem **Lista zbiorów** (File List) kliknij opcję **i5/OS** lub **UNIX** w zależności od tego, jakie ma być domyślne ustawienie parametru LISTFMT na serwerze FTP.
5. Kliknij **OK**, aby zaakceptować zmiany.

NAMEFMT 0
Użyj formatu nazwy LIBRARY/FILE.MEMBER. Ten format nazewnictwa dopuszczalny jest jedynie dla zbiorów baz danych systemu plików bibliotek.

NAMEFMT 1
Użyj formatu nazewnictwa ścieżek. Ten format nazw jest przeznaczony dla wszystkich systemów plików, które są obsługiwane przez protokół FTP, w tym systemu plików bibliotek. Współpraca ze wszystkimi systemami plików systemu i5/OS innymi niż system plików bibliotek wymaga użycia formatu nazw 1.

NAMEFMT
Zwraca komunikat, który zawiera aktualne ustawienia formatu nazewnictwa plików serwera.

Uwaga: Ustawienie domyślne parametru NAMEFMT dla serwera FTP i5/OS można skonfigurować za pomocą opcji NAMEFMT komendy CHGFTPA.

CRTCCSID *CALC
Nowe zbiory baz danych utworzone w trakcie przesyłania plików ASCII używają odpowiedniego domyślnego identyfikatora CCSID EBCDIC jako identyfikatora CCSID przesyłania plików ASCII.

CRTCCSID *USER
Nowe zbiory baz danych tworzone podczas przesyłania plików ASCII używają identyfikatora CCSID bieżącego zadania. Jeśli jest to identyfikator CCSID 65535, domyślny identyfikator CCSID określany jest przez identyfikator języka w bieżącej specyfikacji zadania.

CRTCCSID *SYSVAL
Nowe zbiory baz danych tworzone podczas przesyłania plików ASCII używają identyfikatora CCSID podanego przez wartość systemową QCCSID.

CRTCCSID [numer_CCSID]
Podczas tworzenia zbiorów baz danych w trakcie przesyłania plików ASCII, należy określić identyfikator CCSID. Serwer sprawdza, czy podana wartość jest poprawna.

CRTCCSID
Wyświetlenie komunikatu, który zawiera aktualne ustawienia CRTCCSID klienta FTP.

NULLFLDS 0
Serwer FTP nie pozwala na przesyłanie zbiorów baz danych zawierających pola NULL. Jest to wartość domyślna.

NULLFLDS 1
Serwer FTP pozwala na przesyłanie zbiorów baz danych zawierających pola NULL.

Uwaga: Przesyłanie zbiorów, które zawierają pola NULL, wymaga włączenia tego ustawienia zarówno w serwerze, jak i w kliencie. Jeśli serwer przesyła zbiór zawierający pola NULL do serwera FTP, który nie jest platformą System i, lub jeśli typ przesyłania wymaga konwersji strony kodowej danych, wyniki przesyłania są nieprzewidywalne.

NULLFLDS
Zwraca komunikat wskazujący bieżące ustawienia NULLFLDS serwera FTP.

TRIM 0
Ustawienie opcji Trim na OFF (Wyłączone). Serwer FTP wysyła końcowe odstępy rekordów bazy danych.

TRIM 1
Ustawienie opcji Trim na ON (Włączone). Serwer FTP nie wysyła końcowych odstępów rekordów bazy danych podczas przesyłania zbiorów bazy danych, które używają struktury zbiorów i trybu strumieniowego. Jest to wartość domyślna.

TRIM 2
Serwer FTP nie wysyła końcowych odstępów rekordów bazy danych w żadnych operacjach przesyłania, w tym przeprowadzanych za pomocą struktury rekordu i trybu blokowego.

TRIM Zwraca komunikat zawierający aktualne ustawienia opcji Trim serwera FTP.

Uwagi:

1. Dopóki ta podkomenda nie będzie dostępna, przed przesłaniem zbioru do serwera FTP końcowe odstępy rekordów systemu plików QSYS.LIB będą zawsze usuwane.
2. Ustawienia TRIM nie dotyczą binarnego przesyłania plików (TYPE I). Podczas przesyłania plików binarnych (TYPE I), bez względu na ustawienia opcji TRIM, odstępy nigdy nie są usuwane.

Zadania pokrewne

“Konfigurowanie serwerów FTP w celu współpracy z klientami FTP z interfejsem graficznym oraz narzędziami WWW” na stronie 8
Serwery FTP w systemie operacyjnym i5/OS obsługują klienty FTP z interfejsem graficznym, przeglądarki WWW oraz narzędzia WWW. Ponieważ większość klientów FTP z interfejsem graficznym używa formatu listingu przypominającego system UNIX oraz pliku ścieżek jako formatu nazw plików, serwer FTP musi być tak skonfigurowany, aby obsługiwał te formaty.

Odsyłacze pokrewne

“Pozycje pliku i katalogu w formacie i5/OS” na stronie 9
Klienty platformy System i umożliwiają listing plików na serwerze FTP zarówno w formacie systemu i5/OS, jak i w formacie właściwym dla systemu UNIX. W tym temacie omówiono format systemu i5/OS.

“Pozycje pliku i katalogu w formacie systemu UNIX” na stronie 10
Klienty platformy System i umożliwiają listing plików i katalogów na serwerze FTP zarówno w formacie systemu i5/OS, jak i w formacie systemu UNIX. W tym temacie omówiono format systemu UNIX.

“LIST (Lista zbiorów - File List)” na stronie 48
Podkomenda LIST serwera FTP i5/OS służy do wyświetlania listy pozycji katalogu, zawartości biblioteki lub zbiorów w grupie zbiorów.

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

STOR (Zapisanie pliku - Store File)

Podkomenda STOR serwera FTP i5/OS służy do składowania danych na serwerze i zastępuje istniejący plik.

Podkomenda serwera FTP

```
STOR plik_zdalny
```

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

STOU (Zapisanie unikalnych - Store Unique)

Podkomenda STOU serwera FTP i5/OS służy do składowania danych na serwerze FTP i nie zastępuje istniejącego pliku. Serwer tworzy unikalną nazwę pliku. Nazwa przypisana do pliku zostanie umieszczona w odpowiedzi wysłanej do klienta.

Podkomenda serwera FTP

```
STOU plik_zdalny
```

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

STRU (Określenie struktury plików - Specify File Structure)

Podkomenda STRU serwera FTP i5/OS służy do określania struktury pliku jako ciągłej sekwencji bajtów danych.

Podkomenda serwera FTP

```
STRU [F | R]
```

F Struktura plików. Struktura pliku zdefiniowana jest jako ciągła sekwencja bajtów danych.

R Struktura rekordów. Plik przesyłany jest jako ciąg rekordów sekwencyjnych.

Uwagi:

1. Struktura pliku wpływa na tryb przesyłania, interpretację i pojemność pliku.
2. Jeśli nie podano żadnych parametrów, serwer zwraca odpowiedź wskazującą aktualne ustawienia struktury plików.

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

SYST (Identyfikacja nazwy systemu operacyjnego - Identify the Name of the Operating System)

Podkomenda SYST serwera FTP i5/OS służy do wyświetlania nazwy systemu operacyjnego, w którym jest uruchomiony serwer FTP.

Podkomenda serwera FTP

SYST

Zwrócone informacje zależą od systemu.

Odpowiedź serwera FTP zawiera wersję protokołu TCP/IP. Oto przykładowa odpowiedź serwera:

```
Zdalnym systemem operacyjnym jest system i5/OS. Wersja protokołu
TCP/IP: "V4R4M0".
```

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

TIME (Ustawienie wartości limitu czasu dla serwera FTP - Set Timeout Values for FTP Server)

Podkomenda TIME serwera FTP i5/OS służy do ustawiania wartości limitu czasu przesyłania i braku aktywności serwera FTP.

Podkomenda serwera FTP

Po nawiązaniu połączenia sterującego pomiędzy klientem a serwerem FTP, serwer FTP kontroluje limit czasu dla tego połączenia. Jest to wartość limitu czasu braku aktywności.

Istnieje także wartość limitu czasu dla połączenia danych, nazywana limitem czasu przesyłania.

Komenda TIME serwera FTP ma następujący format:

TIME brak_aktywności [przesyłanie]

brak_aktywności
: Liczba sekund, podczas których serwer oczekuje na zakończenie połączenia z klientem. Dozwolony zakres wartości limitu czasu braku aktywności wynosi od 1 do 9 999 999 sekund. Wartością domyślną limitu czasu braku aktywności jest 300 sekund.

przesyłanie
: Limit czasu przesyłania w sekundach. Parametr opcjonalny. Jeśli nie zostanie podany, serwer nie zmieni bieżącej wartości. Dozwolony zakres wartości limitu czasu przesyłania wynosi od 1 do 9 999 999 sekund. Wartością domyślną limitu czasu przesyłania jest 420 sekund.

Aby na przykład ustawić wartość limitu czasu braku aktywności serwera FTP na 1000 sekund i zachować bieżącą wartość limitu czasu przesyłania, należy wpisać:

```
QUOTE TIME 1000
```

Komenda TIME nie jest standardową komendą protokołu FTP. Jest ona właściwa dla serwera FTP i5/OS.

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

TYPE (Określenie typu reprezentacji - Specify Representation Type)

Podkomenda TYPE serwera FTP i5/OS służy do określania typu przesyłania plików lub reprezentacji, w jakiej odbywa się przesyłanie.

Podkomenda serwera FTP

```
TYPE   [ A
       |  B [ 1 | 2 | 3 [A|R] | 4 [A|R  ] | 5 | 6 | 7]
       |  C ccsid#
       |  E
       |  F [ 1 ]
       |  I ]
```

A Określa typ przesyłania jako typ domyślny (ASCII). Serwer nie przypisuje do pliku żadnej kontroli formatu pionowego. Obsługuje jedynie domyślny format NON PRINT dla ASCII. Typ przesyłania ASCII przeznaczony jest do przesyłania plików tekstowych, z wyjątkiem sytuacji, gdy oba systemy używają typu EBCDIC.

Uwaga: Identyfikator CCSID dla TYPE A to wartość CCSID atrybutów konfiguracyjnych serwera FTP. Atrybuty te można zmienić za pomocą komendy CHGFTPA.

B JIS Kanji (CCSID 932)

B 1 JIS Kanji (CCSID 932)

B 2 Rozszerzony kod UNIX Kanji (CCSID 5050)

B 3 JIS 1983 używający sekwencji ASCII shift-in o zmienionym znaczeniu (CCSID 5054)

B 3 A JIS 1983 używający sekwencji ASCII shift-in o zmienionym znaczeniu (CCSID 5054)

B 3 R JIS 1983 używający JISROMAN sekwencji shift-in o zmienionym znaczeniu (CCSID 5052)

B 4 JIS 1978 używający sekwencji ASCII shift-in o zmienionym znaczeniu (CCSID 5055)

B 4 A JIS 1978 używający sekwencji ASCII shift-in o zmienionym znaczeniu (CCSID 5055)

B 4 R JIS 1978 używający sekwencji JISROMAN shift-in o zmienionym znaczeniu (CCSID 5053)

B 5 Hangeul (CCSID 934)

B 6 Koreański kod standardowy KSC-5601, wersja 1989 (CCSID 949)

B 7 Tradycyjny chiński (5550 - CCSID 938)

C Określa typ przesyłania jako dowolny identyfikator CCSID zainstalowany w systemie. Numer identyfikatora CCSID musi być zgodny z C.

E Określa typ przesyłania jako EBCDIC. Serwer nie przypisuje do pliku żadnej kontroli formatu pionowego. Obsługuje jedynie domyślny format NON PRINT dla EBCDIC. Typ przesyłania EBCDIC przeznaczony jest do wydajnego przesyłania plików pomiędzy systemami, które używają kodowania EBCDIC dla wewnętrznych reprezentacji znaków.

F Kod IBM EBCDIC Kanji (CCSID 5035)

F 1 Kod IBM EBCDIC Kanji (CCSID 5035)

I Określa typ przesyłania jako obraz (binarny). W tym typie przesyłania dane wysyłane są jako łańcuch bitów zestawionych w 8-bitowe bajty. Ten typ przesyłania binarnego używany jest do wydajnego przechowywania i pobierania plików i przesyłania danych binarnych, takich jak kod obiektów.

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

USER (Wysłanie ID użytkownika do serwera - Send a User Logon ID to the Server)

Podkomenda USER serwera FTP i5/OS służy do wysyłania identyfikatora logowania użytkownika do serwera FTP. Jeśli wykonanie podkomendy USER powiedzie się, a w w systemie skonfigurowano zabezpieczenie hasłem, do klienta zostanie wysłana odpowiedź z żądaniem hasła.

Podkomenda serwera FTP

```
USER nazwa_użytkownika
```

nazwa_użytkownika
Profil użytkownika w systemie operacyjnym i5/OS.

Uwaga: Jeśli serwer FTP tego zażąda, klient wysyła do niego hasło za pomocą podkomendy serwera PASS. Zapytanie o hasło nie występuje, jeśli serwer FTP pracuje na poziomie bezpieczeństwa 10.

Odsyłacze pokrewne

“Konwencje składni komend serwera FTP” na stronie 146
Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

Podkomendy klienta FTP

Za pomocą podkomend klienta FTP można nawiązywać połączenia ze zdalnymi serwerami FTP, przechodzić do bibliotek i katalogów oraz tworzyć, usuwać i przesyłać pliki.

Komendy protokołu FTP umożliwiają przesyłanie plików pomiędzy komputerami.

Opisy i składnie komend klienta zamieszczone są w tematach znajdujących się w dalszej części dokumentu.

Te podkomendy są wykorzystywane przez klienta FTP systemu i5/OS. W poniższej tabeli przedstawiono podkomendy klienta, skróty oraz opis każdej podkomendy.

Podkomenda	Do czego służy
?	Opisuje sposób używania klienta FTP
ACCT	Wysyła informacje o koncie użytkownika do systemu zdalnego
APPEND	Dodaje lokalny podzbiór zbioru do zbioru w systemie zdalnym
ASCII	Ustawia typ przesyłania plików na format ASCII
BINARY	Ustawia typ przesyłania plików na format BINARY
“CCC (Kanał komendy usuwania zawartości - Clear Command Channel)” na stronie 64	Zmienia tryb transmisji danych przez połączenie sterujące z trybu zaszyfrowanego na tryb jawnego tekstu
CD	Zmienia katalog roboczy w systemie zdalnym
CDUP	Przechodzi do katalogu nadrzędnego w systemie zdalnym
CLOSE	Kończy sesję z systemem zdalnym
DEBUG	Włącza lub wyłącza debugowanie
DEBUG	Zmienia wartości limitu czasu klienta
DELETE	Usuwa plik z systemu zdalnego
DIR	Wyświetla katalogi i pliki systemu zdalnego
EBCDIC	Ustawia typ przesyłania plików na format EBCDIC

Podkomenda	Do czego służy
GET	Kopiuje plik z systemu zdalnego do lokalnego
HELP	Pobiera informacje o podkomendach klienta FTP
LCD	Zmienia katalog roboczy w systemie lokalnym
LOCSITE	Podaje informacje dotyczące lokalnej witryny
LOCSTAT	Wyświetla informacje o statusie lokalnym
LPWD	Wyświetla katalog roboczy w systemie lokalnym
LS	Wyświetla listę nazw plików w zestawie plików w systemie zdalnym
LTYPE	Określa typ przesyłania plików w systemie lokalnym
MDELETE	Usuwa wiele plików z serwera
MGET	Kopiuje plik lub pliki z systemu zdalnego
MKDIR	Tworzy katalog lub podkatalog
MODE	Określa format danych dla przesyłanych plików
MPUT	Wysyła plik lokalny lub pliki lokalne do systemu zdalnego
NAMEFMT	Określa obowiązujący format nazw plików
NOOP	Sprawdza, czy uzyskiwane są odpowiedzi
NULLFLDS	Umożliwia przesyłanie pól NULL
OPEN	Nawiązuje połączenie z serwerem FTP
PASS	Wysyła hasło użytkownika
PUT	Kopiuje lokalny podzbiór zbioru do systemu zdalnego
PWD	Wyświetla bieżący katalog systemu zdalnego
QUIT	Kończy sesję FTP
QUOTE	Wysyła podkomendę do serwera FTP
REINITIALIZE	Ponownie uruchamia sesję w systemie zdalnym
RENAME	Zmienia nazwę pliku w systemie zdalnym
RESET	Usuwa zawartość kolejki odpowiedzi serwera
RMDIR	Usuwa katalog z systemu zdalnego
SECDATA	Określa poziom ochrony używany dla połączeń danych, jeśli z serwerem FTP jest nawiązane bezpieczne połączenie
SECOPEN	Otwiera bezpieczne połączenie sterujące z serwerem FTP, używając określonego protokołu bezpieczeństwa
SENDPASV	Określa, czy wysyłana jest podkomenda PASV
SENDPORT	Określa, czy wysyłana jest podkomenda PORT
SENDSITE	Określa, czy wysyłana jest podkomenda SITE
SITE	Wysyła informacje, które mogą być użyte przez system zdalny
STATUS	Pobiera informacje o statusie z systemu zdalnego
STRUCT	Określa strukturę pliku wysyłanych danych
SUNIQUE	Steruje zastępowaniem plików
SYSCMD	Uruchamia komendę CL w systemie lokalnym bez zamykania klienta FTP
SYSTEM	Wyświetla system operacyjny systemu zdalnego
TYPE	Określa typ przesyłania plików

Podkomenda	Do czego służy
USER	Wysyła identyfikator użytkownika do systemu zdalnego
VERBOSE	Steruje wyświetlaniem odpowiedzi serwera FTP

Odsyłacze pokrewne

“Podkomendy serwera FTP” na stronie 41
Poniższe podkomendy przedstawiają komunikację pomiędzy klientem FTP a serwerem FTP. W tym temacie opisano podkomendy odpowiadające komendom CL w systemie i5/OS, które są unikalne dla serwera FTP i5/OS.

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

“Komunikaty o statusie z serwera FTP” na stronie 144
Po wpisaniu podkomendy podczas trwania sesji klienta FTP komunikaty o statusie zwracane są przez serwer za pomocą 3-cyfrowego kodu: *xyz*. Do każdej cyfry przypisane są pewne wartości wskazujące różne statusy.

ACCT (Wysłanie informacji o koncie - Send Account Information)

Wiele systemów przed udostępnieniem niektórych funkcji systemu wymaga podania informacji o koncie. System zdalny żąda podania tych informacji. Podkomenda ACCT klienta FTP i5/OS służy do wysyłania do systemu zdalnego informacji o koncie użytkownika.

Podkomenda klienta FTP

ACCT *informacje_o_koncie*

informacje_o_koncie
Łańcuch tekstu identyfikujący konto użytkownika. Informacje o koncie mogą mieć formę hasła, którego host używa do nadawania określonych uprawnień. Hasło to nie jest hasłem użytkownika, lecz hasłem w systemie zdalnym.

Na przykład protokół TCP/IP w systemie operacyjnym maszyny wirtualnej IBM może zażądać hasła dostępu do minidysków w celu wykonania operacji odczytu i zapisu. Komenda ACCT służy do podania hasła do minidysków bieżącego katalogu. Jeśli systemem zdalnym jest produkt System i, podkomenda ACCT nie wykonuje żadnego działania.

Odsyłacze pokrewne

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

“APPEND (Dodanie podzbioru zbioru lokalnego do pliku zdalnego - Append a Local File Member to a Remote File)”
Podkomenda APPEND klienta FTP i5/OS służy do dodawania lokalnego podzbioru zbioru, dokumentu lub innego pliku systemu plików do zbioru zdalnego.

“DELETE (Usunięcie pliku z systemu zdalnego - Delete a File on a Remote System)” na stronie 68
Podkomenda DELETE klienta FTP i5/OS służy do usuwania zbioru lub podzbioru zbioru bazy danych w systemie zdalnym. System zdalny może zażądać uprawnień do usunięcia pliku. W celu wysłania odpowiedzi na to żądanie należy użyć podkomendy ACCT (Wysłanie informacji o koncie - Send Account Information).

APPEND (Dodanie podzbioru zbioru lokalnego do pliku zdalnego - Append a Local File Member to a Remote File)

Podkomenda APPEND klienta FTP i5/OS służy do dodawania lokalnego podzbioru zbioru, dokumentu lub innego pliku systemu plików do zbioru zdalnego.

Podkomenda klienta FTP

Append *plik_lokalny* [plik_zdalny]

plik_lokalny
Nazwa lokalnego podzbioru zbioru, dokumentu lub innego pliku systemu i5/OS. Nazwa pliku hierarchicznego systemu plików (HFS), który został dodany do katalogu w systemie zdalnym.

plik_zdalny
Plik w systemie zdalnym. Jeśli nie zostanie podany plik zdalny, klient FTP utworzy nazwę domyślną.

Jeśli plik zdalny nie istnieje w systemie, utworzy go serwer FTP.

Do dodania pliku do systemu zdalnego wymagane są uprawnienia zapisu w tym systemie. Wymagane informacje o koncie można dostarczyć za pomocą podkomendy ACCT (patrz sekcja ACCT, Wysłanie informacji o koncie - Send Account Information).

Domyślnym trybem kopiowania plików jest tryb strumieniowy (stream). Tryb ten można zmienić za pomocą podkomendy MODE. W przypadku zbioru zdalnego w formacie o stałej długości rekordów, serwer FTP zachowuje format zbioru i długość rekordów. Gdy jest to wymagane, rekordy podzbioru zbioru lokalnego są wypełniane znakami pustymi lub skracane.

Odsyłacze pokrewne

"NAMEFMT (Wybranie formatu nazw plików - Select File Naming Format)" na stronie 79
Podkomenda NAMEFMT klienta FTP i5/OS służy do wybierania formatu nazw plików, który będzie używany w systemie lokalnym i zdalnym.

"Nazwy plików dla podkomend klienta służących do przesyłania danych" na stronie 148
W przypadku niektórych podkomend można używać domyślnych nazw plików źródłowych i docelowych; należy jednak określić nazwę pliku dla pozostałych podkomend.

"ACCT (Wysłanie informacji o koncie - Send Account Information)" na stronie 62
Wiele systemów przed udostępnieniem niektórych funkcji systemu wymaga podania informacji o koncie. System zdalny żąda podania tych informacji. Podkomenda ACCT klienta FTP i5/OS służy do wysyłania do systemu zdalnego informacji o koncie użytkownika.

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

"Nazwy plików do przesyłania" na stronie 150
Podkomendy klienta FTP używane do przesyłania danych mogą zawierać parametr **plik_lokalny**, **plik_zdalny** lub oba te parametry. Można ich użyć do nazwania danych, które mają być przesłane.

ASCII (Zmiana typu pliku na ASCII - Change File Type to ASCII)

Podkomenda ASCII klienta FTP i5/OS służy doustawiania typu przesyłania plików na format ASCII.

Podkomenda klienta FTP

AScii

Istnieją dwa podstawowe typy plików, które można używać podczas przesyłania plików za pomocą serwera FTP: ASCII i BINARY. Pliki ASCII są zwykłymi plikami tekstowymi. Mogą one mieć różne rozszerzenia, na przykład .txt, lub nie mieć żadnego rozszerzenia. Pliki BINARY są programami lub plikami innymi niż tekstowe, zapisanymi w formacie aplikacji, w której zostały stworzone, albo formatami plików zarchiwizowanych lub skompresowanych.

Użyj typu przesyłania ASCII do przesyłania plików tekstowych do lub z systemu ASCII, który nie obsługuje reprezentacji znaków w formacie EBCDIC. ASCII jest domyślnym typem przesyłania. Serwer FTP nie przypisuje do pliku sterowania w formacie pionowym. ASCII obsługuje jedynie domyślny format NON PRINT.

Pojęcia pokrewne

“Metody przesyłania danych” na stronie 133
Przed rozpoczęciem przesyłania plików należy wybrać właściwy format ich przesyłania. Można użyć domyślnego formatu ASCII lub podać inny format, na przykład EBDCIC lub BINARY.

Odsyłacze pokrewne

“Scenariusz: przesyłanie pliku ze zdalnego hosta” na stronie 1
Ten scenariusz opisuje, jak za pomocą podstawowych funkcji protokołu FTP pobrać pliki ze zdalnego hosta. W tym scenariuszu klient i serwer są systemami używającymi protokołu FTP i5/OS.

“BINARY (Ustawienie typu przesyłania dla obrazu - Set Transfer Type to Image)”
Podkomenda BINARY klienta FTP i5/OS służy do ustawiania typu przesyłania plików na format BINARY.

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

BINARY (Ustawienie typu przesyłania dla obrazu - Set Transfer Type to Image)

Podkomenda BINARY klienta FTP i5/OS służy do ustawiania typu przesyłania plików na format BINARY.

Podkomenda klienta FTP

Binary

Istnieją dwa podstawowe typy plików, które można używać podczas przesyłania plików za pomocą serwera FTP: ASCII i BINARY. Pliki ASCII są zwykłymi plikami tekstowymi. Mogą one mieć różne rozszerzenia, na przykład .txt, lub nie mieć żadnego rozszerzenia. Pliki BINARY są programami lub plikami innymi niż tekstowe, zapisanymi w formacie aplikacji, w której zostały stworzone, albo formatami plików zarchiwizowanych lub skompresowanych.

Podczas przesyłania danych binarnych do istniejącego pliku systemu i5/OS jest stosowana długość rekordu istniejącego pliku systemu i5/OS. Na przykład wielkość istniejącego pliku powinna być wystarczająca, aby pomieścić nowe dane. Jeśli taki zbiór nie istnieje w systemie, długość rekordu zostanie określona przez protokół FTP.

Niektóre zbiory, na przykład zbiory składowania, wymagają przesyłania obrazu binarnego. Jeśli podczas próby przesyłania takich zbiorów nie zostanie wybrany tryb (TYPE) binarny, wyświetli się komunikat mówiący o konieczności zmiany trybu.

Pojęcia pokrewne

“Metody przesyłania danych” na stronie 133
Przed rozpoczęciem przesyłania plików należy wybrać właściwy format ich przesyłania. Można użyć domyślnego formatu ASCII lub podać inny format, na przykład EBDCIC lub BINARY.

Odsyłacze pokrewne

“Scenariusz: przesyłanie pliku ze zdalnego hosta” na stronie 1
Ten scenariusz opisuje, jak za pomocą podstawowych funkcji protokołu FTP pobrać pliki ze zdalnego hosta. W tym scenariuszu klient i serwer są systemami używającymi protokołu FTP i5/OS.

“ASCII (Zmiana typu pliku na ASCII - Change File Type to ASCII)” na stronie 63
Podkomenda ASCII klienta FTP i5/OS służy doustawiania typu przesyłania plików na format ASCII.

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

CCC (Kanał komendy usuwania zawartości - Clear Command Channel)

Podkomenda CCC klienta FTP i5/OS służy do zmiany trybu transmisji danych przez połączenie sterujące z trybu zaszyfrowanego na tryb jawnego tekstu.

Podkomenda klienta FTP

CCC

Protokół FTP obsługuje dwa rodzaje trybów przesyłania: tryb jawnego tekstu i tryb zaszyfrowany. W przypadku korzystania z trybu jawnego tekstu dla połączenia sterującego FTP istnieje ryzyko ujawnienia intruzowi poufnych informacji. Jeśli jest używany tryb zaszyfrowany, zapora firewall nie jest w stanie monitorować informacji wysyłanych przez połączenie sterujące FTP ani ich zmienić. W związku z tym nie może wykonywać pewnych funkcji, jak na przykład translacja adresu sieciowego.

Podkomenda CCC (Kanał komendy usuwania zawartości - Clear Command Channel) zmienia tryb transmisji danych przez połączenie sterujące z trybu zaszyfrowanego na tryb jawnego tekstu. Pozwala to zabezpieczyć poufne informacje, w tym nazwę użytkownika i hasło, przez wysłanie ich w trybie zaszyfrowanym. Następnie przy użyciu podkomendy CCC można zmienić tryb przesyłania na tryb jawnego tekstu i wysłać informacje o porcie i adresie IP.

Uwaga:

> Po wykonaniu podkomendy CCC wszystkie informacje przesyłane przez połączenie sterujące są wysyłane w trybie jawnego tekstu. Jeśli nazwy plików lub katalogów w systemie zawierają poufne informacje, należy pamiętać, że wszystkie nazwy wysyłane przez połączenie sterujące po uruchomieniu podkomendy CCC nie są zabezpieczone. Podkomenda ta nie ma jednak wpływu na tryb przesyłania połączenia danych, dzięki czemu przesyłanie danych po wykonaniu tej komendy jest nadal chronione.

Klienci mogą zezwalać lub nie zezwalać poszczególnym użytkownikom na korzystanie z podkomendy CCC, udzielając uprawnienia prywatnego do QIBM_QTMF_CLIENT_REQ_10 za pomocą funkcji Administrowanie aplikacjami programu System i Navigator lub komendy Zmiana użycia funkcji (Change Function Usage - CHGFCNUSG), na przykład:

```
CHGFCNUSG FCNID(QIBM_QTMF_CLIENT_CCC) USER(user) USAGE(*ALLOWED)
```

Odsyłacze pokrewne

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

Informacje pokrewne

Zabezpieczanie protokołu FTP za pomocą protokołu TLS

CD (Zmiana katalogu roboczego lub biblioteki - Change Working Directory or Library)

Podkomenda CD klienta FTP i5/OS służy do zmiany katalogu roboczego, biblioteki lub grupy plików w systemie zdalnym.

Podkomenda klienta FTP

CD *katalog*

katalog

> Nazwa znajdujących się w systemie zdalnym: katalogu plików, biblioteki lub specyfikatora grupy plików zależnych od systemu.
>
> Jeśli systemem zdalnym jest produkt System i, podkomenda ta zmienia bieżącą bibliotekę lub bieżący katalog. Aby sprawdzić, jakie katalogi znajdują się w systemie zdalnym, należy użyć komendy DIR. Spowoduje ona wyświetlenie listy katalogów.

Komendy DIR należy używać ostrożnie.

Uwaga: Używając podkomendy CD (lub LCD) w celu zmiany jednego systemu plików i5/OS na inny system, należy podać katalog główny systemu plików, który zawiera nowy katalog bieżący.

Odsyłacze pokrewne

"DIR (Wyświetlenie listy pozycji katalogu, bibliotek lub plików - List Directory Entries, Libraries, or Files)" na stronie 68
Podkomenda DIR klienta FTP i5/OS służy do wyświetlania bibliotek i ich zawartości lub listy katalogów i pozycji katalogów w systemie zdalnym.

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

"LS (Wyświetlenie nazw plików zdalnych - List Remote File Names)" na stronie 74
Podkomenda LS klienta FTP i5/OS służy do wyświetlania listy nazw plików w zestawie plików w systemie zdalnym.

"Nazwy plików dla podkomend klienta służących do przesyłania danych" na stronie 148
W przypadku niektórych podkomend można używać domyślnych nazw plików źródłowych i docelowych; należy jednak określić nazwę pliku dla pozostałych podkomend.

"Nazwy plików do przesyłania" na stronie 150
Podkomendy klienta FTP używane do przesyłania danych mogą zawierać parametr **plik_lokalny**, **plik_zdalny** lub oba te parametry. Można ich użyć do nazwania danych, które mają być przesłane.

CLOSE (Zamknięcie sesji FTP z systemem zdalnym - End an FTP Session with the Remote System)

Podkomenda CLOSE klienta FTP i5/OS służy do kończenia sesji z systemem zdalnym i utrzymywania aktywnego klienta FTP w systemie lokalnym.

Podkomenda klienta FTP

CLose

Komenda CLOSE umożliwia zachowanie otwartego środowiska FTP po zamknięciu sesji z systemem zdalnym. Ma to na celu nawiązanie nowej sesji z innym systemem. Aby nawiązać nowe połączenie z tym samym lub innym systemem zdalnym, należy użyć komendy OPEN. W celu zakończenia działania usługi FTP i powrotu do środowiska System i, z którego została uruchomiona, należy użyć podkomendy QUIT.

Odsyłacze pokrewne

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

DEBUG (Włączenie śledzenia klienta i kontroli wyświetlania komend serwera wysłanych do systemu zdalnego - Create Client Trace and Control Display of Server Subcommands Sent to Remote System)

Podkomenda DEBUG klienta FTP i5/OS służy do włączania lub wyłączania debugowania.

Uwaga: Śledzenie klienta FTP powinno być używane tylko w celu raportowania firmie IBM problemów z oprogramowaniem. Użycie tej funkcji może wpłynąć na wydajność systemu.

Podkomenda klienta FTP

Podkomenda DEBUG klienta FTP tworzy zapis śledzenia klienta FTP lub wyświetla jego podkomendy. Komenda DEBUG przełącza tryb debugowania. Jeśli klient poda opcjonalną wartość debugowania, zostanie ona użyta do ustawienia poziomu debugowania. Gdy tryb ten jest włączony, komendy klienta poprzedzane są na ekranie łańcuchem znaków ″>>>″. Aby włączyć śledzenie klienta FTP, parametr trybu debugowania należy ustawić na wartość 100.

DEBug [wartość_debugowania]

wartość debugowania
Jeśli wartość ta wynosi 0, debugowanie jest wyłączone. Jeśli wartość debugowania jest dodatnią liczbą całkowitą, debugowanie jest włączone. Jeśli wartość ta nie zostanie podana, debugowanie jest przełączane z wartości zero na jeden lub z wartości dodatniej na zero.

100 Włącza tworzenie zapisu aktywności klienta FTP. Klient zapisuje wyniki debugowania, dopóki wartość DEBUG nie zostanie zmieniona lub działanie klienta nie zostanie zakończone przez serwer FTP. Formatowanie wyników po zakończeniu śledzenia przez serwer FTP może zająć dużo czasu.

Aby śledzenie rozpoczęło się w momencie uruchomienia klienta FTP, w bibliotece QTEMP należy utworzyć obszar danych QTMFTPD100 za pomocą następującej komendy:

```
CRTDTAARA DTAARA(QTEMP/QTMFTPD100)
TYPE(*LGL) AUT(*USE)
```

Jeśli obszar danych QTMFTPD100 istnieje, wówczas klient zmieni wartość debugowania na 100 i uruchomi śledzenie klienta FTP. Zadaniem tej opcji jest włączenie śledzenia klienta FTP w sytuacjach, gdy śledzenie to *nie może* być włączone za pomocą komendy DEBUG 100.

Odsyłacze pokrewne

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

DEBUG (Zmiana wartości limitu czasu oczekiwania dla klienta - Change Client Time-Out Limit Values)

Podkomenda DEBUG klienta FTP i5/OS służy do zmiany limitów czasu klienta, jeśli domyślne wartości limitu czasu są niewystarczające, aby przesyłanie danych zakończyło się pomyślnie. Wartości te należy zmieniać jedynie wtedy, gdy ruch w sieci lub inne warunki spowodują znaczne wydłużenie czasu przesyłania.

Podkomenda klienta FTP

DEBug T1 | T2 [wartość]

T1 Zmiana lub wyświetlenie limitu czasu odczytu odpowiedzi serwera. Jeśli klient FTP nie otrzyma oczekiwanej odpowiedzi serwera w określonym czasie, klient zamknie połączenie sterujące z serwerem.

T2 Zmiana lub wyświetlenie limitu czasu oczekiwania na przesyłanie danych serwera dla klienta FTP. Jeśli klient FTP nie otrzyma oczekiwanej odpowiedzi połączenia danych w określonym czasie, klient zamyka połączenie danych z serwerem.

wartość
Limit czasu oczekiwania w sekundach. Wartość ta musi być liczbą dodatnią, większą niż zero. Gdy wartość ta nie zostanie podana, klient wyświetli bieżącą wartość limitu czasu oczekiwania.

Na przykład:

```
DEBUG  T1 900
```

Wartość ta ustawia limit czasu oczekiwania na odpowiedź serwera na 900 sekund.

Odsyłacze pokrewne

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

"Nazwy plików dla podkomend klienta służących do przesyłania danych" na stronie 148
W przypadku niektórych podkomend można używać domyślnych nazw plików źródłowych i docelowych; należy jednak określić nazwę pliku dla pozostałych podkomend.

DELETE (Usunięcie pliku z systemu zdalnego - Delete a File on a Remote System)

Podkomenda DELETE klienta FTP i5/OS służy do usuwania zbioru lub podzbioru zbioru bazy danych w systemie zdalnym. System zdalny może zażądać uprawnień do usunięcia pliku. W celu wysłania odpowiedzi na to żądanie należy użyć podkomendy ACCT (Wysłanie informacji o koncie - Send Account Information).

Podkomenda klienta FTP

DELete *plik_zdalny*

plik_zdalny

Plik, który ma być usunięty z systemu zdalnego.

Odsyłacze pokrewne

"NAMEFMT (Wybranie formatu nazw plików - Select File Naming Format)" na stronie 79
Podkomenda NAMEFMT klienta FTP i5/OS służy do wybierania formatu nazw plików, który będzie używany w systemie lokalnym i zdalnym.

"ACCT (Wysłanie informacji o koncie - Send Account Information)" na stronie 62
Wiele systemów przed udostępnieniem niektórych funkcji systemu wymaga podania informacji o koncie. System zdalny żąda podania tych informacji. Podkomenda ACCT klienta FTP i5/OS służy do wysyłania do systemu zdalnego informacji o koncie użytkownika.

"MDELETE (Usunięcie wielu plików w systemie zdalnym - Delete Multiple Files on a Remote System)" na stronie 75
Podkomenda MDELETE klienta FTP i5/OS służy do usuwania wielu plików z serwera FTP.

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

"Nazwy plików dla podkomend klienta służących do przesyłania danych" na stronie 148
W przypadku niektórych podkomend można używać domyślnych nazw plików źródłowych i docelowych; należy jednak określić nazwę pliku dla pozostałych podkomend.

"Nazwy plików do przesyłania" na stronie 150
Podkomendy klienta FTP używane do przesyłania danych mogą zawierać parametr **plik_lokalny**, **plik_zdalny** lub oba te parametry. Można ich użyć do nazwania danych, które mają być przesłane.

DIR (Wyświetlenie listy pozycji katalogu, bibliotek lub plików - List Directory Entries, Libraries, or Files)

Podkomenda DIR klienta FTP i5/OS służy do wyświetlania bibliotek i ich zawartości lub listy katalogów i pozycji katalogów w systemie zdalnym.

Podkomenda klienta FTP

DIr [*nazwa*] [(Disk]

name (nazwa)

Nazwa katalogu lub biblioteki. Domyślną wartością jest cały bieżący katalog lub biblioteka. Aby dany katalog lub biblioteka stały się bieżącymi, należy użyć komendy Katalog roboczy (Working Directory - CD). Sposób podawania zestawu plików zdalnych zależy od systemu. W większości systemów jest dozwolone używanie symbolu gwiazdki (*). Jeśli na przykład systemem zdalnym jest produkt System i, podkomenda DIR MYLIB/MYFILE.* spowoduje utworzenie listy wszystkich podzbiorów zbioru MYFILE w bibliotece MYLIB.

Istnieją dwa dopuszczalne formaty nazw plików, których można używać. W powyższym przykładzie użyto formatu NAMEFMT 0. Więcej informacji o nazewnictwie plików FTP zawiera sekcja “NAMEFMT (Wybranie formatu nazw plików - Select File Naming Format)” na stronie 79.

(Disk Zapisuje wynik działania komendy DIR w pliku * CURLIB/DIROUTPUT.DIROUTPUT. Wynik ten nie jest wyświetlany na ekranie.

Jeśli systemem zdalnym jest produkt System i, informacje te obejmują:

- dla zbiorów baz danych, obiekty *FILE i ich podzbiory,
- dla plików hierarchicznego systemu plików (HFS):
  - Wszystkie foldery usług biblioteki dokumentów (QDLS) i ich zawartość, czyli inne foldery lub dokumenty.
  - Wszystkie woluminy optyczne (QOPT) i ich zawartość, czyli katalogi lub pliki.

Komendy DIR należy używać ostrożnie. Jeśli komenda DIR zostanie podana bez parametrów, serwer utworzy listing wszystkich plików znajdujących się w bieżącym katalogu. Lista ta może być znacznie dłuższa niż użytkownik oczekuje.

Aby uzyskać listę nazw plików znajdujących się w danym katalogu, należy użyć podkomendy List (LS).

Odsyłacze pokrewne

“CD (Zmiana katalogu roboczego lub biblioteki - Change Working Directory or Library)” na stronie 65
Podkomenda CD klienta FTP i5/OS służy do zmiany katalogu roboczego, biblioteki lub grupy plików w systemie zdalnym.

“LS (Wyświetlenie nazw plików zdalnych - List Remote File Names)” na stronie 74
Podkomenda LS klienta FTP i5/OS służy do wyświetlania listy nazw plików w zestawie plików w systemie zdalnym.

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

EBCDIC (Zmiana typu pliku na EBCDIC - Change File Type to EBCDIC)

Podkomenda EBCDIC klienta FTP i5/OS służy do ustawiania typu przesyłania plików na format EBCDIC. Typ przesyłania EBCDIC jest przydatny podczas przesyłania plików do lub z innego systemu EBCDIC, ponieważ pozwala uniknąć konwersji między formatami ASCII i EBCDIC w obu systemach.

Podkomenda klienta FTP

EBcdic

Pojęcia pokrewne

“Metody przesyłania danych” na stronie 133
Przed rozpoczęciem przesyłania plików należy wybrać właściwy format ich przesyłania. Można użyć domyślnego formatu ASCII lub podać inny format, na przykład EBDCIC lub BINARY.

Odsyłacze pokrewne

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

GET (Kopiowanie pliku z systemu zdalnego do lokalnego - Copy a File from a Remote System to the Local System)

Podkomenda GET klienta FTP i5/OS służy do kopiowania pliku z systemu zdalnego do systemu lokalnego.

Podkomenda klienta FTP

Get *Plik_zdalny* [*plik_lokalny*]
[(Replace]

plik_zdalny
Plik, który ma być pobrany z systemu zdalnego.

plik_lokalny
Podzbiór zbioru lokalnego, dokument lub inny plik, który ma być utworzony. Jeśli nazwa pliku lokalnego nie zostanie podana, klient FTP przyjmie nazwę domyślną. Więcej informacji o nazwach domyślnych zawiera sekcja Domyślne nazwy plików dla podkomend klienta służących do przesyłania danych.

(Replace
Jeśli plik o podanej nazwie już istnieje, opcja ta powoduje nadpisanie pliku lokalnego. Serwer nie zastąpi pliku lokalnego, jeśli nie zostanie określona opcja (Replace.

System plików, w którym znajduje się dany plik, określa format nazewnictwa plików, który ma być użyty dla komendy GET.

- Jeśli plik nie znajduje się w systemie plików bibliotek (QSYS.LIB), komendy GET należy użyć w formacie nazewnictwa (NAMEFMT) 1:

  ```
  GET /QDLS/QIWSOS2/PCSMENU.EXE
  ```

- Jeśli plik znajduje się w systemie plików bibliotek, należy użyć komendy GET i formatu nazewnictwa (NAMEFMT) z wartością 0.

  ```
  GET BIBL/ZB.PODZB (REPLACE
  ```

  Przyjmując, że systemem zdalnym jest produkt System i, ta komenda pobiera podzbiór YOURMBR zbioru YOURFILE z biblioteki YOURLIB i umieszcza go w podzbiorze YOURMBR zbioru YOURFILE w bieżącym katalogu w systemie lokalnym.

Uwaga: Jeśli nazwa pliku zdalnego wymaga użycia apostrofów jako części nazwy pliku, nazwa pliku powinna być ujęta w dodatkowe dwa apostrofy. W poniższym przykładzie podzbiór "PODZB.PIERW" został pobrany ze zdalnego hosta.

```
GET BIBL/ZB.PODZB 'PODZB.PIERW'
```

Zadania pokrewne

“Ujmowanie parametrów podkomend w cudzysłowy lub apostrofy” na stronie 147
Parametry podkomend można ująć w znaki apostrofu (’) lub cudzysłowu (″).

Odsyłacze pokrewne

“Nazwy plików dla podkomend klienta służących do przesyłania danych” na stronie 148
W przypadku niektórych podkomend można używać domyślnych nazw plików źródłowych i docelowych; należy jednak określić nazwę pliku dla pozostałych podkomend.

“LCD (Zmiana biblioteki roboczej lub katalogu w systemie lokalnym - Change Working Library or Directory on Local System)” na stronie 72
Podkomenda LCD klienta FTP i5/OS służy do zmiany katalogu roboczego w systemie lokalnym.

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

“MGET (Kopiowanie wielu plików z systemu zdalnego do systemu lokalnego - Copy Multiple Files from a Remote System to the Local System)” na stronie 76
Podkomenda MGET klienta FTP i5/OS służy do kopiowania wielu plików z systemu zdalnego.

“PUT (Kopiowanie podzbioru zbioru z systemu lokalnego do pliku w systemie zdalnym - Copy a File Member from the Local System to a File on a Remote System)” na stronie 81
Podkomenda PUT klienta FTP i5/OS służy do kopiowania lokalnego podzbioru zbioru do systemu zdalnego.

"MPUT (Wysłanie wielu podzbiorów z systemu lokalnego do systemu zdalnego - Send Multiple File Members from the Local System to a Remote System)" na stronie 78
Podkomenda MPUT klienta FTP i5/OS służy do kopiowania wielu plików do systemu zdalnego.

"Nazwy plików do przesyłania" na stronie 150
Podkomendy klienta FTP używane do przesyłania danych mogą zawierać parametr **plik_lokalny**, **plik_zdalny** lub oba te parametry. Można ich użyć do nazwania danych, które mają być przesłane.

HELP (Uzyskiwanie pomocy dla komend FTP - Getting Help for FTP Subcommands)

Podkomenda HELP klienta FTP i5/OS służy do uzyskiwania informacji o podkomendach FTP używanych przez system lokalny i system zdalny.

Pomoc dotycząca podkomend klienta FTP

Aby uzyskać informacje o komendach FTP używanych przez system lokalny, należy użyć komendy HELP w następującym formacie:

```
Help [* | ALL | komenda ]
```

*** lub ALL**
Powodują wyświetlenie listy komend klienta FTP.

podkomenda
Powoduje wyświetlenie szczegółowych informacji o danej komendzie klienta. Na przykład HELP GET wyświetli informacje o sposobie przesyłania plików z systemu zdalnego do systemu lokalnego. Większości komend można używać w skróconych formach.

Użycie komendy HELP bez parametru spowoduje wyświetlenie listy komend i ogólny opis dostępnych informacji pomocy. Pomoc kontekstowa wyświetlana jest po umieszczeniu kursora na nazwie komendy na ekranie pomocy i naciśnięciu klawisza Enter.

Aby uzyskać listę lokalnych podkomend w systemie, należy wpisać następującą komendę:

```
HELP
```

Informacje pomocy można uzyskać korzystając z komendy ? .

Pomoc dotycząca podkomend serwera FTP

Aby uzyskać informacje o komendach FTP systemu zdalnego, należy użyć komendy HELP w następującym formacie:

```
Help SERVER [podkomenda]
```

SERVER
Powoduje wyświetlenie informacji pomocy udostępnianych przez system zdalny dla komend serwera FTP. Działanie tego parametru jest podobne do działania komendy QUOTE z parametrem HELP. QUOTE HELP wyświetla listę komend FTP obsługiwanych przez system zdalny.

podkomenda
Nazwa komendy serwera, dla której mają być wyświetlone informacje. Na przykład komenda HELP SERVER STOR zażąda od serwera udostępnienia informacji o komendzie STOR.

Uwaga: RHELP jest synonimem komendy HELP SERVER. Na przykład komendy HELP SERVER SITE i RHELP SITE są tożsame.

Odsyłacze pokrewne

"QUOTE (Wysłanie komendy do serwera FTP - Send a Subcommand to an FTP Server)" na stronie 83
Podkomenda QUOTE klienta FTP i5/OS służy do wysyłania podkomendy do serwera FTP.

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

LCD (Zmiana biblioteki roboczej lub katalogu w systemie lokalnym - Change Working Library or Directory on Local System)

Podkomenda LCD klienta FTP i5/OS służy do zmiany katalogu roboczego w systemie lokalnym.

Podkomenda klienta FTP

```
LCd nazwa_ścieżki
```

nazwa_ścieżki
Nazwa biblioteki, folderu lub katalogu w systemie lokalnym.

Uwagi:

1. Komenda LCD nie zmienia na liście bibliotek pozycji biblioteki bieżącej.
2. Używając podkomendy CD (lub LCD) w celu zmiany jednego systemu plików na inny, należy podać katalog główny, na przykład /QDLS lub /QOP.

Odsyłacze pokrewne

"GET (Kopiowanie pliku z systemu zdalnego do lokalnego - Copy a File from a Remote System to the Local System)" na stronie 69
Podkomenda GET klienta FTP i5/OS służy do kopiowania pliku z systemu zdalnego do systemu lokalnego.

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

"Nazwy plików dla podkomend klienta służących do przesyłania danych" na stronie 148
W przypadku niektórych podkomend można używać domyślnych nazw plików źródłowych i docelowych; należy jednak określić nazwę pliku dla pozostałych podkomend.

"Nazwy plików do przesyłania" na stronie 150
Podkomendy klienta FTP używane do przesyłania danych mogą zawierać parametr **plik_lokalny**, **plik_zdalny** lub oba te parametry. Można ich użyć do nazwania danych, które mają być przesłane.

LOCSITE (Podanie informacji o środowisku lokalnym - Specify Local Site Information)

Podkomenda LOCSITE klienta FTP i5/OS służy do określania informacji wykorzystywanych przez klienta FTP do udostępniania usług właściwych dla systemu klienta.

Podkomenda klienta FTP

```
LOCSITE [ parametry ]
```

Klient FTP i5/OS obsługuje następujące parametry i opcje parametrów podkomendy LOCSITE:

CRTCCSID *CALC
Nowe zbiory baz danych utworzone w trakcie przesyłania plików ASCII używają odpowiedniego domyślnego identyfikatora CCSID EBCDIC jako identyfikatora CCSID przesyłania plików ASCII. Jest to wartość domyślna.

CRTCCSID *USER
Nowe zbiory baz danych tworzone podczas przesyłania plików ASCII używają identyfikatora CCSID bieżącego zadania. Jeśli jednak jest to identyfikator CCSID 65535, domyślny CCSID określany jest przez identyfikator języka w bieżącej specyfikacji zadania.

CRTCCSID *SYSVAL
Nowe zbiory baz danych tworzone podczas przesyłania plików ASCII używają identyfikatora CCSID pobranego z wartości systemowej QCCSID.

CRTCCSID [numer_CCSID]
Określa identyfikator CCSID, który ma być używany podczas tworzenia zbiorów baz danych podczas przesyłania plików ASCII. Serwer FTP sprawdza poprawność podanej wartości.

CRTCCSID
Wyświetlenie komunikatu, który zawiera aktualne ustawienia CRTCCSID klienta FTP.

TRIM 0
Ustawienie opcji Trim na OFF (Wyłączone). Serwer FTP wysyła końcowe odstępy rekordów bazy danych.

TRIM 1
Ustawienie opcji Trim na ON (Włączone). Serwer FTP nie wysyła końcowych odstępów rekordów bazy danych podczas przesyłania zbiorów bazy danych, które używają struktury zbiorów i trybu strumieniowego. Jest to wartość domyślna.

TRIM 2
Zmiana opcji Trim powodująca, że dla każdego przesyłania (w tym za pomocą struktury rekordów i trybu blokowego), serwer nie wysyła odstępów na końcu rekordów bazy danych.

TRIM Wyświetlenie komunikatu, który zawiera aktualne ustawienia opcji TRIM klienta FTP.

Uwagi:

1. Zanim komenda ta została udostępniona, przed przesłaniem pliku do serwera FTP końcowe odstępy rekordów systemu plików QSYS.LIB były zawsze usuwane.
2. Ustawienia TRIM nie dotyczą binarnego przesyłania plików (TYPE I). Podczas przesyłania plików binarnych (TYPE I), bez względu na ustawienia opcji TRIM, odstępy nigdy nie są usuwane.

DTAPROT C
Ustawienie zmiennej ochrony danych na C (Jawne). Ta zmienna jest używana do ustawiania poziomu ochrony danych podczas otwierania chronionego połączenia sterującego. Więcej szczegółów na temat ustawiania ochrony danych znajduje się w sekcjach opisujących komendy SECDATA i SECOPEN.

DTAPROT P
Ustawienie zmiennej ochrony danych na P (Poufne). Ta zmienna jest używana do ustawiania poziomu ochrony danych podczas otwierania chronionego połączenia sterującego.

DTAPROT
Wyświetlenie komunikatu, który zawiera bieżącą wartość zmiennej ochrony danych.

Odsyłacze pokrewne

“SECData (Konfigurowanie ochrony danych - Setting data security protection)” na stronie 85
Podkomenda SECData klienta FTP i5/OS służy do określania poziomu ochrony, który ma być stosowany dla połączeń danych, gdy z systemem zdalnym jest już nawiązane chronione połączenie sterujące.

“SECOpen (Konfigurowanie ochrony danych - Setting data security protection)” na stronie 86
Podkomenda SECOPEN klienta FTP i5/OS służy do otwierania chronionego połączenia sterującego z serwerem FTP przy użyciu określonej opcji ochrony.

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

LOCSTAT (Wyświetlenie informacji o statusie lokalnym - Display Local Status Information)

Podkomenda LOCSTAT klienta FTP i5/OS służy do wyświetlania informacji o statusie lokalnym.

Podkomenda klienta FTP

LOCSTat

Komenda ta powoduje wyświetlenie takich informacji o statusie lokalnym, jak:

- aktualne ustawienia komendy SENDSITE,
- aktualne ustawienia komendy SENDPORT,
- nazwa systemu zdalnego, numer portu i status zalogowania,
- typ danych i tryb przesyłania,
- wartość formatu nazwy dla klienta i dla serwera,
- ustawienia trybu VERBOSE,
- ustawienia trybu DEBUG.

Odsyłacze pokrewne

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

LS (Wyświetlenie nazw plików zdalnych - List Remote File Names)

Podkomenda LS klienta FTP i5/OS służy do wyświetlania listy nazw plików w zestawie plików w systemie zdalnym.

Podkomenda klienta FTP

LS [*nazwa*] [(Disk]

name (nazwa)
Nazwa zdalnego katalogu, pliku lub biblioteki, która ma zostać wyświetlona. Jeśli systemem zdalnym jest produkt System i, serwer FTP wyświetla listę nazw zbiorów i ich podzbiorów. Wartością domyślną jest wyświetlenie listy całego bieżącego katalogu, biblioteki lub folderu. Aby zmienić bieżący katalog, bibliotekę lub folder, należy użyć komendy CD. Specyfikacja zdalnego pliku zależy od systemu.

(Disk Zapisuje wynik wydania komendy LS w zbiorze * CURLIB/LSOUTPUT.LSOUTPUT. Wynik ten nie jest wyświetlany na ekranie. Za każdym razem, gdy zostanie podany parametr (Disk i ta sama wartość *CURLIB, serwer FTP zmienia zawartość podzbioru zbioru LSOUTPUT.LSOUTPUT.

Uwaga: Jeśli serwer FTP zwróci kod odpowiedzi negatywnej (550), nie zostanie utworzony żaden podzbiór LSOUTPUT. Jeśli serwer FTP zwróci kod odpowiedzi pozytywnej (150) bez nazw plików, utworzony zostanie podzbiór LSOUTPUT nie zawierający żadnych rekordów.

Komenda LS powoduje wyświetlenie samych nazw plików. Aby uzyskać listę wszystkich pozycji katalogu z dodatkowymi informacjami o plikach, należy zapoznać się z informacjami zawartymi w sekcji “DIR (Wyświetlenie listy pozycji katalogu, bibliotek lub plików - List Directory Entries, Libraries, or Files)” na stronie 68.

Odsyłacze pokrewne

“DIR (Wyświetlenie listy pozycji katalogu, bibliotek lub plików - List Directory Entries, Libraries, or Files)” na stronie 68
Podkomenda DIR klienta FTP i5/OS służy do wyświetlania bibliotek i ich zawartości lub listy katalogów i pozycji katalogów w systemie zdalnym.

"CD (Zmiana katalogu roboczego lub biblioteki - Change Working Directory or Library)" na stronie 65
Podkomenda CD klienta FTP i5/OS służy do zmiany katalogu roboczego, biblioteki lub grupy plików w systemie zdalnym.

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

LTYPE (Typ lokalny - Local Type)

Podkomenda LTYPE klienta FTP i5/OS służy do określania typu przesyłania plików lub reprezentacji, w jakiej odbywa się przesyłanie w systemie lokalnym.

Podkomenda klienta FTP

LType C nr_ccsid

C Typ identyfikatora CCSID. Należy wpisać C.

nr_ccsid
Wartość identyfikatora CCSID. Należy wpisać CCSID z zakresu 1-65533.

Uwaga: Podkomenda LTYPE jest podobna do podkomendy TYPE. Komenda LTYPE zmienia jedynie typ reprezentacji znaków po stronie klienta. Podkomenda TYPE zmienia typ reprezentacji znaków klienta i serwera.

Odsyłacze pokrewne

"TYPE (Określenie typu przesyłania plików - Specify File Transfer Type)" na stronie 92
Podkomenda TYPE klienta FTP i5/OS służy do określania typu przesyłania plików lub reprezentacji, w jakiej odbywa się przesyłanie.

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

MDELETE (Usunięcie wielu plików w systemie zdalnym - Delete Multiple Files on a Remote System)

Podkomenda MDELETE klienta FTP i5/OS służy do usuwania wielu plików z serwera FTP.

Podkomenda klienta FTP

MDelete {*plik_zdalny* [*plik_zdalny...*]}

plik_zdalny
Pliki, które mają być usunięte z serwera FTP.

Uwaga: Jeśli zbiór zdalny jest zbiorem QSYS.LIB, serwer FTP usuwa wszystkie podzbiory zbioru fizycznego. Sam zbiór nie jest usuwany.

Przykładowy system plików biblioteki w formacie NAMEFMT 0 jest następujący:

```
MDELETE MYLIB/FILE1.MBRA YOURLIB/FILE2.MBRB
```

W przykładzie tym jest usuwany podzbiór MBRA zbioru FILE1 w bibliotece MYLIB oraz podzbiór MBRB zbioru FILE2 w bibliotece YOURLIB w systemie zdalnym. Ten sam przykład dla formatu NAMEFMT 1:

```
MDELETE /QSYS.LIB/BIBLM.LIB/ZB1.FILE/PODZBA.MBR
/QSYS.LIB/BIBLT.LIB/ZB2.FILE./PODZBB.MBR
```

Przykładowy system biblioteki dokumentów w formacie NAMEFMT 1 jest następujący:

```
MDELETE /QDLS/QIWSOS2/PCSMENU.EXE /QDLS/PCSDIR/PCSFILE.EXE
```

W przykładzie tym jest usuwany dokument PCSMENU.EXE w folderze QIWSOS2 w bibliotece usług biblioteki dokumentów oraz PCSFILE.EXE w folderze PCSDIR w bibliotece QDLS.

Aby usunąć wiele plików, można użyć znaku gwiazdki (*). Jeśli system zdalnym jest produkt System i i jest używany format NAMEFMT 0, można wpisać na przykład:

```
MDELETE BIBL/ZB.*
```

W przykładzie tym usunięte zostałyby wszystkie podzbiory zbioru ZB w bibliotece BIBL. Użycie gwiazdki dopuszczalne jest jedynie na końcu łańcucha znaków.

Odsyłacze pokrewne

"DELETE (Usunięcie pliku z systemu zdalnego - Delete a File on a Remote System)" na stronie 68
Podkomenda DELETE klienta FTP i5/OS służy do usuwania zbioru lub podzbioru zbioru bazy danych w systemie zdalnym. System zdalny może zażądać uprawnień do usunięcia pliku. W celu wysłania odpowiedzi na to żądanie należy użyć podkomendy ACCT (Wysłanie informacji o koncie - Send Account Information).

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

"Nazwy plików dla podkomend klienta służących do przesyłania danych" na stronie 148
W przypadku niektórych podkomend można używać domyślnych nazw plików źródłowych i docelowych; należy jednak określić nazwę pliku dla pozostałych podkomend.

"Nazwy plików do przesyłania" na stronie 150
Podkomendy klienta FTP używane do przesyłania danych mogą zawierać parametr **plik_lokalny**, **plik_zdalny** lub oba te parametry. Można ich użyć do nazwania danych, które mają być przesłane.

MGET (Kopiowanie wielu plików z systemu zdalnego do systemu lokalnego - Copy Multiple Files from a Remote System to the Local System)

Podkomenda MGET klienta FTP i5/OS służy do kopiowania wielu plików z systemu zdalnego.

Podkomenda klienta FTP

Przekazywanie plików za pomocą komendy MGET:

Po wpisaniu podkomendy MGET dla każdego przesyłanego pliku zdalnego jest wykonywana osobna podkomenda GET. Serwer FTP automatycznie tworzy nazwę odpowiedniego pliku lokalnego zgodnie z regułami nadawania nazw domyślnych.

Komenda MGET klienta FTP do określenia miejsca, do którego mają być skopiowane pliki, wykorzystuje następujący proces:

- komenda MGET zawsze umieszcza pliki w bieżącej bibliotece lub bieżącym katalogu,
- jeśli użytkownik wydał komendę LCD, serwer FTP używa bieżącej biblioteki lub bieżącego katalogu,
- jeśli użytkownik nie wydał komendy LCD, serwer FTP ustawia katalog bieżący w następujący sposób:
  - jeśli zadanie użytkownika ma ustawioną bieżącą bibliotekę, biblioteka ta jest przyjmowana dla FTP jako bieżący katalog,
  - jeśli zadanie użytkownika nie ma ustawionej biblioteki bieżącej, serwer FTP używa QPGL jako katalogu bieżącego.

```
MGet {plik_zdalny
[plik_zdalny...]}[(Replace]
```

plik_zdalny
Plik lub pliki, które mają być pobrane z systemu zdalnego.

(Replace

Powoduje nadpisanie istniejącego pliku w systemie lokalnym. Jeśli dany plik istnieje już w systemie lokalnym i nie użyto opcji Replace, istniejący plik nie jest zastępowany. Nazwa pliku lokalnego, do którego kopiowany jest plik zdalny, tworzona jest automatycznie.

Aby skopiować wszystkie podzbiory do bieżącej biblioteki lub katalogu można użyć znaku gwiazdki (*). Jeśli systemem zdalnym jest produkt System i, można zastosować następujące przykłady:

- MGET BIBL/ZB. * spowoduje skopiowanie wszystkich podzbiorów zbioru ZB zawartego w bibliotece BIBL systemu zdalnego do bieżącej biblioteki systemu lokalnego,
- MGET /QSYS.LIB/BIBL.LIB/ZB.FILE/ * .MBR byłaby komendą dla wersji NAMEFMT 1 tej komendy,
- MGET /QOPT/RYSUNKI/OBRAZY/. * kopiuje wszystkie pliki z katalogu OBRAZY z woluminu optycznego RYSUNKI do bieżącej biblioteki (lub katalogu) w systemie lokalnym,
- MGET ZBTEKST.A * kopiuje wszystkie podzbiory o nazwie zaczynającej się od litery A w zbiorze ZBTEKST,
- MGET /QDLS/QISSOS2/A * kopiuje wszystkie dokumenty o nazwach zaczynających się literą A w folderze QISSOS2.

Odsyłacze pokrewne

"GET (Kopiowanie pliku z systemu zdalnego do lokalnego - Copy a File from a Remote System to the Local System)" na stronie 69
Podkomenda GET klienta FTP i5/OS służy do kopiowania pliku z systemu zdalnego do systemu lokalnego.

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

"MPUT (Wysłanie wielu podzbiorów z systemu lokalnego do systemu zdalnego - Send Multiple File Members from the Local System to a Remote System)" na stronie 78
Podkomenda MPUT klienta FTP i5/OS służy do kopiowania wielu plików do systemu zdalnego.

"PUT (Kopiowanie podzbioru zbioru z systemu lokalnego do pliku w systemie zdalnym - Copy a File Member from the Local System to a File on a Remote System)" na stronie 81
Podkomenda PUT klienta FTP i5/OS służy do kopiowania lokalnego podzbioru zbioru do systemu zdalnego.

"Nazwy plików dla podkomend klienta służących do przesyłania danych" na stronie 148
W przypadku niektórych podkomend można używać domyślnych nazw plików źródłowych i docelowych; należy jednak określić nazwę pliku dla pozostałych podkomend.

"Nazwy plików do przesyłania" na stronie 150
Podkomendy klienta FTP używane do przesyłania danych mogą zawierać parametr **plik_lokalny**, **plik_zdalny** lub oba te parametry. Można ich użyć do nazwania danych, które mają być przesłane.

MKDIR (Utworzenie katalogu - Make Directory)

Podkomenda MKDIR klienta FTP i5/OS służy do tworzenia katalogu lub podkatalogu.

Podkomenda klienta FTP

```
MKdir nazwa_ścieżki
```

nazwa_ścieżki

Nazwa znajdujących się w systemie zdalnym: katalogu plików, biblioteki lub specyfikatora grupy plików zależnych od systemu.

Odsyłacze pokrewne

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

MODE (Określenie trybu przesyłania danych - Specify Transmission Mode of Data)

Podkomenda MODE serwera FTP i5/OS służy do określania formatu danych dla przesyłania plików.

Podkomenda klienta FTP

MODE [B | S]

B Tryb blokowy. W tym trybie serwer FTP przesyła dane jako serie bloków danych poprzedzonych nagłówkiem liczącym jeden lub więcej bajtów. Jeśli dane przesyłane są w trybie blokowym, typ danych musi zostać ustawiony na EBCDIC.

S Tryb strumieniowy. W trybie tym serwer FTP przesyła dane jako strumień bajtów. W trybie strumieniowym można użyć dowolnego typu reprezentacji.

Uwagi:

1. Tryb strumieniowy jest domyślnym trybem przesyłania używanym w protokole FTP. Niektóre systemy nie obsługują trybu blokowego.
2. Jeśli opcjonalny parametr zostanie pominięty, klient wyświetli wysłaną uprzednio wartość MODE.

Odsyłacze pokrewne

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

MPUT (Wysłanie wielu podzbiorów z systemu lokalnego do systemu zdalnego - Send Multiple File Members from the Local System to a Remote System)

Podkomenda MPUT klienta FTP i5/OS służy do kopiowania wielu plików do systemu zdalnego.

Podkomenda klienta FTP

Po wpisaniu podkomendy MPUT dla każdego przesyłanego pliku lokalnego klient wykonuje osobną podkomendę PUT. Nazwa odpowiedniego pliku zdalnego tworzona jest automatycznie zgodnie z regułami nadawania nazw domyślnych.

MPut {*plik_lokalny* [*plik_lokalny...*]}

plik_lokalny

Podaj jeden lub więcej podzbiorów zbioru lokalnego systemu plików bibliotek lub innego systemu plików obsługiwanego przez FTP, które mają być przesłane do systemu zdalnego. Klient automatycznie generuje nazwę nadawaną plikowi w systemie zdalnym.

Uwaga: Jeśli plik zdalny już istnieje, jego zawartość zastępowana jest zawartością *pliku_lokalnego*, chyba że włączono opcję Składowanie unikalne (Store Unique - SUNIQUE).

Informacje na temat sposobu podawania nazwy pliku, jeśli systemem zdalnym jest produkt System i, zawiera sekcja “NAMEFMT (Wybranie formatu nazw plików - Select File Naming Format)” na stronie 79.

W następującym przykładzie użyto formatu NAMEFMT 0:

```
MPUT BIBL/ZB1.PODZB1 BIBL/ZB1.PODZB2
```

W powyższym przykładzie wysyłane są do systemu zdalnego podzbiory MBR1 i MBR2 zbioru FILE1 w bibliotece MYLIB.

W następującym przykładzie użyto formatu NAMEFMT 1:

```
MPUT /QDLS/QIWSOS2/PCSMENU.EXE /QDLS/QIWSOS2/PCSMENU2.EXE
```

W powyższym przykładzie wysyłane są do systemu zdalnego dokumenty PCSMENU.EXE i PCSMENU2.EXE z folderu QIWSOS2.

Aby wysłać wszystkie podzbiory zbioru, można użyć znaku gwiazdki (*). Na przykład komenda MPUT BIBL/ZB. * powoduje wysłanie wszystkich podzbiorów zbioru ZB z biblioteki BIBL.

Odsyłacze pokrewne

"GET (Kopiowanie pliku z systemu zdalnego do lokalnego - Copy a File from a Remote System to the Local System)" na stronie 69
Podkomenda GET klienta FTP i5/OS służy do kopiowania pliku z systemu zdalnego do systemu lokalnego.

"SUNIQUE (Sterowanie nadpisywaniem plików - Control Overwriting of Files)" na stronie 90
Podkomenda SUNIQUE klienta FTP i5/OS służy do sterowania zastępowaniem plików. Podkomenda SUNIQUE jest komendą odrębną, której należy użyć przed wydaniem podkomend PUT lub MPUT.

"MGET (Kopiowanie wielu plików z systemu zdalnego do systemu lokalnego - Copy Multiple Files from a Remote System to the Local System)" na stronie 76
Podkomenda MGET klienta FTP i5/OS służy do kopiowania wielu plików z systemu zdalnego.

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

"PUT (Kopiowanie podzbioru zbioru z systemu lokalnego do pliku w systemie zdalnym - Copy a File Member from the Local System to a File on a Remote System)" na stronie 81
Podkomenda PUT klienta FTP i5/OS służy do kopiowania lokalnego podzbioru zbioru do systemu zdalnego.

"Nazwy plików dla podkomend klienta służących do przesyłania danych" na stronie 148
W przypadku niektórych podkomend można używać domyślnych nazw plików źródłowych i docelowych; należy jednak określić nazwę pliku dla pozostałych podkomend.

"Nazwy plików do przesyłania" na stronie 150
Podkomendy klienta FTP używane do przesyłania danych mogą zawierać parametr **plik_lokalny**, **plik_zdalny** lub oba te parametry. Można ich użyć do nazwania danych, które mają być przesłane.

NAMEFMT (Wybranie formatu nazw plików - Select File Naming Format)

Podkomenda NAMEFMT klienta FTP i5/OS służy do wybierania formatu nazw plików, który będzie używany w systemie lokalnym i zdalnym.

Podkomenda klienta FTP

```
NAmefmt [ 0 | 1 ]
```

0 Format nazewnictwa dopuszczalny jedynie dla zbiorów bazy danych systemu plików bibliotek. Ogólny format to:

```
[nazwa_biblioteki/]nazwa_zbioru[.nazwa_podzbioru]
```

1 Format nazewnictwa dla wszystkich systemów plików, które obsługiwane są przez FTP, w tym systemu plików bibliotek. Aby możliwa była praca ze wszystkimi systemami plików i5/OS, należy ustawić format nazwy na 1.

Zbiory systemu plików bibliotek w tym formacie nazewnictwa to:

```
[/QSYS.LIB/][nazwa_biblioteki.LIB/]nazwa_zbioru.FILE[/nazwa_podzbioru.MBR]
```

Dla zbiorów składowania można także użyć następującego formatu:

```
/QSYS.LIB/nazwa_biblioteki.LIB/nazwa_zbioru.SAVF
```

Nazwy zbiorów w systemie plików usług biblioteki dokumentacji tworzone są w następującym formacie:

```
[/QDLS/][{nazwa_folderu[.ext]/}]nazwa_zbioru[.ext]
```

Dla napędów optycznych przyjmowany jest następujący format:

```
/QOPT/nazwa_woluminu/nazwa_katalogu/nazwa_pliku.roz
```

Uwagi:

1. Format nazewnictwa może mieć wartość 0 jedynie wtedy, gdy katalog roboczy jest biblioteką bazy danych.
2. Jeśli wydana zostanie komenda NAMEFMT bez parametru, klient wyświetli bieżący format nazewnictwa.

Odsyłacze pokrewne

"APPEND (Dodanie podzbioru zbioru lokalnego do pliku zdalnego - Append a Local File Member to a Remote File)" na stronie 62
Podkomenda APPEND klienta FTP i5/OS służy do dodawania lokalnego podzbioru zbioru, dokumentu lub innego pliku systemu plików do zbioru zdalnego.

"DELETE (Usunięcie pliku z systemu zdalnego - Delete a File on a Remote System)" na stronie 68
Podkomenda DELETE klienta FTP i5/OS służy do usuwania zbioru lub podzbioru zbioru bazy danych w systemie zdalnym. System zdalny może zażądać uprawnień do usunięcia pliku. W celu wysłania odpowiedzi na to żądanie należy użyć podkomendy ACCT (Wysłanie informacji o koncie - Send Account Information).

"Systemy plików i konwencje nazewnictwa" na stronie 143
Serwer FTP organizuje jednostki informacji systemu plików w struktury wielowarstwowe, podobne do drzewa.

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

NULLFLDS (Umożliwienie przesyłania zbiorów z polami NULL -Allow Transfer of Files with NULL Fields)

Podkomenda NULLFLDS klienta FTP i5/OS służy do określania, czy w systemie lokalnym i zdalnym ma być dozwolone przesyłanie zbiorów bazy danych zawierających wartości pól NULL.

Podkomenda klienta FTP

```
NUllflds [ 0 | 1 ]
```

Podczas wpisywania tego parametru poprawne są następujące wartości:

0 Przesyłanie zbiorów bazy danych, które zawierają pola NULL, nie jest możliwe. Jest to wartość domyślna.

1 Przesyłanie zbiorów bazy danych, które zawierają pola NULL, jest możliwe.

Uwagi:

1. Przesyłanie zbiorów, które zawierają pola NULL, wymaga włączenia tego ustawienia zarówno w serwerze, jak i w kliencie. Zbiór docelowy musi istnieć zanim przesyłanie zostanie rozpoczęte. Musi on także mieć tę samą definicję zbioru, co zbiór źródłowy.
2. Wyniki przesyłania są nieprzewidywalne, jeśli zbiór zawierający pola NULL przesyłany jest do systemu, który nie jest produktem System i, lub jeśli typ przesyłania wymaga konwersji strony kodowej danych.
3. Jeśli wydana zostanie komenda NULLFLDS bez parametru, klient wyświetli bieżące ustawienia.

Odsyłacze pokrewne

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

OPEN (Połączenie z serwerem FTP w systemie zdalnym - Connect to FTP Server on a Remote System)

Podkomenda OPEN klienta FTP i5/OS służy do łączenia klienta FTP z serwerem FTP.

Podkomenda klienta FTP

Open *nazwa_systemu* [*numer_portu*]

nazwa_systemu
Nazwa lub adres internetowy systemu zdalnego.

numer_portu
Numer portu, którego ma używać dana sesja, dopóki serwer FTP nie zamknie połączenia. Wartość opcjonalna. Jeśli numer portu nie zostanie podany, serwer FTP wybierze go sam.

Gdy połączenie z systemem zdalnym zostanie otwarte, nie można połączyć się z innym systemem, zanim bieżąca sesja nie zostanie zamknięta.

Odsyłacze pokrewne

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

PASS (Wysłanie hasła - Send Your Password)

Podkomenda PASS klienta FTP i5/OS służy do wysyłania hasła użytkownika do serwera FTP.

Podkomenda klienta FTP

PASS *hasło*

hasło Łańcuch tekstu będący hasłem.

Podkomendę tę muszą poprzedzać podkomendy OPEN i USER. Dla niektórych systemów komenda ta kończy weryfikację podczas kontroli dostępu. Ta podkomenda nie jest konieczna, gdy serwer FTP wymaga wpisania hasła podczas łączenia się z serwerem FTP lub logowania się do niego.

Odsyłacze pokrewne

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

PUT (Kopiowanie podzbioru zbioru z systemu lokalnego do pliku w systemie zdalnym - Copy a File Member from the Local System to a File on a Remote System)

Podkomenda PUT klienta FTP i5/OS służy do kopiowania lokalnego podzbioru zbioru do systemu zdalnego.

Podkomenda klienta FTP

PUT *plik_lokalny* [*plik_zdalny*]

plik_lokalny
Nazwa podzbioru zbioru systemowego biblioteki lokalnej, zbioru składowania, dokumentu lub innego pliku.

plik_zdalny
Nazwa dostarczonego pliku w systemie zdalnym. Jeśli nazwa pliku lokalnego nie zostanie podana, klient FTP przyjmie nazwę domyślną. Jeśli plik zdalny o tej nazwie już istnieje, serwer FTP zastępuje jego zawartość zawartością pliku lokalnego, chyba że włączono opcję Ochrona zbioru (Store Unique - SUNIQUE).

Aby wysłać plik do systemu zdalnego, należy wybrać bieżący katalog roboczy z uprawnieniami do zapisu.

W następującym przykładzie użyto podkomendy PUT do przesłania podzbioru zbioru:

```
PUT MYLIB/MYFILE.MYMBR  (NAMEFMT = 0)
```

W poprzednim przykładzie podzbiór MYMBR zbioru MYFILE w bibliotece MYLIB jest wysyłany do systemu zdalnego.

W następującym przykładzie dokument PCSMENU.EXE w folderze QIWSOS2 znajdującym się w systemie plików usług biblioteki dokumentów jest wysyłany do systemu zdalnego.

```
PUT /QDLS/QIWSOS2/PCSMENU.EXE  (NAMEFMT = 1)
```

Uwaga: Jeśli nazwa pliku zdalnego wymaga zastosowania apostrofów jako części nazwy pliku, nazwa pliku powinna być ujęta w dwa dodatkowe apostrofy. W poniższym przykładzie do systemu zdalnego wysyłana jest nazwa "MEMBER.ONE", która ma zostać nadana przesyłanemu plikowi.

```
PUT LIBRARY/FILE.MEMBER 'MEMBER.ONE'
```

Zadania pokrewne

“Ujmowanie parametrów podkomend w cudzysłowy lub apostrofy” na stronie 147
Parametry podkomend można ująć w znaki apostrofu (’) lub cudzysłowu (″).

Odsyłacze pokrewne

“GET (Kopiowanie pliku z systemu zdalnego do lokalnego - Copy a File from a Remote System to the Local System)” na stronie 69
Podkomenda GET klienta FTP i5/OS służy do kopiowania pliku z systemu zdalnego do systemu lokalnego.

“MPUT (Wysłanie wielu podzbiorów z systemu lokalnego do systemu zdalnego - Send Multiple File Members from the Local System to a Remote System)” na stronie 78
Podkomenda MPUT klienta FTP i5/OS służy do kopiowania wielu plików do systemu zdalnego.

“Nazwy plików dla podkomend klienta służących do przesyłania danych” na stronie 148
W przypadku niektórych podkomend można używać domyślnych nazw plików źródłowych i docelowych; należy jednak określić nazwę pliku dla pozostałych podkomend.

“SUNIQUE (Sterowanie nadpisywaniem plików - Control Overwriting of Files)” na stronie 90
Podkomenda SUNIQUE klienta FTP i5/OS służy do sterowania zastępowaniem plików. Podkomenda SUNIQUE jest komendą odrębną, której należy użyć przed wydaniem podkomend PUT lub MPUT.

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

“MGET (Kopiowanie wielu plików z systemu zdalnego do systemu lokalnego - Copy Multiple Files from a Remote System to the Local System)” na stronie 76
Podkomenda MGET klienta FTP i5/OS służy do kopiowania wielu plików z systemu zdalnego.

“Nazwy plików do przesyłania” na stronie 150
Podkomendy klienta FTP używane do przesyłania danych mogą zawierać parametr **plik_lokalny**, **plik_zdalny** lub oba te parametry. Można ich użyć do nazwania danych, które mają być przesłane.

PWD (Wyświetlenie bieżącego katalogu, folderu lub biblioteki - Display Current Directory, Folder, or Library)

Komenda PWD klienta FTP i5/OS służy do wyświetlania katalogu bieżącego systemu zdalnego.

Podkomenda klienta FTP

Komenda PWD klienta FTP służy do wyświetlenia bieżącego katalogu lub biblioteki w systemie zdalnym.

PWd

Jeśli serwer zdalny jest systemem operacyjnym i5/OS, serwer wyświetli bibliotekę bieżącą lub katalog systemu plików w systemie zdalnym. Serwer wyświetla także katalog roboczy ujęty w znaki cudzysłowu. Aby dany katalog lub biblioteka systemu zdalnego stały się bieżącymi, należy użyć komendy CD (Katalog roboczy - Working Directory).

Odsyłacze pokrewne

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

QUOTE (Wysłanie komendy do serwera FTP - Send a Subcommand to an FTP Server)

Podkomenda QUOTE klienta FTP i5/OS służy do wysyłania podkomendy do serwera FTP.

Podkomenda klienta FTP

QUOTE *łańcuch*

łańcuch

Komenda serwera, która ma zostać wysłana do zdalnego serwera FTP i przez niego interpretowana. Serwer FTP wysyła ten łańcuch tekstu do zdalnego serwera FTP.

Uwagi:

1. Klient wymaga podkomendy QUOTE do uruchomienia specjalnej podkomendy Wysłanie komendy języka CL do serwera FTP (Send a CL Command to an FTP Server System - RCMD) serwera FTP i5/OS. Aby na przykład zapisać protokół zadania serwera FTP w zbiorze buforowym, należy wpisać:

   ```
   QUOTE RCMD DSPJOBLOG
   ```

   W celu uzyskania dostępu do protokołu zadania można użyć komendy Praca ze zbiorami buforowymi (Work with Spooled Files - WRKSPLF). Jeśli komenda WRKSPLF jest uruchamiana z poziomu innego profilu użytkownika, należy podać profil użytkownika, który jest zalogowany na serwerze FTP.
2. Długość łańcucha w serwerze FTP i5/OS jest ograniczona do 1000 znaków.
3. Podkomenda QUOTE umożliwia przekazanie do serwera FTP dowolnie wpisanego łańcucha. Na przykład, jeśli wpisane zostanie:

   ```
   QUOTE CWD 'SYS1'
   ```

   serwer FTP otrzyma

   ```
   CWD 'SYS1'
   ```

Informacje pomocnicze można uzyskać z serwera FTP, wpisując podkomendę:

```
QUOTE HELP
```

Serwer FTP wysyła podkomendę HELP do zdalnego hosta, który wyświetla ekran ze wszystkimi obsługiwanymi podkomendami. Wyświetlane informacje różnią się w zależności od typu zdalnego hosta.

Należy zauważyć, że podkomendy serwera FTP wpisane za pomocą podkomendy QUOTE mają wpływ tylko na serwer FTP, ale podobne podkomendy klienta mogą mieć wpływ zarówno na klienta, jak i na serwer. Na przykład podkomenda klienta REIN wysyła do serwera FTP podkomendę serwera REIN i reinicjuje określone zmienne stanu klienta. Podkomenda QUOTE REIN wysyła do serwera FTP tylko podkomendę REIN, ale nie zmienia żadnych zmiennych stanu klienta.

Uwaga: Używając podkomendy QUOTE do bezpośredniego wpisywania podkomend serwera, należy zachować ostrożność, aby nie otrzymać niepożądanych wyników. Zazwyczaj komenda QUOTE wykorzystywana jest jedynie w wyjątkowych sytuacjach, w których nie można użyć innych komend klienta. Sytuacja taka może zaistnieć w przypadku potrzeby użycia specjalnych podkomend serwera FTP i5/OS, jak na przykład CTRL.

Pojęcia pokrewne

“Uwagi na temat przekroczenia limitu czasu przez serwer” na stronie 31
Wartość limitu czasu nieaktywności to liczony w sekundach czas braku aktywności serwera FTP, po którym zamyka on sesję. Połączenie FTP można podtrzymywać, aby nie zostało zamknięte wskutek przekroczenia tego limitu czasu.

Odsyłacze pokrewne

"HELP (Uzyskiwanie pomocy dla komend FTP - Getting Help for FTP Subcommands)" na stronie 71
Podkomenda HELP klienta FTP i5/OS służy do uzyskiwania informacji o podkomendach FTP używanych przez system lokalny i system zdalny.

"RCMD (Wysłanie komendy języka CL do serwera FTP - Send a CL Command to an FTP Server System)" na stronie 53
Podkomenda serwera RCMD służy do wykonywania komend CL systemu i5/OS na serwerze FTP. Łańcuch komendy RCMD ma długość do 1000 znaków. Ponieważ dla podkomendy RCMD nie jest dostępny żaden wiersz komend, łańcuch podkomendy RCMD musi zawierać wszystkie parametry niezbędne do uruchomienia komendy CL.

Praca ze zbiorami buforowymi (Work with Spooled Files - WRKSPLF)

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

"Systemy plików i konwencje nazewnictwa" na stronie 143
Serwer FTP organizuje jednostki informacji systemu plików w struktury wielowarstwowe, podobne do drzewa.

REINITIALIZE (Reinicjowanie sesji pomiędzy systemami - Reinitialize Session between Systems)

Podkomenda REINITIALIZE klienta FTP i5/OS służy do ponownego uruchamiania sesji na systemie zdalnym.

Podkomenda klienta FTP

REInitialize

Jeśli serwer FTP obsługuje podkomendę REINITIALIZE, sesja USER z serwerem FTP zostaje zakończona. Serwer FTP wraca do stanu, w jakim był po ponownym nawiązaniu połączenia i użytkownik musi ponownie zalogować się do systemu, aby kontynuować pracę.

Zanim sesja USER zostanie zakończona, wszystkie rozpoczęte przesyłania plików są doprowadzane do końca.

Odsyłacze pokrewne

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

RENAME (Zmiana nazwy pliku w systemie zdalnym - Rename a File on a Remote System)

Podkomenda RENAME klienta FTP i5/OS służy do zmiany nazwy pliku w systemie zdalnym.

Podkomenda klienta FTP

REname *nazwa_pierwotna nowa_nazwa*

nazwa_pierwotna
Obecna nazwa zdalnego pliku.

nowa_nazwa
Nowa nazwa zdalnego pliku. Jeśli plik podany jako *nowa_nazwa* już istnieje, zastępowany jest nowym plikiem.

Poniższa komenda zmienia nazwę pliku SPORTSCAR.BMP w katalogu IMAGES wolumenu optycznego PICTURES na CAR.BMP:

```
REN /QOPT/PICTURES/IMAGES/SPORTSCAR.BMP
 /QOPT/PICTURES/IMAGES/CAR.BMP
```

Uwaga: W systemie operacyjnym i5/OS nie można zmienić nazwy pliku na nazwę z innego systemu plików.

Odsyłacze pokrewne

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

RESET (Resetowanie - Reset)

Podkomenda RESET klienta FTP i5/OS służy do usuwania zawartości kolejki odpowiedzi serwera. Komenda ta używana jest do ponownego zsynchronizowania sekwencji komend i odpowiedzi serwera z serwerem zdalnym FTP. Ponowna synchronizacja może być niezbędna po naruszeniu protokołu FTP przez system zdalny.

Podkomenda klienta FTP

Aby usunąć zawartość kolejki odpowiedzi serwera FTP, można użyć podkomendy RESET klienta FTP:

```
REset
```

Odsyłacze pokrewne

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

RMDIR (Usuwanie katalogu - Remove Directory)

Podkomenda RMDIR klienta FTP i5/OS służy do usuwania katalogu w systemie zdalnym.

Podkomenda klienta FTP

```
RMdir nazwa_ścieżki
```

nazwa_ścieżki

Nazwa znajdujących się w systemie zdalnym: katalogu plików, biblioteki lub specyfikatora grupy plików zależnych od systemu. W hierarchicznym systemie plików (HFS) usuwać można jedynie puste katalogi. Biblioteki są usuwane przez serwer FTP bezwarunkowo.

Odsyłacze pokrewne

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

SECData (Konfigurowanie ochrony danych - Setting data security protection)

Podkomenda SECData klienta FTP i5/OS służy do określania poziomu ochrony, który ma być stosowany dla połączeń danych, gdy z systemem zdalnym jest już nawiązane chronione połączenie sterujące.

Podkomenda klienta FTP

```
SECData [ C | P ]
```

Uwaga: SData jest synonimem dla tej komendy.

C Poziom ochrony kanału danych jest ustawiony na jawny. Takie połączenie **nie** jest chronione. Może ono być używane do przesyłania danych wstępnie zaszyfrowanych lub danych, które nie są poufne.

P Poziom ochrony kanału danych jest ustawiony na poufny. Takie połączenie jest bezpieczne. Zanim jakiekolwiek dane zostaną przesłane za pomocą tego połączenia, pomiędzy klientem a serwerem FTP musi dojść do negocjacji TLS.

1. Jeśli nie zostanie podany żaden parametr, komenda SECData wyświetla aktualną wartość używaną do ustawienia ochrony danych.
2. Kiedy z serwerem FTP jest ustanawiane chronione połączenie sterujące, poziom ochrony ma początkowo wartość określoną przez parametr DTAPROT komendy CL STRTCPFTP.
3. Do korzystania z komendy SECData wymagane jest chronione połączenie sterujące.
4. Podkomenda serwera PROT jest wydawana na serwerze FTP za każdym razem, gdy podkomenda SECDATA pomyślnie ustawi poziom ochrony danych.
5. Podczas ustawiania poziomu ochrony danych komenda SECData wysyła do serwera FTP podkomendy PBSZ i PROT. Komenda SECData ustawia także zmienną klienta przy każdym pomyślnym wywołaniu komendy PROT. Zmienna ta przedstawia ostatni poziom ochrony danych (C lub P) zaakceptowany przez serwer FTP. Jest ona używana do ustawiania poziomu ochrony danych podczas otwierania chronionego połączenia sterującego przez komendę SECOpen. Można ją zmienić za pomocą opcji LOCSITE DTAPROT.
6. Parametry ″C″ i ″P″ komendy SECData są takie same, jak parametry komendy serwera PROT.

Pojęcia pokrewne

“Zabezpieczanie klientów FTP za pomocą protokołu TLS lub SSL” na stronie 22
Dane przesyłane za pomocą połączeń sterujących i połączeń danych protokołu FTP można szyfrować, korzystając z połączeń TLS lub SSL.

Odsyłacze pokrewne

“LOCSITE (Podanie informacji o środowisku lokalnym - Specify Local Site Information)” na stronie 72
Podkomenda LOCSITE klienta FTP i5/OS służy do określania informacji wykorzystywanych przez klienta FTP do udostępniania usług właściwych dla systemu klienta.

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

SECOpen (Konfigurowanie ochrony danych - Setting data security protection)

Podkomenda SECOPEN klienta FTP i5/OS służy do otwierania chronionego połączenia sterującego z serwerem FTP przy użyciu określonej opcji ochrony.

Podkomenda klienta FTP

```
SECOpen nazwa_systemu [numer_portu] [ opcja_ochrony ]
```

Uwaga: SOpen jest synonimem dla SECOPEN.

nazwa_systemu
Wprowadź nazwę lub adres internetowy systemu zdalnego.

numer_portu
Numer portu wykorzystywany dla tego połączenia.

Uwagi:

- Jeśli ten parametr zostanie pominięty, a zostanie podany parametr (SSL, będzie używany port numer 21.
- Jeśli ten parametr zostanie pominięty, a zostanie podany parametr (IMPLICIT, będzie używany port numer 990.
- Jeśli pominięte zostaną zarówno parametry numer_portu, jak i opcja_ochrony, wtedy przyjęte zostaną port numer 21 i parametr (SSL.

opcja_ochrony

Określ rodzaj ochrony, który ma być używany.

(SSL Do połączeń z serwerem FTP wykorzystywana jest ochrona za pomocą SSL. Podczas nawiązywania połączenia używana jest komenda serwera AUTH (Autoryzacja - Authorization).

(IMPLICIT

Wykorzystywane jest niejawne połączenie chronione SSL/TLS z serwerem FTP. Niejawne połączenie SSL z serwerem jest nawiązywane bez wysyłania do serwera FTP podkomend serwera AUTH, PBSZ i PROT. W tym przypadku serwer FTP musi być tak skonfigurowany, aby oczekiwał na negocjację połączenia SSL/TLS dla określonego numeru portu.

W przypadku niejawnego połączenia SSL serwer FTP działa tak, jakby klient przesłał te podkomendy z następującymi parametrami:

- AUTH SSL
- PBSZ 0
- PROT P

Uwaga: Jeśli nie zostaną podane parametry opcje_ochrony, wtedy przyjmowany jest parametr (SSL. Kiedy używany jest port z numerem 990, przyjmowany jest parametr (IMPLICIT.

Pojęcia pokrewne

"Zabezpieczanie klientów FTP za pomocą protokołu TLS lub SSL" na stronie 22
Dane przesyłane za pomocą połączeń sterujących i połączeń danych protokołu FTP można szyfrować, korzystając z połączeń TLS lub SSL.

Odsyłacze pokrewne

"LOCSITE (Podanie informacji o środowisku lokalnym - Specify Local Site Information)" na stronie 72
Podkomenda LOCSITE klienta FTP i5/OS służy do określania informacji wykorzystywanych przez klienta FTP do udostępniania usług właściwych dla systemu klienta.

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

SENDPASV (Określenie, czy wysyłać podkomendę PASV - Specify whether to send a PASV Subcommand)

Podkomenda SENDPASV klienta FTP i5/OS służy do określania, czy do serwera FTP podczas przesyłania danych lub wydawania podkomend DIR i LS ma być wysyłana podkomenda PASV.

Podkomenda klienta FTP

```
SENDPAsv [ 0 | 1 ]
```

Jeśli nie zostanie wpisany żaden parametr, SENDPASV działa jak przełącznik. Wartość SENDPASV przełączana jest z 1 (ON - Włączony) na 0 (OFF - Wyłączony) lub z 0 na 1.

Gdy parametr zostanie wpisany, dopuszczalne wartości to:

0 Komenda PASV nie jest wysyłana.

1 Komenda PASV jest wysyłana. Jest to wartość domyślna.

Domyślnie opcja ta jest włączona, co oznacza wysyłanie podkomendy PASV. Jeśli opcja SENDPASV jest wyłączona, klient FTP nie wysyła podkomendy PASV.

Uwagi:

1. Ta podkomenda spełnia wymagania dokumentu RFC 1579, Firewall-Friendly FTP (FTP przyjazny dla zapory firewall.″ Użycie komendy PASV do nawiązania połączenia dla danych jest lepszą metodą, gdy dane muszą być przesyłane poprzez zaporę firewall. W niektórych scenariuszach przesyłanie danych poprzez zaporę firewall może być niemożliwe bez użycia komendy PASV.
2. Niektóre serwery FTP mogą nie obsługiwać komendy PASV. W takim przypadku, gdy opcja SENDPASV jest włączona (ON), klient FTP wyświetli komunikat wskazujący, że serwer nie obsługuje PASV. System będzie usiłował nawiązać połączenie danych bez wysyłania komendy PASV.

3. Jeśli opcja SENDPASV jest wyłączona (OFF) lub jest nieaktywna, a opcja SENDPORT jest włączona (ON), klient FTP wysyła podkomendę PORT.
4. Serwery FTP, które nie obsługują PASV, nie spełniają warunków RFC 1123.

Ograniczenie:

W przypadku połączenia z serwerem FTP poprzez serwer SOCKS, podkomenda SENDPASV może być użyta jedynie przed uruchomieniem przesyłania lub wydaniem podkomendy wyświetlenia zawartości katalogu. Jeśli podkomenda SENDPASV zostanie użyta po jednej z tych podkomend, klient nie jest w stanie nawiązać połączenia danych z serwerem FTP.

Gdy klient wyda podkomendę przesyłania danych lub wyświetlenia zawartości katalogu, przed ponownym wydaniem podkomendy SENDPASV połączenie z serwerem FTP poprzez serwer SOCKS powinno zostać zamknięte.

Podkomendy SENDPASV można użyć, gdy klient FTP nie jest połączony z serwerem.

Odsyłacze pokrewne

"SENDPORT (Określenie, czy wysyłać komendę PORT - Specify Whether to Sends a PORT Subcommand)"
Podkomenda SENDPORT klienta FTP i5/OS służy do określania, czy do serwera FTP podczas przesyłania danych lub wydawania podkomend DIR i LS ma być przesyłana podkomenda PORT.

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

Informacje pokrewne

Mechanizm wyszukiwania indeksów RFC

Edytor RFC

SENDPORT (Określenie, czy wysyłać komendę PORT - Specify Whether to Sends a PORT Subcommand)

Podkomenda SENDPORT klienta FTP i5/OS służy do określania, czy do serwera FTP podczas przesyłania danych lub wydawania podkomend DIR i LS ma być przesyłana podkomenda PORT.

Podkomenda klienta FTP

```
SENDPOrt [ 0 | 1 ]
```

Jeśli nie zostanie określony żaden parametr, komenda SENDPORT działa jak przełącznik. Wartość SENDPORT przełączana jest z 1 (Włączony) na 0 (Wyłączony) lub z 0 na 1.

Gdy parametr zostanie wpisany, dopuszczalne wartości to:

0 Komenda PORT nie jest wysyłana.

1 Komenda PORT jest wysyłana. Jest to wartość domyślna.

Uwagi:

1. Podkomendy SENDPORT należy używać tylko wtedy, gdy bez niej nie można nawiązać połączenia z serwerem FTP. Niewłaściwe użycie komendy SENDPORT może wywołać błędy.
2. Wskazane może być niewysyłanie podkomendy PORT do tych systemów, które ignorują podkomendy PORT, ponieważ wprowadzają one w błąd podając, że komenda ta została zaakceptowana.
3. Klient FTP nie wysyła podkomendy PORT, gdy opcja SENDPASV jest włączona (ON).

Odsyłacze pokrewne

"SENDPASV (Określenie, czy wysyłać podkomendę PASV - Specify whether to send a PASV Subcommand)" na stronie 87
Podkomenda SENDPASV klienta FTP i5/OS służy do określania, czy do serwera FTP podczas przesyłania danych lub wydawania podkomend DIR i LS ma być wysyłana podkomenda PASV.

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

SENDSITE (Określenie, czy wysłać komendę SITE - Specify Whether to Send a SITE Subcommand)

Podkomenda SENDSITE klienta FTP i5/OS służy do określania, czy podczas przeprowadzania operacji PUT lub MPUT ma być automatycznie wysyłana podkomenda SITE z informacjami o formacie rekordu.

Podkomenda klienta FTP

```
SENDSite [ 0 | 1 ]
```

Jeśli nie zostanie wpisany żaden parametr, SENDSITE działa jak przełącznik. Wartość SENDSITE przełączana jest z 1 (Włączony - ON) na 0 (Wyłączony - OFF) lub z 0 na 1.

Gdy parametr zostanie wpisany, dopuszczalne wartości to:

0 Komenda SITE nie jest wysyłana. Jest to wartość domyślna.

1 Wysłanie podkomendy SITE (zawierającej informacje o formacie rekordu) przed wysłaniem podkomend PUT i MPUT. Tego ustawienia należy użyć podczas przesyłania plików do serwera IBM Virtual Machine używającego informacji o formacie rekordu, które są wysyłane z podkomendą SITE.

Odsyłacze pokrewne

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

"SITE (Wysłanie informacji używanych przez system zdalny - Send Information Used by a Remote System)"
Podkomenda SITE klienta FTP i5/OS służy do wysyłania informacji wykorzystywanych przez system zdalny do udostępniania usług właściwych dla systemu zdalnego.

SITE (Wysłanie informacji używanych przez system zdalny - Send Information Used by a Remote System)

Podkomenda SITE klienta FTP i5/OS służy do wysyłania informacji wykorzystywanych przez system zdalny do udostępniania usług właściwych dla systemu zdalnego.

Podkomenda klienta FTP

```
SIte [parametry]
```

parametry
Zależne od systemu zdalnego.

Aby uzyskać więcej informacji o tych parametrach i poznać specyfikacje ich składni, należy wydać komendę HELP SERVER SITE. Niektóre serwery FTP nie obsługują komendy SITE.

Uwaga: Komenda SITE używana jest przez komendy PUT i MPUT do wskazania formatu i długości rekordów. Domyślnie, komenda PUT wysyła komendę SITE automatycznie. Podkomenda SITE jest używana przez podkomendę NAMEFMT w celu wskazania serwerowi FTP, czy nazwy mają format NAMEFMT 0 czy NAMEFMT 1.

Odsyłacze pokrewne

"SENDSITE (Określenie, czy wysłać komendę SITE - Specify Whether to Send a SITE Subcommand)" na stronie 89
Podkomenda SENDSITE klienta FTP i5/OS służy do określania, czy podczas przeprowadzania operacji PUT lub MPUT ma być automatycznie wysyłana podkomenda SITE z informacjami o formacie rekordu.

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

STATUS (Pobranie informacji o statusie z systemu zdalnego - Retrieve Status Information from a Remote System)

Podkomenda STATUS klienta FTP i5/OS służy do wyświetlania informacji o statusie systemu zdalnego.

Podkomenda klienta FTP

STAtus [*nazwa*]

name (nazwa)
Nazwa zdalnego katalogu lub pliku, dla którego zażądano informacji o statusie. Nie jest to parametr wymagany.

Uwaga: Aplikacja serwera FTP i5/OS nie obsługuje tego parametru nazwy.

Jeśli nie podano żadnego parametru, serwer FTP zwraca ogólne informacje o statusie procesu serwera FTP. Obejmują one bieżące wartości wszystkich parametrów przesyłania i status połączeń. Zwracane informacje o statusie zależą od konkretnej implementacji serwera FTP.

Odsyłacze pokrewne

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

STRUCT (Określenie struktury plików - Specify File Structure)

Podkomenda STRUCT klienta FTP i5/OS służy do określania struktury wysyłanych danych pliku.

Podkomenda klienta FTP

STRuct [F | R]

F Struktura plików. Struktura pliku zdefiniowana jest jako ciągła sekwencja bajtów danych.

R Struktura rekordów. Plik przesyłany jest jako ciąg rekordów sekwencyjnych.

Struktura pliku wpływa na tryb przesyłania, interpretację i pojemność pliku.

Odsyłacze pokrewne

"Konwencje składni komend klienta FTP" na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

SUNIQUE (Sterowanie nadpisywaniem plików - Control Overwriting of Files)

Podkomenda SUNIQUE klienta FTP i5/OS służy do sterowania zastępowaniem plików. Podkomenda SUNIQUE jest komendą odrębną, której należy użyć przed wydaniem podkomend PUT lub MPUT.

Podkomenda serwera FTP

Podkomenda SUNIQUE ustawia pewien „tryb" (w ten sam sposób jak podkomendy NAMEFMT, LISTFMT itd.), co oznacza, że każda uruchomiona następnie komenda PUT/MPUT korzysta z ustawienia wprowadzonego za pomocą podkomendy SUNIQUE. Na przykład:

```
FTP> SUNIQUE 1
FTP> MPUT *.FILES
```

Jeśli nie zostanie wpisany żaden parametr, SUNIQUE działa jak przełącznik. Wartość SUNIQUE przełączana jest z 1 (Włączony - ON) na 0 (Wyłączony - OFF) lub z 0 na 1.

Gdy parametr zostanie wpisany, dopuszczalne wartości to:

0 Nadpisanie pliku, jeśli istnieje. Jest to wartość domyślna.

1 Zamiast nadpisywania istniejącego pliku utworzenie w systemie zdalnym nowego pliku o unikalnej nazwie. Serwer FTP systemu zdalnego wysyła nazwę tworzonego pliku z powrotem do użytkownika.

Uwaga: Jeśli system zdalny jest produktem System i, serwer FTP tworzy nazwy typu zbiór.podzbiór przez dodanie numerów na końcu *pliku_lokalnego* określonego za pomocą podkomendy PUT lub MPUT. Jeśli zatem w systemie zdalnym istnieje już nazwa *NEWFILE.NEWMBR*, serwer FTP utworzy zbiór *NEWFILE.NEWMBR1* i zapisze w nim dane.

Nazwy plików dla innych systemów plików, takich jak hierarchiczny system plików (HFS), działają podobnie. Jeśli nazwa już istnieje, tworzony jest nowy plik, który składa się z podanej nazwy pliku i końcówki liczbowej. Jeśli zatem w systemie zdalnym istnieje już nazwa *xfsname*, system zdalny utworzy plik *xfsname1*.

Odsyłacze pokrewne

“MPUT (Wysłanie wielu podzbiorów z systemu lokalnego do systemu zdalnego - Send Multiple File Members from the Local System to a Remote System)” na stronie 78
Podkomenda MPUT klienta FTP i5/OS służy do kopiowania wielu plików do systemu zdalnego.

“PUT (Kopiowanie podzbioru zbioru z systemu lokalnego do pliku w systemie zdalnym - Copy a File Member from the Local System to a File on a Remote System)” na stronie 81
Podkomenda PUT klienta FTP i5/OS służy do kopiowania lokalnego podzbioru zbioru do systemu zdalnego.

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

SYSCMD (Wysłanie komendy CL do systemu lokalnego - Pass a CL Command to Your Local System)

Podkomenda SYSCMD klienta FTP i5/OS umożliwia wykonanie komendy CL w systemie lokalnym bez wychodzenia ze środowiska FTP.

Podkomenda klienta FTP

SYSCmd *wiersz_komend*

wiersz_komend

Dowolna komenda CL. Nazwę komendy można poprzedzić znakiem zapytania (?), aby uzyskać wiersz komend. Na przykład, jeśli wpisane zostanie:

```
SYSCMD ? SNDBRKMSG
```

wyświetlony zostanie ekran komendy Wysłanie komunikatu przerywającego (Send Break Message - SNDBRKMSG).

Jeśli mają być wyświetlane komunikaty niskiego poziomu, które są skutkiem komendy CL, lub ma zostać wprowadzonych wiele komend CL przed powrotem do środowiska FTP, należy użyć komendy CALL QCMD systemu i5/OS.

Aby uzyskać ekran Wpisywanie komend (Command Entry), należy wpisać następujący przykład:

```
SYSCMD CALL QCMD
```

Na ekranie Wpisywanie komend (Command Entry) można następnie uruchamiać aplikacje lub wpisywać komendy języka CL. Po zakończeniu działania aplikacji lub komendy CL wyświetlany jest ponownie ekran Wpisywanie komend (Command Entry). Na ekranie tym można wyświetlić komunikaty, rozpocząć dodatkową pracę w systemie lub nacisnąć klawisz F3 (Wyjście) lub F12 (Anuluj) i powrócić do FTP.

Komendy CL można wprowadzać po naciśnięciu klawisza F21 (Wiersz komend CL) na głównym ekranie serwera FTP. Serwer FTP nie akceptuje użycia klawisza F21, gdy do punktu wyjścia potwierdzenia żądania klienta FTP dodano program obsługi wyjścia.

Uwagi:

1. W większości serwerów FTP jest wyznaczony limit czasu, który kończy sesję, jeśli w określonym przedziale czasu nie wystąpi żadna aktywność. Jeśli komenda jest wykonywana dłużej niż ten limit czasu, serwer FTP zakończy połączenie z klientem.
2. System operacyjny i5/OS obsługuje znak wykrzyknika (!) jako synonim komendy SYSCMD.
3. Podkomenda SYSCMD przekazuje systemowi jako komendę CL dokładnie to, co wprowadzi użytkownik.

Odsyłacze pokrewne

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

TYPE (Określenie typu przesyłania plików - Specify File Transfer Type)

Podkomenda TYPE klienta FTP i5/OS służy do określania typu przesyłania plików lub reprezentacji, w jakiej odbywa się przesyłanie.

Podkomenda klienta FTP

```
TYpe [ A
  | B [ 1 | 2 | 3 [A|R] | 4 [A|R] | 5 | 6 | 7]
  | C numer CCSID
  | E
  | F [ 1 ]
  |   I ]
```

A Określa typ przesyłania jako typ domyślny (ASCII). Parametr ten ma takie samo działanie, jak komenda ASCII. Serwer FTP nie przypisuje do pliku żadnego sterowania w formacie pionowym. Obsługuje jedynie domyślny format NON PRINT dla ASCII. Typem przesyłania ASCII lub plikami tekstowymi należy posługiwać się zawsze, z wyjątkiem sytuacji, gdy oba systemy używają typu EBCDIC.

Domyślnym identyfikatorem CCSID dla TYPE A (ASCII) jest CCSID podany w parametrze CCSID komendy STRTCPFTP lub komendy FTP.

B JIS Kanji (CCSID 932)

B 1 JIS Kanji (CCSID 932)

B 2 Rozszerzony kod UNIX Kanji (CCSID 5050)

B 3 JIS 1983 używający sekwencji ASCII shift-in o zmienionym znaczeniu (CCSID 5054)

B 3 A JIS 1983 używający sekwencji ASCII shift-in o zmienionym znaczeniu (CCSID 5054)

B 3 R JIS 1983 używający JISROMAN sekwencji shift-in o zmienionym znaczeniu (CCSID 5052)

B 4 JIS 1978 używający sekwencji ASCII shift-in o zmienionym znaczeniu (CCSID 5055)

B 4 A JIS 1978 używający sekwencji ASCII shift-in o zmienionym znaczeniu (CCSID 5055)

B 4 R JIS 1978 używający sekwencji JISROMAN shift-in o zmienionym znaczeniu (CCSID 5053)

B 5 Hangeul (CCSID 934)

B 6 Koreański kod standardowy KSC-5601, wersja 1989 (CCSID 949)

B 7 Chiński tradycyjny (5550) (CCSID 938)

C numer CCSID
Określa typ przesyłania jako dowolny identyfikator CCSID zainstalowany w systemie. Numer identyfikatora CCSID musi być zgodny z C.

E Określa typ przesyłania jako EBCDIC. Parametr ten ma takie samo działanie, jak komenda EBCDIC. Serwer FTP nie przypisuje do pliku żadnego sterowania w formacie pionowym. Obsługuje jedynie domyślny format NON PRINT dla EBCDIC. Typ przesyłania EBCDIC przeznaczony jest do wydajnego przesyłania plików pomiędzy systemami, które używają kodowania EBCDIC dla wewnętrznych reprezentacji znaków.

F Kod IBM EBCDIC Kanji (CCSID 5035)

F 1 Kod IBM EBCDIC Kanji (CCSID 5035)

I Określa typ przesyłania jako obraz (binarny). Parametr ten ma takie samo działanie, jak komenda BINARY. W tym typie przesyłania dane wysyłane są jako łańcuch bitów zestawionych w 8-bitowe bajty. Ten typ przesyłania binarnego używany jest do wydajnego przechowywania i pobierania plików oraz przesyłania danych binarnych, takich jak kod obiektów. Dane przesyłane są w niezmienionej postaci; nie jest przeprowadzana żadna konwersja.

Jeśli nie podano żadnych parametrów, serwer FTP wyświetli aktualne ustawienie podkomendy TYPE.

Odsyłacze pokrewne

“LTYPE (Typ lokalny - Local Type)” na stronie 75
Podkomenda LTYPE klienta FTP i5/OS służy do określania typu przesyłania plików lub reprezentacji, w jakiej odbywa się przesyłanie w systemie lokalnym.

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

“Określanie tabel odwzorowań” na stronie 140
Tabele odwzorowań ASCII dla klienta FTP określane są w komendzie FTP. Dla serwera FTP służy do tego komenda Zmiana atrybutów FTP (Change FTP Attributes - CHGFTPA).

USER (Wysłanie ID użytkownika do systemu zdalnego - Send Your User ID to the Remote System)

Podkomenda USER klienta FTP i5/OS służy do wysyłania identyfikatora użytkownika do systemu zdalnego. Wraz z identyfikatorem użytkownika można wysłać również hasło.

Podkomenda klienta FTP

Użytkownik *identyfikator_użytkownika* [*hasło*]

identyfikator_użytkownika
Nazwa użytkownika w systemie zdalnym.

hasło Hasło użytkownika w systemie zdalnym. Podanie hasła jest opcjonalne. Jeśli hasło nie zostanie wpisane podczas wywoływania komendy USER, system zdalny prosi o podanie hasła, jeśli jest ono wymagane.

Odsyłacze pokrewne

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

VERBOSE (Sterowanie wyświetlaniem komunikatów odpowiedzi o błędach - Control of Text Display of Error Reply Messages)

Podkomenda VERBOSE klienta FTP i5/OS służy do sterowania sposobem wyświetlania odpowiedzi serwera FTP. Gdy przełącznik verbose jest włączony, wyświetlane są pełne odpowiedzi serwera, łącznie z kodami odpowiedzi. Gdy przełącznik verbose jest wyłączony, niektóre odpowiedzi serwera FTP i kody odpowiedzi są usuwane i nie są wyświetlane.

Podkomenda klienta FTP

Komenda VERBOSE przestawia przełącznik verbose.

Verbose

Odsyłacze pokrewne

“Konwencje składni komend klienta FTP” na stronie 146
Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

Programy obsługi wyjścia FTP

Istnieje możliwość użycia programów obsługi wyjścia w celu ochrony protokołu FTP. Serwer FTP komunikuje się z każdym programem obsługi wyjścia za pomocą określonego punktu wyjścia. Sekcja zawiera opisy parametrów oraz kody przykładowych programów.

Klient i serwer FTP komunikują się z każdym programem obsługi wyjścia za pomocą określonego punktu wyjścia. Parametry przekazywane są pomiędzy serwerem FTP a programem obsługi wyjścia. Format wymienianych informacji określony jest przez format punktu wyjścia.

FTP korzysta z następujących punktów wyjścia. W niżej wymienionych sekcjach znajduje się więcej informacji, obejmujących takie tematy, jak opisy parametrów i kody programów przykładowych:

- Punkt wyjścia potwierdzenia żądania: klient i serwer
- Punkt wyjścia logowania do serwera

Aby zapewnić poprawność działania programów obsługi wyjścia, należy zainstalować i zarejestrować programy obsługi wyjścia. Jeśli programy obsługi wyjścia nie są już potrzebne, należy je prawidłowo usunąć, aby zapobiec ich uruchamianiu w przyszłości.

Punkty wyjścia i formaty punktów wyjścia TCP/IP

Poniższa tabela zawiera informacje na temat punktów wyjścia różnych aplikacji TCP/IP i powiązanych z nimi formatów punktów wyjścia.

Punkty wyjścia TCP/IP	Aplikacja	VLRQ0100	TCPL0100	TCPL0200	TCPL0300	RXCS0100
QIBM_QTMF_CLIENT_REQ	FTP	X				
QIBM_QTMF_SERVER_REQ	FTP	X				
QIBM_QTMF_SVR_LOGON [1]	FTP		X	X	X [2]	
QIBM_QTMX_SERVER_REQ	REXEC	X				
QIBM_QTMX_SVR_LOGON[1]	REXEC		X		X [2]	
QIBM_QTMX_SVR_SELECT	REXEC					X
QIBM_QTOD_SERVER_REQ	TFTP	X				

Punkty wyjścia TCP/IP	Aplikacja	VLRQ0100	TCPL0100	TCPL0200	TCPL0300	RXCS0100
[1] - Punkt wyjścia może mieć kilka formatów, ale program obsługi wyjścia może być zarejestrowany tylko dla jednego formatu punktu wyjścia. Należy rozważyć każdy z wymienionych formatów, a następnie wybrać najodpowiedniejszy dla posiadanego systemu. [2] - Ten format jest dostępny począwszy od wersji V5R1.						

Pojęcia pokrewne

"Kontrolowanie dostępu do serwera FTP" na stronie 17
Jeśli protokół FTP jest używany, istnieje potrzeba zachowania kontroli nad użytkownikami w celu ochrony danych i sieci. Sekcja ta zawiera wskazówki i uwagi dotyczące ochrony.

"Zarządzanie dostępem za pomocą programów obsługi wyjścia FTP" na stronie 23
Dodatkowe bezpieczeństwo można zapewnić, dodając programy obsługi wyjścia FTP do punktów wyjścia serwera i klienta FTP, które oferują więcej możliwości ograniczenia dostępu do systemu.

Zadania pokrewne

"Instalowanie i rejestrowanie programów obsługi wyjścia" na stronie 15
Istnieje możliwość utworzenia bibliotek zawierających programy obsługi wyjścia i ich protokoły, a następnie skompilowania i zarejestrowania tych programów jako programów używanych przez serwer FTP.

Odsyłacze pokrewne

"Pisanie programów obsługi wyjścia dla anonimowego serwera FTP" na stronie 13
Aby korzystać z anonimowego serwera FTP w systemie operacyjnym i5/OS, należy napisać dwa programy obsługi wyjścia: program obsługi wyjścia logowania do serwera FTP i program obsługi wyjścia potwierdzenia żądania protokołu FTP.

Punkt wyjścia potwierdzenia żądania: klient i serwer

Za pomocą punktów wyjścia potwierdzenia żądania można ograniczyć zakres operacji, jakie mogą wykonywać użytkownicy protokołu FTP.

Są one udostępniane zarówno przez klienta, jak i serwer FTP; aby ograniczyć dostęp do klienta i serwera FTP, do obu punktów wyjścia trzeba dodać programy obsługi wyjścia.

Wskazówka: Ponieważ punkty wyjścia klienta i serwera FTP używają tego samego formatu punktów wyjścia, wystarczy napisać pojedynczy program do obsługi obu punktów.

Jeśli jest zaimplementowany anonimowy serwer FTP, należy napisać program obsługi wyjścia potwierdzenia żądania serwera FTP w celu ograniczenia uprawnień anonimowych użytkowników FTP tylko do komend wczytywania i zabronienia im wykonywania komend CL.

Co powinien zawierać program:

- obsługę wyjątków,
- debugowanie,
- protokołowanie,

Akceptowane i odrzucane komendy

Program obsługi wyjścia potwierdzenia żądania protokołu FTP umożliwia kontrolę nad akceptowaniem i odrzucaniem operacji. Decyzja ta jest podejmowana przez program obsługi wyjścia dodatkowo, poza sprawdzaniem poprawności na poziomie aplikacji klienta lub serwera FTP. Aplikacja klienta lub serwera FTP wywołuje program obsługi wyjścia, zarejestrowany dla tej aplikacji, za każdym razem gdy przetwarzane jest jedno z następujących żądań:

- Tworzenie katalogu lub biblioteki
- Usuwanie katalogu lub biblioteki
- Ustawianie bieżącego katalogu
- Wyświetlanie nazw plików

- Usuwanie plików
- Wysyłanie plików
- Otrzymywanie plików
- Zmiana nazwy pliku
- Uruchamianie komendy CL

Aby na stałe i bezwarunkowo odrzucać komendę, w formacie punktu wyjścia VRLQ0100 można podać wartość -1 parametru 8 (Zezwolenie na operację).

Czy istnieje opcja limitu czasu w programie obsługi wyjścia?

W programach obsługi wyjścia protokołu FTP nie ma obsługi limitu czasu. Jeśli w programie obsługi wyjścia wystąpi błąd lub wyjątek, którego program ten nie będzie mógł obsłużyć, serwer FTP przerwie sesję.

Przykładowe programy

Dostępne są przykładowe programy ułatwiające konfigurowanie anonimowego serwera FTP w systemie. Programy te są tylko ilustracją. Nie zawierają one wszystkich wymaganych opcji, aby można je było uruchomić w systemie produkcyjnym. Przykłady te mogą posłużyć jako wzór do pisania własnych programów. Kopiując fragmenty kodu z tych przykładów, można je dodać do własnych programów. Zalecane jest uruchamianie programów przykładowych na systemie innym niż produkcyjny.

Pojęcia pokrewne

"Zarządzanie dostępem za pomocą programów obsługi wyjścia FTP" na stronie 23
Dodatkowe bezpieczeństwo można zapewnić, dodając programy obsługi wyjścia FTP do punktów wyjścia serwera i klienta FTP, które oferują więcej możliwości ograniczenia dostępu do systemu.

Odsyłacze pokrewne

"Pisanie programów obsługi wyjścia dla anonimowego serwera FTP" na stronie 13
Aby korzystać z anonimowego serwera FTP w systemie operacyjnym i5/OS, należy napisać dwa programy obsługi wyjścia: program obsługi wyjścia logowania do serwera FTP i program obsługi wyjścia potwierdzenia żądania protokołu FTP.

Przykład: kod programu obsługi wyjścia potwierdzenia żądania klienta lub serwera FTP w języku CL:

Przedstawiony przykład jest prostym programem obsługi wyjścia potwierdzenia żądania FTP. Jest on napisany w języku programowania CL. Kod tego programu nie jest kompletny, ale stanowi podstawę do tworzenia własnego programu obsługi punktu wyjścia klienta lub serwera.

Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki zapisane w sekcji "Licencja na kod oraz Informacje dotyczące kodu" na stronie 159.

(Wstępnie sformatowany tekst w poniższym przykładzie nie mieści się w ramce.)

```
/*****************************************************************************/
/*                                                                           */
/*    Przykład programu obsługi wyjścia potwierdzenia żądania serwera FTP    */
/*    dla anonimowego użytkownika FTP.                                                 */    */
/*    Uwaga: Ten program jest tylko przykładem i NIE przechodził formalnego  */
/*           przeglądu i testowania.                                         */
/*                                                                           */
/*  Uwagi dodatkowe:                                                         */
/*  1. Gdy ID aplikacji to 1 (serwer FTP) i ID operacji to 0 (inicjowanie    */
/*     sesji), to gdy wywoływany jest program obsługi wyjścia QTCP zadanie   */
/*     działa w profilu QTCP. W przeciwnym razie zadanie działa w profilu    */
/*     użytkownika.                                                          */
/*  2. Zaleca się, aby program obsługi wyjścia był tworzony w bibliotece     */
/*     z uprawnieniami *PUBLIC ustawionymi na *EXCLUDE oraz nadanie mu       */
/*     uprawnień *PUBLIC ustawionych na *EXCLUDE.  Serwer FTP zaadaptuje     */
```

```
/*     uprawnienia niezbędne do wywołania programu obsługi wyjścia.          */
/*  3. Można wykorzystać ten sam program obsługi wyjścia dla  punktów wyjścia */
/*     zatwierdzenia żądań zarówno klienta, jak i serwera FTP. Jednakże ten   */
/*     program nie bierze pod uwagę klienta.                                  */
/*                                                                            */
/******************************************************************************/

 TSTREQCL:   PGM        PARM(&APPIDIN &OPIDIN &USRPRF&IPADDRIN +
                          &IPLENIN &OPINFOIN &OPLENIN &ALLOWOP)

/* Deklaracja parametrów wejściowych                                                 */
             DCL        VAR(&APPIDIN)   TYPE(*CHAR) LEN(4)  /* ID aplikacji          */
             DCL        VAR(&OPIDIN)    TYPE(*CHAR) LEN(4)  /* ID operacji           */
             DCL        VAR(&USRPRF)    TYPE(*CHAR) LEN(10) /* Profil użytkownika    */
             DCL        VAR(&IPADDRIN)  TYPE(*CHAR)         /* Zdalny adres IP       */
             DCL        VAR(&IPLENIN)   TYPE(*CHAR) LEN(4)  /* Długość adresu IP     */
             DCL        VAR(&OPLENIN)   TYPE(*CHAR) LEN(4)  /* Dł. infor. właściwych dla operacji */
             DCL        VAR(&OPINFOIN)  TYPE(*CHAR) +
                                          LEN(9999) /* Informacja właściwa dla operacji */
             DCL        VAR(&ALLOWOP)   TYPE(*CHAR) LEN(4)    /* Zezwolenie (wyjściowy) */

/* Deklaracja lokalnych kopii parametrów (w formacie używanym przez CL)              */
             DCL        VAR(&APPID)     TYPE(*DEC)  LEN(1 0)
             DCL        VAR(&OPID)      TYPE(*DEC) LEN(1 0)
             DCL        VAR(&IPLEN)     TYPE(*DEC) LEN(5 0)
             DCL        VAR(&IPADDR)    TYPE(*CHAR)
             DCL        VAR(&OPLEN)     TYPE(*DEC) LEN(5 0)
             DCL        VAR(&OPINFO)    TYPE(*CHAR) LEN(9999)
             DCL        VAR(&PATHNAME)  TYPE(*CHAR) LEN(9999) /* Nazwa ścieżki wielkimi literami  */

/* Deklaracja wartości dla allow(1) oraz noallow(0)                                   */
             DCL        VAR(&ALLOW)     TYPE(*DEC) LEN(1 0) VALUE(1)
             DCL        VAR(&NOALLOW)   TYPE(*DEC) LEN(1 0) VALUE(0)

/* Deklaracja bloku sterującego żądaniami dla funkcji API QLGCNVCS (w przypadku konwersji):  */
/* konwersja na wielkie litery z zależności od zadania CCSID                         */
             DCL        VAR(&CASEREQ)   TYPE(*CHAR) LEN(22) +
                          VALUE(X'00000001000000000000000000000000000000+
                          000000000')
             DCL        VAR(&ERROR)     TYPE(*CHAR) LEN(4) +
                          VALUE(X'00000000')

/* Przypisanie parametrów wejściowych do kopii lokalnych                             */
             CHGVAR     VAR(&APPID)     VALUE(%BINARY(&APPIDIN))
             CHGVAR     VAR(&OPID)      VALUE(%BINARY(&OPIDIN))
             CHGVAR     VAR(&IPLEN)     VALUE(%BINARY(&IPLENIN))
             CHGVAR     VAR(&IPADDR)    VALUE(%SUBSTRING(&IPADDRIN 1 &IPLEN))
             CHGVAR     VAR(&OPLEN)     VALUE(%BINARY(&OPLENIN))

/* Obsługa pola informacji właściwej dla operacji (która jest długością zmiennej)   */
             IF         COND(&OPLEN = 0) THEN(CHGVAR VAR(&OPINFO) +
                          VALUE(' '))
             ELSE       CMD(CHGVAR VAR(&OPINFO) VALUE(%SST(&OPINFOIN +
                          1 &OPLEN)))

/* ID operacji 0 (połączenie przychodzące): odrzucenie, jeśli połączenie przez interfejs 9.8.7.6 */
/* w innym przypadku akceptacja. (Podany adres jest tylko przykładem). Tę możliwość można        */
/* wykorzystać tylko do akceptacji połączeń z sieci wewnętrznych i odrzucania tych               */
/* z "prawdziwego" Internetu, o ile połączenie z Internetem jest realizowane przez               */
/* oddzielny interfejs IP.                                                                       */
/* UWAGA: W przypadku serwera FTP, operacja 0 jest ZAWSZE wykonywana z profilem QCTP             */
/*                                                                                               */
             IF         COND(&OPID = 0) THEN(DO)
               IF         COND(&OPINFO = '9.8.7.6') THEN(CHGVAR +
                          VAR(%BINARY(&ALLOWOP)) VALUE(&NOALLOW))
               ELSE       CMD(CHGVAR VAR(%BINARY(&ALLOWOP)) +
                          VALUE(&ALLOW))
```

```
              GOTO     CMDLBL(END)
            ENDDO

/* Sprawdzanie, czy użytkownik anonimowy                                          */
            IF         COND(&USRPRF = 'ANONYMOUS ') THEN(DO)
/* Zakaz wykonania przez użytkownika anonimowego następujących operacji:         */
/*   1 (Tworzenie katalogu/biblioteki); 2 (Usuwanie katalogu/biblioteki);         */
/*   5 (Usuwanie pliku); 7 (Otrzymywanie pliku); 8 (Zmiana nazwy pliku);          */
/*   9 (Wykonanie CL)                                                            */
              IF       COND(&OPID = 1 | &OPID = 2 | +
                          &OPID = 5 | &OPID = 7 | &OPID = 8 | +
                          &OPID = 9) THEN(CHGVAR +
                          VAR(%BINARY(&ALLOWOP)) VALUE(&NOALLOW))
              ELSE     CMD(DO)
/* Operacje: 3 (zmiana katalogu), 4 (wyświetlenie katalogu) oraz 6 (wysłanie pliku), dozwolone   */
/* tylko w bibliotece PUBLIC LUB katalogu "/public".  Należy zwrócić uwagę, że wszystkie          */
/* nazwy ścieżek wykorzystują format nazw zintegrowanego systemu plików.          */
                IF     COND(&OPID = 3 | &OPID = 4 | &OPID = 6) THEN(DO)
/* Na początku należy dokonać konwersji nazwy ścieżki na wielkie litery (ponieważ w nazwach      */
/* katalogu "root" i bibliotekach systemu plików nie rozróżnia się małych              */
/* i wielkich liter).                                                              */
                  CALL PGM(QLGCNVCS) PARM(&CASEREQ &OPINFO &PATHNAME +
                                          &OPLENIN &ERROR)
/* Uwaga: należy sprawdzić sam katalog "/public" oraz nazwy ścieżek zaczynające się              */
/* od "/public/".                                                        */
                  IF   COND((%SUBSTRING(&PATHNAME 1 20) *NE +
                          '/QSYS.LIB/PUBLIC.LIB') *AND +
                          (&PATHNAME *NE '/PUBLIC') *AND +
                          (%SUBSTRING(&PATHNAME 1 8) *NE '/PUBLIC/')) +
                          THEN(CHGVAR +
                          VAR(%BINARY(&ALLOWOP)) VALUE(&NOALLOW))
                  ELSE       CMD(CHGVAR VAR(%BINARY(&ALLOWOP)) +
                          VALUE(&ALLOW))
                ENDDO
              ENDDO
            ENDDO
/* Dla użytkownika innego niż anonimowy: pozwolenie na wszystko                   */
            ELSE       CMD(CHGVAR VAR(%BINARY(&ALLOWOP)) +
                          VALUE(&ALLOW))

 END:       ENDPGM
```

Przykład: kod programu obsługi wyjścia potwierdzenia żądania serwera FTP w języku ILE RPG:

Przedstawiony przykład jest prostym programem obsługi wyjścia potwierdzenia żądania FTP, wykorzystywanym pomiędzy klientem a serwerem. Jest on napisany w języku programowania ILE RPG. Kod tego programu nie jest kompletny, ale jest punktem wyjścia do tworzenia własnego programu.

Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki zapisane w sekcji “Licencja na kod oraz Informacje dotyczące kodu” na stronie 159.

(Uprzednio sformatowany w poniższym przykładzie tekst nie mieści się w ramce.)

```
          * Opis modułu ******************************************************
          *                                                                   *
          *                      FUNKCJA PROGRAMU                             *
          *                                                                   *
          * Program ten przedstawia kilka możliwych funkcji programu obsługi *
          * wyjścia potwierdzenia żądania serwera i klienta FTP.              *            *
          *                                                                   *
          * Uwaga: Ten program jest tylko przykładem i nie przechodził        *
          *        formalnego przeglądu i testowania.                         *
          *                                                                   *
          *********************************************************************
          F/SPACE 3
          *********************************************************************
```

```
 *                                                                     *
 *                       UŻYTE WSKAŹNIKI                               *
 *                                                                     *
 *   WSK.  OPIS                                                        *
 *                                                                     *
 *    LR - ZAMKNIĘCIE PLIKÓW PRZY WYJŚCIU                              *
 *                                                                     *
 **********************************************************************
 F/EJECT
 **********************************************************************
 * STRUKTURY DANYCH UŻYWANE PRZEZ PROGRAM                             *
 **********************************************************************
 *
 * Definicje stałych
 *
D Anonym          C                   CONST('ANONYMOUS ')
D PublicLib       C                   CONST('/QSYS.LIB/ITSOIC400.LIB')
D PublicDir       C                   CONST('//ITSOIC.400')
 *
 * Kilka komend CL użytych w programie
 *
D ClearSavf       C                   CONST('CLRSAVF ITSOIC400/TURVIS')
D SaveLib         C                   CONST('SAVLIB LIB(ITSOIC400) -
D                                     DEV(*SAVF) -
D                                     SAVF(ITSOIC400/TURVIS)')
 *
 * Wartość używana jako wyzwalacz konia trojańskiego
 *
D Savetti         C                   CONST('ITSOIC400.LIB/TURVIS.FILE')
 *                                    Rozszerzeniem jest FILE, mimo że
 *                                    powinno być SAVF (tak jak wprowadził użytkownik)
 *
 *
 * Pola pomocne podczas konwersji z małych liter na wielkie
 *     1
D LW              C                   CONST('abcdefghijklmnopqrstuvwxyz')
D UP              C                   CONST('ABCDEFGHIJKLMNOPQRSTUVWXYZ')
 *
D NeverAllow      C                   CONST(-1)
D DontAllow       C                   CONST(0)
D Allow           C                   CONST(1)
D AlwaysAllw      C                   CONST(2)
C/EJECT
 **********************************************************************
 * DEFINICJE ZMIENNYCH I LISTY UŻYWANE PRZEZ PROGRAM
 **********************************************************************
 C/SPACE 2
 *
 * Definicje parametrów binarnych
 *
D                 DS
D  APPIDds                1      4B 0
D  OPIDds                 5      8B 0
D  IPLENds                9     12B 0
D  OPLENds               13     16B 0
D  ALLOWOPds             17     20B 0
 *
C     *LIKE         DEFINE    APPIDds       APPIDIN
C     *LIKE         DEFINE    OPIDds        OPIDIN
C     *LIKE         DEFINE    IPLENds       IPLENIN
C     *LIKE         DEFINE    OPLENds       OPLENIN
C     *LIKE         DEFINE    ALLOWOPds     ALLOWOP
 *
C     *LIKE         DEFINE    OPINFOIN      OPINFO
 *
 * Definicje listy parametrów
 *
```

```
C     *Entry        PLIST
 * Parametry wejściowe:
C                   PARM                    APPIDIN                       ID aplikacji
 *                                          możliwe wartości:  0 = program klienta FTP
 *                                                             1 = program serwera FTP
C                   PARM                    OPIDIN                        ID operacji
 *                                          możliwe wartości   0 = Inicjowanie sesji
 *                                                             1 = Tworzenie katalogu/biblioteki
 *                                                             2 = Usuwanie katalogu/biblioteki
 *                                                             3 = Ustawianie bieżącego katalogu
 *                                                             4 = Wyświetlanie katalogu/biblioteki
 *                                                             5 = Usuwanie plików
 *                                                             6 = Wysyłanie plików
 *                                                             7 = Odbieranie plików
 *                                                             8 = Zmiana nazw plików
 *                                                             9 = Wykonanie komend CL
C                   PARM                    USRPRF        10   Profil użytkownika
C                   PARM                    IPADDRIN      15   Zdalny adres IP
C                   PARM                    IPLENIN            Długość adresu IP
C                   PARM                    OPINFOIN      999  Informacja właściwa dla operacji
C                   PARM                    OPLENIN            Długość inf. spec. dla operacji
 * Parametry zwracane:
C                   PARM                    ALLOWOP            Zezwolenie na operację (Wyjście)
 *                                          możliwe wartości: -1 = Stały brak zezwolenia na operację
 *                                                                (Operacja nie będzie
 *                                                               możliwa przez całą
 *                                                               bieżącą sesję)
 *                                                             0 = Odrzucenie operacji
 *                                                             1 = Zezwolenie na operację
 *                                                             2 = Stałe zezwolenie na operację
 *                                                                (Operacja nie będzie
 *                                                               możliwa przez całą
 *                                                               bieżącą sesję)
C/EJECT
 ********************************************************************
 * PROGRAM GŁÓWNY                                                   *
 ********************************************************************
 *
C                   SELECT
C     APPIDIN       WHENEQ    0
C                   EXSR      ClientRqs
C     APPIDIN       WHENEQ    1
C                   EXSR      ServerRqs
C                   ENDSL
 *
C                   EVAL      *INLR = *ON
C                   RETURN
C/EJECT
********************************************************************
 * P O D P R O G R A M Y                                           *
********************************************************************
********************************************************************
* Obsługa potwierdzania wszystkich żądań klienta FTP              *
********************************************************************
C     ClientRqs     BEGSR
 *
 * Sprawdzenie profilu użytkownika
 *
C                   SELECT
 *
 * Sprawdzenie 'złych' użytkowników niemających zezwolenia na wykonywanie czegokolwiek
 *
C     USRPRF        WHENEQ    'JOEBAD    '
 *
C                   Z-ADD     NeverAllow    ALLOWOP                   Brak zezwolenia na operację
 *
 * Sprawdzenie 'normalnych' użytkowników niemających zezwolenia na przeprowadzanie części działań
```

```
     *
    C     USRPRF        WHENEQ    'JOENORMAL '
     *
    C                   SELECT
     *
    C     OPIDIN        WHENEQ    0                           Nowe połączenie
    C                   Z-ADD     Allow         ALLOWOP
     *
    C     OPIDIN        WHENEQ    1                           Utworzenie katalogu/biblioteki
    C     OPIDIN        OREQ      2                           Usunięcie katalogu/biblioteki
    C     OPIDIN        OREQ      5                           Usunięcie plików
    C     OPIDIN        OREQ      7                           Odebranie plików z S
    C     OPIDIN        OREQ      8                           Zmiana nazwy plików
    C     OPIDIN        OREQ      9                           Wykonanie komend CL
     *
    C                   Z-ADD     NeverAllow    ALLOWOP       Brak zezwolenia na operację
     *
    C     OPIDIN        WHENEQ    3                           Ustawienie bieżącego katalogu
    C     OPIDIN        OREQ      4                           Wyświetlenie katalogu/biblioteki
    C     OPIDIN        OREQ      6                           Wysłanie plików do serwera
     *
     * Pobranie nazw bibliotek i katalogów dla porównania z dozwolonymi obszarami
     *
    C     OPLENIN       IFGE      11
    C     11            SUBST     OPINFOIN:1    Directory       11
    C                   ELSE
    C     OPLENIN       SUBST(P)  OPINFOIN:1    Directory
    C                   ENDIF
    C  1  LW:UP         XLATE     Directory     Directory
     *
    C     OPLENIN       IFGE      23
    C     23            SUBST     OPINFOIN:1    Library         23
    C                   ELSE
    C     OPLENIN       SUBST(P)  OPINFOIN:1    Library
    C                   ENDIF
     *
    C     Directory     IFEQ      PublicDir                   Dozwolony katalog
    C     Library       OREQ      PublicLib                   lub biblioteka
    C                   Z-ADD     Allow         ALLOWOP
    C                   ELSE
    C                   Z-ADD     DontAllow     ALLOWOP
    C                   ENDIF
     *
    C                   OTHER
    C                   Z-ADD     DontAllow     ALLOWOP
    C                   ENDSL
     *
     * Sprawdzenie użytkowników 'super' mających zezwolenie na wszystko
     *
    C     USRPRF        WHENEQ    'JOEGOOD   '
    C     USRPRF        OREQ      'A960101B  '
    C     USRPRF        OREQ      'A960101C  '
    C     USRPRF        OREQ      'A960101D  '
    C     USRPRF        OREQ      'A960101E  '
    C     USRPRF        OREQ      'A960101F  '
    C     USRPRF        OREQ      'A960101Z  '
     * Udostępnienie wszystkich operacji FTP
    C                   Z-ADD     AlwaysAllw    ALLOWOP
     *
2   * Inni użytkownicy: dla bezpieczeństwa należy użyć NeverAllow.
     * Jeśli czynność ma być dozwolona dla wszystkich innych użytkowników, należy zmienić NeverAllow
     * na AlwaysAllw.
     *
    C                   OTHER
    C                   Z-ADD     NeverAllow    ALLOWOP
     ******************************************************************
     * Obsługa potwierdzania wszystkich żądań serwera FTP              *
```

```
 ********************************************************************
C     ServerRqs     BEGSR
 *
 * Sprawdzanie, czy użytkownik to ANONYMOUS
 *
C     USRPRF        IFEQ      Anonym
 *
C                   SELECT
 *
C     OPIDIN        WHENEQ    1                           Utworzenie katalogu/biblioteki
C     OPIDIN        OREQ      2                           Usunięcie katalogu/biblioteki
C     OPIDIN        OREQ      5                           Usunięcie plików
C     OPIDIN        OREQ      7                           Odebranie plików z C
C     OPIDIN        OREQ      8                           Zmiana nazwy plików
C     OPIDIN        OREQ      9                           Wykonanie komend CL
 *
C                   Z-ADD     NeverAllow    ALLOWOP       Brak zezwolenia na operację
 *
C     OPIDIN        WHENEQ    3                           Ustawienie bieżącego katalogu
C     OPIDIN        OREQ      4                           Wyświetlenie katalogu/biblioteki
C     OPIDIN        OREQ      6                           Wysłanie plików do serwera
 *
 * Pobranie nazw bibliotek i katalogów dla porównania z dozwolonymi obszarami
 *
C     OPLENIN       IFGE      11
C     11            SUBST     OPINFOIN:1    Directory       11
C                   ELSE
C     OPLENIN       SUBST(P)  OPINFOIN:1    Directory
C                   ENDIF
C  1  LW:UP         XLATE     Directory     Directory
 *
C     OPLENIN       IFGE      23
C     23            SUBST     OPINFOIN:1    Library         23
C                   ELSE
C     OPLENIN       SUBST(P)  OPINFOIN:1    Library
C                   ENDIF
 *
C     Directory     IFEQ      PublicDir                 Dozwolony katalog
C     Library       OREQ      PublicLib                 lub biblioteka
C                   Z-ADD     Allow         ALLOWOP
C                   ELSE
C                   Z-ADD     DontAllow     ALLOWOP
C                   ENDIF
 *
C                   OTHER
C                   Z-ADD     DontAllow     ALLOWOP
C                   ENDSL
 *
C                   ELSE
 *
 * Inni użytkownicy: zezwolenie na wykonanie wszystkich operacji FTP
 *
C     OPIDIN        IFEQ      6                           Wysłanie plików do klienta
 *
 * Jeśli klient wysłał GET dla zbioru składowania HESSU w bibl., nastąpi odświeżenie zawart.
 *
 *
C     LW:UP         XLATE     OPINFOIN      OPINFO
C                   Z-ADD     0             i                3 0
C     Savetti       SCAN      OPINFO:1      i
 *
C     i             IFGT      0
 *
 * Zakładamy, że zbiór składowania istnieje i tutaj następuje jego czyszczenie,
 *
C                   MOVEL(p)  ClearSavf     Cmd             80
C                   Z-ADD     19            Len             15 5
```

```
C                   CALL      'QCMDEXC'                     9999
C                   PARM                    Cmd
C                   PARM                    Len
 *
 * a tutaj zapis biblioteki do zbioru składowania
 *
C                   MOVEL(p)  SaveLib       Cmd
C                   Z-ADD     46            Len
C                   CALL      'QCMDEXC'                     9999
C                   PARM                    Cmd
C                   PARM                    Len
C                   ENDIF
C                   ENDIF
 *
C                   Z-ADD     Allow         ALLOWOP
C                   ENDIF
 *
C                   ENDSR
```

Format punktu wyjścia VLRQ0100:

Punktem wyjścia potwierdzenia żądania aplikacji serwera FTP jest QIBM_QTMF_SERVER_REQ. Punktem wyjścia potwierdzenia żądania aplikacji klienta FTP jest QIBM_QTMF_CLIENT_REQ. Interfejs sterujący formatem parametru dla tego punktu wyjścia to VLRQ0100. Interfejs punktu wyjścia VLRQ0100 zawiera określone parametry.

Poniższa tabela przedstawia parametry i format parametrów dla interfejsu VLRQ0100.

Wymagany format parametrów dla interfejsu punktu wyjścia VLRQ0100

Parametr	Opis	Wejściowy lub wyjściowy	Typ i długość
1	Identyfikator aplikacji	Wejściowy	Binary(4)
2	Identyfikator operacji.	Wejściowy	Binary(4)
3	Profil użytkownika	Wejściowy	Char (10)
4	Zdalny adres IP.	Wejściowy	Char (*)
5	Długość zdalnego adresu IP	Wejściowy	Binary(4)
6	Informacja właściwa dla operacji.	Wejściowy	Char (*)
7	Długość informacji właściwej dla operacji.	Wejściowy	Binary(4)
8	Zezwolenie na operację.	Wyjściowy	Binary(4)

Opis parametrów:

VLRQ0100 Parametr 1:
Identyfikator aplikacji

INPUT; BINARY(4)
Identyfikuje aplikację TCP/IP, która wysyła żądanie. Interfejs VLRQ0100 jest używany wspólnie przez cztery różne aplikacje TCP/IP. Pierwszy parametr określa, która aplikacja wywołuje program obsługi wyjścia. W poniższej tabeli przedstawiono możliwe wartości.

Wartość	Aplikacja
0	program klienta FTP
1	program serwera FTP
2	program serwera REXEC

Wartość	Aplikacja
3	program serwera TFTP

VLRQ0100 Parametr 2:
Identyfikator operacji.

Input; Binary(4)
Wskazuje operację (komendę), którą użytkownik FTP chce (żąda) wykonać.

Jeśli identyfikator aplikacji (parametr 1) wskazuje na program klienta FTP lub serwera FTP, możliwe są poniższe wartości.

Wartość	ID operacji	Podkomenda klienta	Podkomenda serwera
0	Rozpoczęcie sesji	Open, SECOpen	Nowe połączenie
1	Utworzenie katalogu/biblioteki	*	MKD, XMDK
2	Usunięcie katalogu/biblioteki	*	RMD, XRMD
3	Określenie bieżącego katalogu/biblioteki	LCD	CWD, CDUP, XCWD, XCUP
4	Wyświetlenie listy zbiorów	*	LIST, NLIST
5	Usunięcie zbioru	*	DELE
6	Wysłanie zbioru	APPEND, PUT, MPUT	RETR
7	Pobranie zbioru	GET, MGET	APPE, STOR, STOU
8	Zmiana nazwy zbioru	*	RNFR, RNTO
9	Wykonanie komendy CL	SYSCMD	RCMD, ADDm, ADDV, CRTL, CRTP, CRTS, DLTF, DLTL

Uwaga: Symbol gwiazdki (*) oznacza operacje sterujące, których wyjście klienta FTP nie rozpoznaje. Jedynym sposobem, w jaki klient może używać tych operacji, jest uruchomienie komendy CL za pomocą komendy SYSCMD klienta FTP. Identyfikator operacji 9 steruje wykonaniem komend CL.

VLRQ0100 Parametr 3:
Profil użytkownika

INPUT; Char(10)
Profil użytkownika dla sesji FTP.

VLRQ0100 Parametr 4:
Zdalny adres IP.

INPUT; CHAR(*)
Adres IP zdalnego hosta. W przypadku połączeń protokołu IPv4 łańcuch ten ma postać dziesiętną z kropkami (123.45.67.89); w przypadku połączeń protokołu IPv6 łańcuch ten ma postać wartości oddzielonych dwukropkami (FE80::204:ACFF:FE7C:C84C). Zdalny host może być klientem lub serwerem, w zależności od ustawienia parametru identyfikatora aplikacji.

VLRQ0100 Parametr 5:
Długość (w bajtach) zdalnego adresu IP (parametru 4).

INPUT; BINARY(4)
Długość zdalnego adresu IP (parametru 4).

VLRQ0100 Parametr 6:
Informacja właściwa dla operacji.

INPUT; CHAR(*)
Informacja opisująca żądaną operację. Zawartość tego pola zależy od wartości identyfikatora operacji (parametr 2) i identyfikatora aplikacji (parametr 1). Na przykład:

Dla identyfikatora operacji 0 i identyfikatora aplikacji 0
Brak informacji właściwej dla operacji. Pole jest puste.

Dla identyfikatora operacji 0 i identyfikatora aplikacji 1
Informacje właściwe dla operacji zawierają adres IP interfejsu TCP/IP wykorzystywanego do połączenia z lokalnym hostem (serwerem FTP) dla danej sesji. Parametr ten ma format dziesiętny rozdzielony kropkami (123.45.67.89), wyrównany w lewo.

Dla identyfikatorów operacji od 1 do 3
Informacja właściwa dla operacji zawiera nazwę katalogu lub biblioteki, w której wykonywana jest operacja. Formatem dla nazwy katalogu lub biblioteki jest bezwzględna nazwa ścieżki.

Dla identyfikatorów operacji od 4 do 8
Informacja właściwa dla operacji zawiera nazwę pliku, na którym wykonywana jest operacja. Formatem nazwy pliku jest bezwzględna nazwa ścieżki.

Dla identyfikatora operacji 9
Informacje właściwe dla operacji zawierają komendę CL żądaną przez użytkownika.

VLRQ0100 Parametr 7:
Długość informacji właściwych dla operacji.

INPUT; BINARY(4)
Wskazuje długość informacji właściwej dla operacji (parametr 6). Długość wynosi 0, gdy punkt wyjścia nie dostarczy informacji właściwych dla operacji.

VLRQ0100 Parametr 8:
Zezwolenie na operację.

OUTPUT; BINARY(4)
Wskazuje, czy przyjąć, czy odrzucić żądanie operacji. W poniższej tabeli przedstawiono możliwe wartości.

Wartość	Opis
-1	*Nieprzyjmowanie* tego identyfikatora operacji: Bezwarunkowe odrzucenie identyfikatora operacji na pozostałą część bieżącej sesji. Ten identyfikator operacji nie wywoła ponownie programu obsługi wyjścia.
0	Odrzucenie operacji
1	Zezwolenie na operację
2	*Każdorazowe* przyjmowanie tego identyfikatora operacji: Bezwarunkowe przyjęcie identyfikatora operacji na pozostałą część bieżącej sesji. Ten identyfikator operacji nie wywoła ponownie programu obsługi wyjścia.

Pojęcia pokrewne

“Zarządzanie dostępem za pomocą programów obsługi wyjścia FTP” na stronie 23
Dodatkowe bezpieczeństwo można zapewnić, dodając programy obsługi wyjścia FTP do punktów wyjścia serwera i klienta FTP, które oferują więcej możliwości ograniczenia dostępu do systemu.

Uwagi dotyczące użycia formatu punktu wyjścia VLRQ0100:

VLRQ0100 jest formatem punktu wyjścia używanym zarówno przez punkt wyjścia potwierdzenia żądania klienta FTP, jak i przez punkt wyjścia potwierdzenia żądania serwera FTP. Korzystając z formatu punktu wyjścia VLRQ0100, należy uwzględnić zamieszczone w tym temacie uwagi dotyczące zastosowania.

Błędne parametry wyjściowe

Jeśli zwrócona wartość parametru Zezwolenie na operację (parametr 8) jest niepoprawna, to serwer FTP odrzuca żądanie operacji, a do protokołu zadania jest wysyłany komunikat:

Data from exit program for exit point &1 is missing or not valid (Dane z programu obsługi wyjścia dla punktu wyjścia 1 nie zostały podane lub są niepoprawne)

Wyjątki

Jeśli podczas wywołania programu obsługi wyjścia serwer FTP napotka jakikolwiek wyjątek, to do protokołu zadania wysyłany jest komunikat:

Exception encountered for FTP exit program &1 in library &2 for exit point &3 (Wystąpił wyjątek dla serwera FTP w programie obsługi wyjścia 1 w bibliotece 2 dla punktu wyjścia 3)

Zestawienie: Informacje zależne od operacji

Poniższa tabela podsumowuje informacje zależne od operacji (VLRQ0100, parametr 6) wymagane dla każdego identyfikatora operacji (VLRQ0100, parametr 2).

Identyfikator operacji (VLRQ0100 Parametr 2)	Informacje zależne od operacji (VLRQ0100 Parametr 6)
0	BRAK, jeśli ID aplikacji=0 (parametr 1)
0	Adres IP hosta klienta w formacie dziesiętnym rozdzielonym kropkami, jeśli ID aplikacji=1 lub 2 (parametr 1)
1-3	Bezwzględna nazwa ścieżki do biblioteki lub katalogu. Przykłady: /QSYS.LIB/QGPL.LIB[(a)] /QOpenSys/DirA/DirAB/DirABC[(b)]
4-8	Bezwzględna nazwa ścieżki do zbioru lub pliku. Przykłady: /QSYS.LIB/MYLIB.LIB/MYFILE.FILE/MYMEMB.MBR[(a)] /QOpenSys/DirA/DirAB/DirABC/FileA1[(b)]

Uwagi:

(a) - nazwy ścieżek systemu plików QSYS.LIB składają się zawsze z wielkich liter

(b) - w nazwach ścieżek systemu plików QOpenSys mogą występować małe i wielkie litery.

Punkt wyjścia logowania do serwera FTP

Uwierzytelnianiem logowania do serwera aplikacji TCP/IP można sterować za pomocą punktu wyjścia logowania do serwera aplikacji TCP/IP. Ten punkt wyjścia umożliwia dostęp do serwera FTP na podstawie adresu systemu, który nawiązał sesję. Dzięki temu można określić początkowy katalog roboczy inny od tego, który znajduje się w profilu użytkownika.

Jeśli do punktu wyjścia zostanie dodany program obsługi wyjścia, serwer FTP wywoła go przy każdej próbie logowania do serwera. Program obsługi wyjścia ustawia parametr wyjściowy kodu powrotu wskazujący, czy serwer FTP będzie kontynuował operację logowania. Możliwe są różne kody powrotu dla przetwarzania logowania i inicjowania informacji o katalogach.

Punktem wyjścia dla logowania do serwera FTP i5/OS jest:

QIBM_QTMF_SVR_LOGON

Dostępne są trzy formaty punktu wyjścia:

- Format TCPL0100 punktu wyjścia umożliwia sterowanie podstawowymi operacjami logowania, takimi jak:
  - akceptacja lub odrzucenie logowania,
  - sterowanie profilem użytkownika, hasłem i biblioteką bieżącą,
- Format TCPL0200 punktu wyjścia udostępnia dodatkowe parametry sterujące procesem logowania, w tym:
  - możliwość ustawienia jako katalogu roboczego dowolnego katalogu w systemie,
  - możliwość zwrócenia informacji właściwej dla aplikacji,
  - możliwość sterowania szyfrowaniem danych FTP wysyłanych do klienta FTP i otrzymywanych od klienta FTP,
- Format punktu wyjścia TCPL0300 jest rozszerzeniem formatu TCPL0200, który pozwala na zastosowanie rozszerzonej obsługi haseł w systemie i5/OS oraz dodatkowych parametrów umożliwiających przetwarzanie identyfikatorów CCSID dla pól hasła i nazwy katalogu. Ponadto, jeśli użytkownik sesji został uwierzytelniony za pomocą certyfikatu klienta, certyfikat ten jest przekazywany do programu obsługi wyjścia.

Uwagi:

1. Dla punktu wyjścia logowania do serwera FTP może być zarejestrowany tylko jeden program obsługi wyjścia. Należy zdecydować, który z trzech formatów punktu wyjścia będzie używany.
2. Dla aplikacji FTP ten punkt wyjścia umożliwia zaimplementowanie anonimowego FTP wraz z informacjami potrzebnymi do protokołowania i sterowania dostępem.
3. Dla wszystkich parametrów znakowych w formatach TCPL0100 i TCPL0200 punktu wyjścia oraz dla wszystkich parametrów znakowych bez identyfikatora CCSID w formacie TCPL0200 punktu wyjścia, dane znakowe przesyłane do programu obsługi wyjścia mają identyfikator zadania CCSID. Jeśli identyfikatorem CCSID zadania jest 65535, to dane znakowe mają domyślny identyfikator CCSID zadania. Wszelkie dane znakowe zwracane przez program obsługi wyjścia w tych parametrach, powinny mieć ten sam identyfikator CCSID.

Punkt wyjścia logowania do serwera dla anonimowego serwera FTP

Dla anonimowego serwera FTP należy napisać program logowania do serwera FTP, który będzie wykonywał następujące funkcje:

- Akceptowanie logowania od użytkowników o identyfikatorze ANONYMOUS.
- Żądanie adresu poczty elektronicznej (e-mail) jako hasła. Zazwyczaj jest wymagane podanie poprawnego adresu e-mail jako hasła. Poprawny adres e-mail jest o tyle mylący, że jedynym kryterium poprawności adresu e-mail zastosowanym przez program obsługi wyjścia jest sprawdzenie, czy w środku łańcucha znaków alfanumerycznych występuje symbol @. Dlatego ważne jest protokołowanie adresu IP użytkownika.
- Sprawdzenie, czy symbol @ występuje w łańcuchu hasła.
- Wymuszenie skierowania użytkowników anonimowych wyłącznie do biblioteki o publicznym dostępie. Patrz także kod powrotu 3 parametru 8 dla formatu TCPL0200).

Co powinien zawierać program:

- obsługę wyjątków,
- debugowanie,
- protokołowanie,
  - protokołowanie adresu IP i adresu poczty elektronicznej (wysyłanego jako hasło) requestera FTP.

Czy istnieje opcja limitu czasu w programie obsługi wyjścia?

W programach obsługi wyjścia protokołu FTP nie ma obsługi limitu czasu. Jeśli w programie obsługi wyjścia wystąpi błąd lub wyjątek, którego program ten nie będzie umiał obsłużyć, to serwer FTP przerwie sesję.

Uprawnienia niezbędne dla QTCP

Jeśli aplikacja wywołuje program obsługi wyjścia logowania do serwera, zadanie serwera FTP jest uruchamiane pod profilem użytkownika QTCP.

Należy się upewnić, czy QTCP ma uprawnienia wystarczające do dostępu i zapisu do plików protokołów lub innych plików związanych z programami obsługi wyjścia.

Przykładowe programy

Dostępne są przykładowe programy ułatwiające konfigurowanie anonimowego serwera FTP w systemie. Programy te są tylko ilustracją. Zawierają one za mało opcji, aby można je było uruchomić na maszynie produkcyjnej. Przykłady te mogą posłużyć jako wzór do pisania własnych programów. Kopiując fragmenty kodu z tych przykładów, można je dodać do własnych programów. Zalecane jest uruchamianie programów przykładowych na systemie innym niż produkcyjny.

Pojęcia pokrewne

"Kontrolowanie dostępu do serwera FTP" na stronie 17
Jeśli protokół FTP jest używany, istnieje potrzeba zachowania kontroli nad użytkownikami w celu ochrony danych i sieci. Sekcja ta zawiera wskazówki i uwagi dotyczące ochrony.

"Zarządzanie dostępem za pomocą programów obsługi wyjścia FTP" na stronie 23
Dodatkowe bezpieczeństwo można zapewnić, dodając programy obsługi wyjścia FTP do punktów wyjścia serwera i klienta FTP, które oferują więcej możliwości ograniczenia dostępu do systemu.

"Konfigurowanie anonimowego serwera FTP" na stronie 12
Anonimowy serwer FTP umożliwia zdalnym użytkownikom korzystanie z serwera FTP bez przypisanego ID użytkownika i hasła.

"Określanie problemów związanych z protokołem FTP" na stronie 152
Jeśli podczas korzystania z protokołu FTP wystąpi problem, należy za pomocą schematu oraz list przyczyn, które są zawarte w poniższym temacie, zidentyfikować przyczynę tego problemu.

Odsyłacze pokrewne

"Pisanie programów obsługi wyjścia dla anonimowego serwera FTP" na stronie 13
Aby korzystać z anonimowego serwera FTP w systemie operacyjnym i5/OS, należy napisać dwa programy obsługi wyjścia: program obsługi wyjścia logowania do serwera FTP i program obsługi wyjścia potwierdzenia żądania protokołu FTP.

Przykład: kod programu obsługi wyjścia logowania do serwera FTP w języku CL:

Przedstawiony przykład jest prostym programem obsługi wyjścia logowania do serwera FTP. Jest on napisany w języku programowania CL.

Poniższy kod nie jest kompletny, ale może służyć jako punkt wyjścia do utworzenia własnego programu.

Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki zapisane w sekcji "Licencja na kod oraz Informacje dotyczące kodu" na stronie 159.

(Wstępnie sformatowany tekst w poniższym przykładzie nie mieści się w ramce.)

```
/*********************************************************************/
/*                                                                   */
/*    Przykładowy program obsługi wyjścia logowania do serwera FTP.                                  */
/*    Uwaga: Ten program jest tylko przykładem i nie przechodził formalnego   */
/*           przeglądu i testowania.                                 */
```

```
/*                                                                    */
/*  Uwagi dodatkowe:                                                  */
/*  1. Gdy zostanie wywołany program obsługi wyjścia logowania do serwera FTP,*/
/*     to zadanie serwera FTP jest uruchamiane pod profilem użytkownika QTCP. */
/*  2. W przypadku użytkownika anonimowego można zwiększyć ilość informacji   */
/*     protokołowanych (np. zapisywać adres e-mail podawany jako hasło oraz   */
/*     adres IP klienta do pliku protokołu).                          */
/*  3. Firma IBM zaleca, aby utworzyć program obsługi wyjścia w bibliotece    */
/*     z uprawnieniami *PUBLIC ustawionymi na *EXCLUDE oraz nadać mu          */
/*     uprawnienia *PUBLIC ustawione na *EXCLUDE. Serwer FTP zaadaptuje       */
/*     uprawnienia, gdy
będzie to konieczne do określenia i wywołania         */
/*     programu obsługi wyjścia.                                      */
/*                                                                    */
/**********************************************************************/

 TSTLOGCL:   PGM        PARM(&APPIDIN &USRIN &USRLENIN &AUTIN &AUTLENIN +
                           &IPADDRIN &IPLENIN &RETCDOUT &USRPRFOUT &PASSWDOUT +
                           &CURLIBOUT)

/* Deklaracja parametrów wejściowych                                                 */
             DCL        VAR(&APPIDIN)    TYPE(*CHAR) LEN(4)  /* Identyfikator aplikacji */
             DCL        VAR(&USRIN)      TYPE(*CHAR) LEN(999)/* ID użytkownika          */
             DCL        VAR(&USRLENIN)   TYPE(*CHAR) LEN(4)  /* Długość ID użytkownika  */
             DCL        VAR(&AUTIN)      TYPE(*CHAR) LEN(999)/* Łańcuch uwierzyteln.    */
             DCL        VAR(&AUTLENIN)   TYPE(*CHAR) LEN(4)  /* Dł. łańc. uwierzyteln.  */
             DCL        VAR(&IPADDRIN)   TYPE(*CHAR) LEN(15) /* Adres IP klienta        */
             DCL        VAR(&IPLENIN)    TYPE(*CHAR) LEN(4)  /* Długość adresu IP       */
             DCL        VAR(&RETCDOUT)   TYPE(*CHAR) LEN(4)  /* Kod powrotu (wyjściowy) */
             DCL        VAR(&USRPRFOUT)  TYPE(*CHAR) LEN(10) /* Profil użytkownika (wyj)*/
             DCL        VAR(&PASSWDOUT)  TYPE(*CHAR) LEN(10) /* Hasło (wyjściowe)       */
             DCL        VAR(&CURLIBOUT)  TYPE(*CHAR) LEN(10) /* Bieżąca biblioteka (wyj)*/

/* Deklaracja lokalnych kopii parametrów (w formacie używanym przez CL)              */
             DCL        VAR(&APPID)     TYPE(*DEC)  LEN(1 0)
             DCL        VAR(&USRLEN)     TYPE(*DEC) LEN(5 0)
             DCL        VAR(&AUTLEN)     TYPE(*DEC) LEN(5 0)
             DCL        VAR(&IPLEN)     TYPE(*DEC) LEN(5 0)

/* Przypisanie parametrów wejściowych do kopii lokalnych                             */
             CHGVAR     VAR(&APPID)     VALUE(%BINARY(&APPIDIN))
             CHGVAR     VAR(&USRLEN)     VALUE(%BINARY(&USRLENIN))
             CHGVAR     VAR(&AUTLEN)     VALUE(%BINARY(&AUTLENIN))
             CHGVAR     VAR(&IPLEN)     VALUE(%BINARY(&IPLENIN))

/* Sprawdzenie, czy jest to użytkownik ANONYMOUS.  Pozwolenie na dostęp użytkowników  */
/* ANONYMOUSA itd. na "standardowych" zasadach                                       */
/* i od tej pory traktowanie go jako "regularnego" profilu użytkownika.          */
             IF       COND(&USRLEN = 9) THEN(DO)
               IF       COND(%SST(&USRIN 1 9) = 'ANONYMOUS') THEN(DO)
/* Dla użytkowników anonimowych : wymuszenie ustawienia bieżącej biblioteki w profilu */
/* użytkownika anonimowego na PUBLIC                                                 */
                 CHGVAR VAR(%BINARY(&RETCDOUT))  VALUE(6)
                 CHGVAR VAR(&USRPRFOUT)  VALUE('ANONYMOUS ')
                 CHGVAR VAR(&CURLIBOUT)  VALUE('PUBLIC    ')
               ENDDO
/* Inni użytkownicy: wykonanie normalnego przetwarzania logowania                    */
               ELSE     CMD(CHGVAR VAR(%BINARY(&RETCDOUT))  VALUE(1))
             ENDDO
             ELSE     CMD(CHGVAR VAR(%BINARY(&RETCDOUT))  VALUE(1))

 END:        ENDPGM
```

Przykład: kod programu obsługi wyjścia logowania do serwera FTP w języku C:

Przedstawiony przykład jest prostym programem obsługi wyjścia logowania do serwera FTP. Jest on napisany w języku programowania C.

Kod tego programu nie jest kompletny, ale jest punktem wyjścia do tworzenia własnego programu.

Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki zapisane w sekcji “Licencja na kod oraz Informacje dotyczące kodu” na stronie 159.

(Wstępnie sformatowany tekst w poniższym przykładzie nie mieści się w ramce.)

```
/* Opis Modułu ************************************************************/
/*                                                                        */
/**************************************************************************/
/*                                                                        */
/* Uwaga: Ten program jest tylko przykładem i nie przechodził             */
/*         formalnego przeglądu i testowania.                             */
/*                                                                        */
/**************************************************************************/
/*                                                                        */
/* Nazwa pliku źródłowego: qtmfsvrlgn.c                                   */
/*                                                                        */
/* Nazwa modułu: program obsługi wyjścia logowania do serwera FTP         */
/*                                                                        */
/* Nazwa programu serwisowego:  ND                                        */
/*                                                                        */
/* Opis pliku źródłowego:                                                 */
/*   Ten przykładowy program obsługi wyjścia pozwala na dodatkowe         */
/*    sterowanie podczas procesu uwierzytelniania użytkowników na         */
/*    serwerze aplikacji TCP/IP.                                          */
/*    Po zainstalowaniu, ten przykładowy program obsługi wyjścia          */
/*    będzie wywoływany podczas każdej próby zalogowania do serwera.      */
/*                                                                        */
/**************************************************************************/
/*                                                                        */
/* Lista funkcji: main       - Część główna programu obsługi wyjścia      */
/*                             logowania do serwera FTP.                  */
/*                qtmfsvrlgn - Funkcja programu obsługi wyjścia           */
/*                             logowania do serwera FTP.                  */
/*                CheckClientAddress - Sprawdzanie adresu IP              */
/*                                     inicjowanej sesji.                 */
/*                                                                        */
/* Koniec opisu modułu ****************************************************/
#define _QTMFSVRLGN_C



/**************************************************************************/
/* Wszystkie pliki nagłówkowe znajdują się tutaj                          */
/**************************************************************************/
#ifndef __stdio_h
#include <stdio.h>
#endif

#ifndef __ctype_h
#include <ctype.h>
#endif

#ifndef __string_h
#include <string.h>
#endif

#ifndef __stdlib_h
#include <stdlib.h>
#endif

#include "qusec.h"            /* Include for API error code structure */
```

```
#include "qsyrusri.h"         /* Include for User Information API     */

/*********************************************************************/
/* Wszystkie stałe w zakresie całego pliku znajdują się tutaj        */
/*********************************************************************/
#define  EQ      ==
#define  NEQ     !=
#define  BLANK   ' '
#define  FWIDTH  128   /* Wielkość jednego rekordu bazy danych        */
#define  FNAME   21    /* Wielkość nazwy bazy danych                  */

/* Poprawne znaki dla adresu IP klienta. Funkcja CheckClientAddress() */
/* sprawdzi argument wejściowy adresu IP klienta                      */
/* (ClientIPaddr_p), aby upewnić się, czy ma on poprawny format       */
/* dziesiętny z kropkami.                                             */
/* To jest przykład kontroli poprawności wejścia.                    */
const char ValidChars[] = "0123456789.";
/*********************************************************************/
/* Wszystkie deklaracje w zakresie całego pliku znajdują się tutaj    */
/*********************************************************************/


/*********************************************************************/
 /* Wszystkie wywołania makrodefinicji znajdują się tutaj            */
/*********************************************************************/


/*********************************************************************/
/* Wszystkie prototypy funkcji wewnętrznych znajdują się tutaj       */
/*********************************************************************/

static void qtmfsvrlgn
    (int,char *,int,char *,int,char *,int,int *,char *,char *,char *);

static int CheckClientAddress(char *, int);


/*********************************************************************/
/* Wszystkie deklaracje zmiennych znajdują się tutaj                 */
/*********************************************************************/


/*********************************************************************/
/*                                ** UWAGA **                        */
/* Poniższy adres IP klienta jest przykładowy. Ewentualne podobieństwo*/
/* do adresu IP rzeczywistego systemu jest przypadkowe.              */
/*********************************************************************/

/* WYKLUCZAJĄCA lista systemowa - Próba logowania z adresu IP klienta */
/*                                NIE z listy jest dozwolona.         */
/*                                                                    */
/* Odrzucenie próby logowania do serwera użytkowników z następujących */
/* systemów-klientów (kod powrotu = 0)                                */
char Reject[] = "1.2.3.4 5.6.7.8";
/* Ograniczenie możliwości logowania użytkowników starających się     */
/* zalogować jako ANONYMOUS z poniższych systemów-klientów            */
/* (kod powrotu = 6).                                                 */
/* W tym przykładowym programie początkowa biblioteka bieżąca jest    */
/* ustawiana i zwracana jako parametr wyjściowy do użytkowników       */
/* starających się zalogować jako ANONYMOUS z poniższych              */
/* systemów-klientów.                                                 */
char Limit[] = "9.8.7.6 4.3.2.1 8.7.6.5";

/* Specyfikacja funkcji ********************************************/
/*                                                                    */
/* Nazwa funkcji: Main                                                */
/*                                                                    */
```

```
/* Nazwa opisowa: Część główna programu obsługi wyjścia logowania do  */
/* serwera FTP.                                                       */
/*                                                                    */
/*    Ten przykładowy program obsługi wyjścia umożliwia sterowanie    */
/*    dostępem do serwera TCP/IP przez adres sesji początkowej, daje  */
/*    użytkownikowi dodatkowe sterowanie początkową biblioteką        */
/*    bieżącą i udostępnia możliwość zaimplementowania anonimowego
      dostępu FTP.       */
/*                                                                    */
/* Uwagi:                                                             */
/*                                                                    */
/*   Zależności:                                                      */
/*     Punkt wyjścia logowania do serwera FTP                         */
/*     QIBM_QTMF_SVR_LOGON zostanie zarejestrowany                    */
/*     podczas instalacji produktu FTP.                               */
/*                                                                    */
/*   Ograniczenia:                                                    */
/*                                                                    */
/*       Brak                                                         */
/*                                                                    */
/*   Komunikaty:                                                      */
/*                                                                    */
/*       Brak                                                         */
/*                                                                    */
/*   Efekty uboczne:                                                  */
/*                                                                    */
/*       Brak                                                         */
/*                                                                    */
/*   Wywoływane funkcje/makro:                                        */
/*                                                                    */
/*       qtmfsvrlgn - Funkcja obsługi wyjścia logowania do serwera    */
/*                                                                    */


/* Wejście:                                                           */
/*   int  * argv[1]     - Identyfikuje aplikację dokonującą żądania   */
/*                          (Klient FTP = 0, Serwer FTP = 1).         */
/*   char * argv[2]     - Identyfikator użytk. z programu klienta.    */
/*                        (Dla serwera FTP są do dane CMD użytkownika)*/
/*   int  * argv[3]     - Długość (w bajtach) łańcucha ID użytkownika.*/
/*   char * argv[4]     - Łańcuch uwierzytelniający z klienta.        */
/*                                (Dla serwera FTP jest to hasło)     */
/*   int  * argv[5]     - Długość (bajty) łańcucha uwierzytelniającego*/
/*   char * argv[6]     - Adres IP, z którego                         */
/*                               inicjowana jest sesja.               */
/*   int  * argv[7]     - Długość (w bajtach) adresu IP.              */
/*   int  * argv[8]     - Kod powrotu (otrzymywany jako 0).           */
/*   char * argv[9]     - Profil użytk. (otrzymany jako łańcuch pusty)*/
/*   char * argv[10]    - Hasło (otrzymywane jako łańcuch pusty).     */
/*   char * argv[11]    - Początkowa biblioteka bieżąca (otrzymywana  */
/*                        jako łańcuch pusty).                        */
/*                                                                    */
/* Normalne wyjście: Zwrot kodu zakończenia, profilu, hasła,          */
/*                   począt. biblioteki bieżącej do aplikacji serwera.*/
/*                                                                    */
/* Zakończenie z błędem: Brak                                         */
/*                                                                    */
/* Koniec specyfikacji funkcji ****************************************/
void main(int argc, char *argv[])
{
 /*********************************************************************/
 /* Kod                                                               */
 /*********************************************************************/

 /*********************************************************************/
 /* Zebranie argumentów wejściowych i wywołanie funkcji określającej,*/
 /* czy klient ma pozwolenie na logowanie do serwera aplikacji FTP.  */
```

```
 /*****************************************************************/
 qtmfsvrlgn(*((int *)(argv[1])),  /* Identyfikator aplikacji
(Wejściowy) */
             argv[2],            /* Identyfikator użytk. (Wejściowy)*/
             *((int *)(argv[3])), /* Długość identyfikatora użytk.
(Wejściowy)                                                      */
             argv[4],            /* Łańcuch uwierzytel. (Wejściowy) */
             *((int *)(argv[5])), /* Długość łańcucha uwierzytel.    */
(Wejściowy) */
             argv[6],            /* Adres IP klienta    (Wejściowy) */
             *((int *)(argv[7])), /* Długość adresu IP klienta       */
(Wejściowy) */
             (int *)(argv[8]),    /* Kod powrotu          (Wyjściowy)*/
             argv[9],            /* Profil użytkownika   (Wyjściowy)*/
             argv[10],           /* Hasło                (Wyjściowy)*/
             argv[11]);          /* Początkowa biblioteka bieżąca   */
                                 /* (Wyjściowy)                     */
  return;
}



/* Specyfikacja funkcji ********************************************/
/*                                                                 */
/* Nazwa funkcji: qtmfsvrlgn                                       */
/*                                                                 */
/* Nazwa opisowa: Funkcja obsługi wyjścia logowania do serwera.    */
/*                                                                 */
/*   Funkcja ta umożliwia sterowanie uwierzytelnianiem użytkownika na */
/*   poziomie serwera FTP.                                         */
/*                                                                 */
/* Uwagi:                                                          */
/*                                                                 */
/*   Zależności:                                                   */
/*                                                                 */
/*       Punkt wyjścia logowania do serwera FTP                    */
/*       QIBM_QTMF_SVR_LOGON został zarejestrowany                 */
/*       podczas instalacji produktu FTP.                          */
/*                                                                 */
/*   Ograniczenia:                                                 */
/*                                                                 */
/*       Brak                                                      */
/*                                                                 */
/*   Komunikaty:                                                   */
/*                                                                 */
/*       Brak                                                      */
/*                                                                 */
/*   Efekty uboczne:                                               */
/*                                                                 */
/*       Brak                                                      */
/*                                                                 */
/*   Wywoływane funkcje/makro:                                     */
/*                                                                 */
/*       CheckClientAddress - Sprawdza argument wejściowy          */
/*                            ClientIPaddr_p.                      */
/*       memcpy  - Kopiuje bajty z miejsca źródłowego do docelowego. */
/*       memset  - Ustawia wartość bajtów.                         */
/*       strstr  - Znajduje pierwsze wystąpienie podciągu.         */
/*       sprintf - Sformatowany wydruk do buforu.                  */
/*                                                                 */
/* Wejście:                                                        */
/*   int    ApplId           - Identyfikator aplikacji (Serwer = 1). */
/*   char * UserId_p         - Identyfikator użytkownika z programu */
/*                             klienta                             */
/*                             (Dla serwera FTP są to dane komendy */
/*                             USER).                              */
/*   int    Lgth_UserId      - Długość(w bajtach) łańcucha ID      */
```

```
/*                              użytkownika.                          */
/*   char * AuthStr_p         - Łańcuch uwierzytelniający z klienta   */
/*                              (Dla serwera FTP jest to hasło).      */
/*   int    Lgth_AuthStr      - Długość (bajty) łańcucha              */
/*                              uwierzytelniającego.                  */
/*   char * ClientIPaddr_p    - Adres IP, z którego                   */
/*                              inicjowana jest sesja.                */
/*   int  * Lgth_ClientIPaddr - Długość (w bajtach) adresu IP.        */
/*                                                                    */


/* Wyjście:                                                          */
/*   int * ReturnCode: Wskazuje stopień poprawności wykonania operacji:            */
/*        ReturnCode = 0 - Odrzucenie logowania.                                    */
/*        ReturnCode = 1 - Kontynuacja logowania; użycie pocz. biblioteki bieżącej  */
/*        ReturnCode = 2 - Kontynuacja logowania; przesłonięcie pocz. biblioteki    */
/*                         bieżącej.                                                */
/*        ReturnCode = 3 - Kontynuacja logowania; przesłonięcie użytkownika i hasła */
/*        ReturnCode = 4 - Kontynuacja logowania; przesłonięcie użytkownika, hasła  */
/*                         i bieżącej biblioteki                                    */
/*        ReturnCode = 5 - Akceptacja logowania; przesłonięcie profilu użytkownika  */
/*        ReturnCode = 6 - Akceptacja logowania; przesłonięcie profilu użytkownika  */
/*                         i bieżącej biblioteki                                    */
/*   char * UserProfile  - Profil użytkownika, który ma zostać użyty w tej sesji    */
/*   char * Password     - Hasło, które ma zostać użyte w tej sesji                 */
/*   char * Init_Cur_Lib - Początkowa biblioteka bieżąca dla tej sesji              */
/*                                                                    */
/* Zakończenie normalne: (Patrz WYJŚCIE)                            */
/*                                                                    */
/* Zakończenie z błędem: Brak                                       */
/*                                                                    */
/* Koniec specyfikacji funkcji ****************************************/
static void qtmfsvrlgn(int ApplId,          /* Punkt wejściowy       */
                       char *UserId_p,
                       int Lgth_UserId,
                       char *AuthStr_p,
                       int Lgth_AuthStr,
                       char *ClientIPaddr_p,
                       int Lgth_ClientIPaddr,
                       int *ReturnCode,
                       char *UserProfile_p,
                       char *Password_p,
                       char *InitCurrLib_p)
{
  /********************************************************************/
  /* Zmienne lokalne                                                  */
  /********************************************************************/
  /* Następująca lista jest przykładem dodatkowej warstwy                          */
  /* sterowania uwierzytelnianiem użytkowników na poziomie serwera aplikacji.      */
  /*  Operacje logowania z użyciem poniższych identyfikatorów użytkownika          */
  /*  są kontynuowane, ale parametry wyjściowe zwracane                            */
  /*  przez ten przykładowy program obsługi wyjścia zależą od tego, na której      */
  /*  liście znajduje się identyfikator użytkownika (UserId_p).                    */
  /*  Na przykład próba logowania jako FTPUSR11 lub FTPUSR2 zostanie               */
  /*  zaakceptowana, a ten przykład programu zwróci parametr wyjściowy             */
  /*  początkowej biblioteki
  */
  /*  bieżącej oraz kod powrotu 2.                                                 */
  /********************************************************************/
  /* Kontynuacja operacji logowania, kod powrotu = 1                               */
  char Return1[] = "FTPUSR10  ";
  /* Kontynuacja operacji logowania, kod powrotu = 2                               */
  char Return2[] = "FTPUSR11  FTPUSR2   ";
  /* Kontynuacja operacji logowania, kod powrotu = 3                               */
  char Return3[] = "FTPUSR12  FTPUSR3   FTPUSR23  ";
  /* Kontynuacja operacji logowania, kod powrotu = 4                               */
  char Return4[] = "FTPUSER   FTPUSR4   FTPUSR24  FTPUSR94  ";
```

```
int rc;                          /* Wynik żądania logowania do serwera      */
Qsy_USRI0300_T Receiver_var;     /* Zmienna Receiver funkcji QSYRUSRI       */
                                       /* interfejsu API                          */
int   Lgth_Receiver_var;         /* Długość zmiennej Receiver               */
char  Format_Name[8];            /* Bufor nazwy formatu                     */
char  User_Id[10];               /* Bufor identyfikatora użytkownika        */
Qus_EC_t error_code =            /* Struktura kodów błędów funkcji QSYRUSRI */
                                       /* interfejsu API:                         */
{
 sizeof(Qus_EC_t),               /* Ustawienie wielkości                    */
 0,                              /* Inicjacja bajtów                        */
 ' ',' ',' ',' ',' ',' ',' '     /* Inicjacja identyfikatora wyjątku        */
};
char *pcTest_p;                  /*  Wskaźnik na identyfikator użytkownika  */
                                       /*  (wielkie litery)                       */
int i;                                 /*  Zmienna licznika pętli "For"           */



/*********************************************************************/
/* Kod                                                               */
/*********************************************************************/

/* Testowanie poprawności argumentu wejściowego ID aplikacji        */
if(1 NEQ ApplId)
  {
  /* BŁĄD - Aplikacja nie jest aplikacją serwera FTP.                */
  /*         Kod powrotu 0 jest używany aby wskazać, że              */
  /*         został otrzymany niepoprawny argument wejściowy.        */
  /*         Operacja logowania na serwer zostanie odrzucona.        */
  rc = 0;                                /* Błędny ID aplikacji      */
  }      /* Koniec, jeśli identyfikator aplikacji NIE jest serwerem */
         /* FTP                                                      */
else                        /* Identyfikator aplikacji serwera FTP */
  {
  /* Zatwierdzenie argumentu wejściowego adresu IP klienta.          */
  rc = CheckClientAddress(ClientIPaddr_p,
                    Lgth_ClientIPaddr);
  if(0 NEQ rc)               /* Poprawny, dopuszczalny adres klienta*/
    {
    /* Inicjacja User_Id; zmienna ta przechowuje identyfikator       */
    /* użytkownika (wielkie litery)                                  */
    memset(User_Id, BLANK, sizeof(User_Id));

    /* Inicjacja pcTest_p wskazującego na argument wejściowy         */
    /* UserId_p.                                                     */
    pcTest_p = UserId_p;

    /* Zapisanie wszystkich ID użytkowników wielkimi literami, aby   */
    /* porównać z użytkownikiem ANONYMOUS.                           */
    for(i = 0; i < Lgth_UserId; i++)
      {
      User_Id[i] = (char)toupper(*pcTest_p);
      pcTest_p += 1;
      }

    /* Jeśli użytkownik zalogował się jako ANONYMOUS.                */
    if(0 == memcmp("ANONYMOUS ", User_Id, 10))
      {
      /* Określenie postępowania podczas próby logowania ANONYMOUS. */
      if(NULL NEQ strstr(Limit, ClientIPaddr_p))
        {
        /* Jeśli adres IP systemu użytkowników został znaleziony na liście "Limit", */
        /* zwrócenie kodu powrotu 6, profilu użytkownika i początkowej              */
        /* biblioteki bieżącej jako parametrów wyjściowych.                         */
        memcpy(UserProfile_p, "USERA1    ", 10);
        memcpy(InitCurrLib_p, "PUBLIC    ", 10);
```

```
    rc = 6;
    }
  else
    {
    /* Adres IP systemu użytkowników NIE został znaleziony na liście "Limit",*/
    /* zwrócenie kodu powrotu 5, parametru wyjściowego profilu użytkownika:  */
    /* użycie początkowej biblioteki bieżącej określonej przez               */
    /* informacje profilu użytkownika.                                       */
    memcpy(UserProfile_p, "USERA1    ", 10);
    rc = 5;
    }
  }              /* Koniec, jeśli UŻYTKOWNIKIEM jest ANONYMOUS  */


else                          /* Jeśli UŻYTKOWNIKIEM nie jest ANONYMOUS      */
  {
  /* Ustawienie długości zmiennej Receiver                                    */
  Lgth_Receiver_var = sizeof(Qsy_USRI0300_T);
  /* Ustawienie formatu zwracanej informacji.                                 */
  memcpy(Format_Name, "USRI0300", sizeof(Format_Name));
  /* Ustawienie przekazywanego identyfikatora użytkownika                     */
  memset(User_Id, BLANK, sizeof(User_Id));
  memcpy(User_Id, UserId_p, Lgth_UserId);
  /* Wywołanie funkcji API QSYRUSRI - Retrieve User Information               */
  QSYRUSRI(&Receiver_var,    /* Zwracana: zmienna Receiver  */
           Lgth_Receiver_var,    /* Długość zmiennej            */
           Format_Name,          /* Nazwa formatu zwracanej inf.*/
           User_Id,              /* Informacja przeszukiwania   */
                                          /* ID użytkownika             */
           &error_code);                 /* Zwrócona informacja: błąd   */
  /* Sprawdzenie wystąpienia błędu (byte_available różna od 0)                */
  if(0 NEQ error_code.Bytes_Available)
    {
    /* Tylko zwrócenie kodu powrotu 0 (Odrzucenie logowania);                 */
    rc = 0;                    /* Odrzucenie operacji logowania     */
    *ReturnCode = rc;                     /* Przypisanie wyniku do ReturnCode*/
    }
  else                             /* Nie wystąpił błąd w Retrieve User Info*/
    {                              /* (Bytes_Available = 0)                  */
    /* Ustawienie bieżącej biblioteki dla profilu użytkownika                 */
    memcpy(InitCurrLib_p, Receiver_var.Current_Library, 10);
    if(NULL NEQ strstr("*CRTDFT   ",
                       Receiver_var.Current_Library))
      {
      memcpy(InitCurrLib_p, "FTPDEFAULT", 10);
      }
    else
      {
      if(NULL NEQ strstr(Return1, UserId_p))
        {
        /* Zwrócenie ReturnCode = 1 (Kontynuacja logowania).               */
        /*  Zwrócenie także parametrów wyjściowych profilu użytkownika     */
        /*  i hasła, aby zapewnić, że zostaną one zignorowane przez serwer.*/
        memcpy(UserProfile_p, UserId_p, Lgth_UserId);
        memcpy(Password_p, AuthStr_p, Lgth_AuthStr);
        rc = 1;               /* Kontynuacja operacji logowania         */

        }
      else
        {
        if(NULL NEQ strstr(Return2, UserId_p))
          {
          /* Zwrócenie ReturnCode = 2 oraz początkowej biblioteki bieżącej */
          /*  Zwrócenie także wartości profilu użytkownika i hasła,        */
          /*  pomimo że zostaną one zignorowane przez serwer.              */
          memcpy(UserProfile_p, UserId_p, Lgth_UserId);
          memcpy(Password_p, AuthStr_p, Lgth_AuthStr);
```

```
                memcpy(InitCurrLib_p, "FTPEXT2",
                                      strlen("FTPEXT2"));
                rc = 2;              /* Kontynuacja logowania; zwrócenie InitCurLib */
                }


              else
                {
                if(NULL NEQ strstr(Return3, UserId_p))
                  {
                  /* Zwrócenie ReturnCode = 3 oraz profilu użytkownika i hasła.  */
                  /*  Zwrócenie także wartości początkowej biblioteki bieżącej,  */
                  /*  pomimo że zostanie ona zignorowana.                        */
                  memcpy(UserProfile_p, UserId_p, Lgth_UserId);
                  memcpy(Password_p, AuthStr_p, Lgth_AuthStr);

                  memcpy(InitCurrLib_p, "FTPEXT3",
                                strlen("FTPEXT3")); /* Serwer ignoruje           */
                  rc = 3;
                  }
                else
                  {
                  if(NULL NEQ strstr(Return4, UserId_p))
                    {
                    /*Zwrócenie ReturnCode = 4 oraz wartości profilu użytkownika,           */
                    /* hasła i początkowej biblioteki bieżącej                              */
                    memcpy(UserProfile_p, UserId_p, Lgth_UserId);
                    memcpy(Password_p, AuthStr_p, Lgth_AuthStr);
                    memcpy(InitCurrLib_p, "FTPEXT4",
                                          strlen("FTPEXT4"));

                    rc = 4;
                    }
                  else
                    /* To jest wartość domyślna kodu powrotu dla                          */
                    /* próby logowania za pomocą jakiegokolwiek identyfikatora            */
                    /* nieznajdującego się na żadnej z czterech list                      */
                    /* zdefiniowanych w części zmiennych lokalnych tej funkcji.           */
                    {
                    /*Zwrócenie ReturnCode = 1, kontynuacja operacji logowania            */
                    rc = 1;
                    }
                  }
                }
              }
            }            /* Koniec: Nie wystąpił żaden błąd (byte_available = 0) */
          }              /* Koniec: Jeśli UŻYTKOWNIKIEM nie jest ANONYMOUS       */
        }                /* Koniec: Poprawny, dopuszczalny adres klienta         */
      }                  /* Koniec: Identyfikator aplikacji serwera FTP          */
    *ReturnCode = rc;
    return;
}                                     /* Koniec programu qtmfsvrlgn.c */



/* Specyfikacja funkcji ********************************************/
/*                                                                 */
/* Nazwa funkcji: CheckClientAddress                               */
/*                                                                 */
/* Nazwa opisowa: Sprawdzanie adresu IP inicjowanej sesji znajdującego*/
/*                się w argumencie wejściowym (ClientIPaddr_p), dla   */
/*                upewnienia się, czy ma on poprawny format dziesiętny*/
/*                oraz czy system klient ma zezwolenie na dostęp.     */
/*                Jest to przykład kontroli poprawności wejścia.      */
/*                                                                 */
```

```
/* Uwagi:                                                            */
/*                                                                   */
/*   Zależności:                                                     */
/*       Brak                                                        */
/*                                                                   */
/*   Ograniczenia:                                                   */
/*       Brak                                                        */
/*                                                                   */
/*   Komunikaty:                                                     */
/*       Brak                                                        */
/*                                                                   */
/*   Efekty uboczne:                                                 */
/*       Brak                                                        */
/*                                                                   */
/*   Wywoływane funkcje/makro:                                       */
/*                                                                   */
/*       strspn - Szukanie pierwszego wystąpienia łańcucha.          */
/*                                                                   */
/* Wejście:                                                          */
/*   char * ClientIPaddr_p    - Adres IP, z którego                  */
/*                              inicjowana jest sesja.               */
/*   int  * Lgth_ClientIPaddr - Długość (w bajtach) adresu IP.       */
/*                                                                   */
/* Wyjście:                                                          */
/*   int    rc                - Kod powrotu wskazujący poprawność    */
/*                              adresu IP pochodzącego z wejścia     */
/*                              ClientIPaddr_p.                      */
/*                            0 = Odrzucenie operacji logowania.     */
/*                                ClientIPaddr_p jest jednym z       */
/*                                niedozwolonych lub zawiera         */
/*                                niedozwolony znak.                 */
/*                            1 = Kontynuacja operacji logowania.    */
/*                                                                   */
/* Zakończenie normalne: (Patrz WYJŚCIE)                             */
/*                                                                   */
/* Zakończenie z błędem: Brak                                        */
/*                                                                   */
/* Koniec specyfikacji funkcji ***************************************/


static int CheckClientAddress(char *ClientIPaddr_p, /* Punkt wejściowy*/
                              int Lgth_ClientIPaddr)
{
  /*********************************************************************/
  /* Zmienne lokalne                                                   */
  /*********************************************************************/
  int rc;                                             /* Kod powrotu */

  /*********************************************************************/
  /* Kod                                                               */
  /*********************************************************************/

  /* Sprawdzenie, czy argument wejściowy adresu IP klienta jest w     */
  /* formacie dziesiętnym o odpowiedniej długości, nie zawiera znaków */
  /* pustych początku lub przerw i zawiera tylko poprawne znaki.      */
  if((Lgth_ClientIPaddr < 7) ||         /* Minim.długość adresu IP */
     (strspn(ClientIPaddr_p, ValidChars) < Lgth_ClientIPaddr)||
     (strspn(ClientIPaddr_p, ".") EQ 1)||  /* Czołowy znak '.' w adresie IP*/
     (strspn(ClientIPaddr_p, " ") EQ 1))   /* Czołowa spacja w adresie IP  */
    {
    /* Adres IP klienta jest niepoprawny lub zawiera niepoprawne znaki*/
    rc = 0;  /* Argument wejściowy adresu IP klienta jest niepoprawny */
    }
  else
    {
    /* Czy system-klient ma zezwolenie na logowanie do serwera FTP    */
    if(NULL NEQ strstr(Reject, ClientIPaddr_p))
```

```
        {
        /* Kod powrotu = 0 - Odrzucenie operacji logowania do serwera,  */
        /*                   ponieważ adres klienta został znaleziony   */
        /*                   Lista "Reject".                             */
        rc = 0;                   /* Odrzucenie operacji logowania     */
        }
      else
        {
        /* Kontynuacja operacji logowania do serwera.                   */
        rc = 1;               /* Kontynuacja operacji logowania         */
        }
      }
    return(rc);
  }

  #undef _QTMFSVRLGN_C
```

Przykład: kod programu obsługi wyjścia logowania do serwera FTP w języku ILE RPG:

Przedstawiony przykład jest prostym programem obsługi wyjścia logowania do serwera FTP. Jest napisany w języku ILE RPG.

Kod tego programu nie jest kompletny, ale jest punktem wyjścia do tworzenia własnego programu.

Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki zapisane w sekcji “Licencja na kod oraz Informacje dotyczące kodu” na stronie 159.

(Wstępnie sformatowany tekst w poniższym przykładzie nie mieści się w ramce.)

```
     *Opis modułu ***********************************************
     *                                                           *
     *************************************************************
     *                                                           *
     * Uwaga: Ten program jest tylko przykładem i nie przechodził*
     *        formalnego przeglądu i testowania.                 *
     *                                                           *
     *************************************************************
     *                                                           *
     *                     FUNKCJA PROGRAMU                      *
     *                                                           *
     * Program ten demonstruje kilka możliwości, które może mieć*
     * program obsługi wyjścia logowania do serwera FTP.         *
     *                                                           *
     *************************************************************
     F/SPACE 3
     *************************************************************
     *                                                           *
     *                      UŻYTE WSKAŹNIKI                      *
     *                                                           *
     *   WSK.  OPIS                                              *
     *                                                           *
     *    LR - ZAMKNIĘCIE PLIKÓW PRZY WYJŚCIU                    *
     *                                                           *
     *************************************************************
     F/EJECT
     *************************************************************
     * STRUKTURY DANYCH UŻYWANE PRZEZ PROGRAM                    *
     *************************************************************
     *
     * Definicje stałych
     *
1    D Anonym          C                   CONST('ANONYMOUS ')
     D Text1           C                   CONST('Anonymous (')
     D Text2           C                   CONST(') FTP logon')
     D InvalidNet      C                   CONST('10.')
```

```
C/EJECT
*****************************************************************
* DEFINICJE ZMIENNYCH I LISTY UŻYWANE PRZEZ PROGRAM             *
*****************************************************************
C/SPACE 2
 *
 * Definicje parametrów binarnych
 *
D                 DS
D  APPIDds                1      4B 0
D  USRLENds               5      8B 0
D  AUTLENds               9     12B 0
D  IPLENds               13     16B 0
D  RETCDds               17     20B 0
 *
C     *LIKE         DEFINE    APPIDds       APPIDIN
C     *LIKE         DEFINE    USRLENds      USRLENIN
C     *LIKE         DEFINE    AUTLENds      AUTLENIN
C     *LIKE         DEFINE    IPLENds       IPLENIN
C     *LIKE         DEFINE    RETCDds       RETCDOUT
 *
 * Definicje listy parametrów
 *
C     *Entry        PLIST
 * Parametry wejściowe:
C                   PARM                    APPIDIN                        ID aplikacji
 *                                                 możliwe wartości:  1 = program serwera FTP
C                   PARM                    USRIN           999            ID użytkownika
C                   PARM                    USRLENIN                       Długość ID użytkownika
C                   PARM                    AUTIN           999            Łań. uwierzytelniający
C                   PARM                    AUTLENIN                       Długość łań. uwierz.
C                   PARM                    IPADDRIN         15            Adres IP klienta
C                   PARM                    IPLENIN                        Długość adresu IP
 * Parametry zwracane:
C                   PARM                    RETCDOUT                       Kod powrotu (Wyjście)
 *                                                 możliwe wartości:  0 = Odrzucenie logowania
 *                                                                    1 = Kontynuacja logowania
 *                                                                    2 = Kontynuacja logowania,
 *                                                                        zastąpienie bieżącej
 *                                                                        biblioteki
 *                                                                    3 = Kontynuacja logowania,
 *                                                                        przesłonięcie profilu
 *                                                                        użytkownika i hasła.
 *                                                                    4 = Kontynuacja logowania,
 *                                                                        przesłonięcie profilu
 *                                                                        użytkownika, hasła i
 *                                                                        biblioteki
 *                                                                    5 = Akceptacja logowania ze
 *                                                                        zwróceniem profilu użytk.
 *                                                                    6 = Akceptacja logowania ze
 *                                                                        zwróceniem profilu użytk.
 *                                                                        zastąpienie bieżącej
 *                                                                        biblioteki
C                   PARM                    USRPRFOUT       10             Profil użytkownika (Wyjście)
C                   PARM                    PASSWDOUT       10             Hasło (Wyjście)
C                   PARM                    CURLIBOUT       10             Biblioteka bieżąca (Wyjście)
C/EJECT
 *****************************************************************
 * PROGRAM GŁÓWNY                                                *
 *****************************************************************
 *
 * Sprawdzanie, czy użytkownik to ANONYMOUS
 *     1
C     USRLENIN      SUBST(P)  USRIN:1       User            10
C     User          IFEQ      Anonym
C                   MOVEL     Anonym        USRPRFOUT
 *
```

```
 * Sprawdzanie, czy użytkownik wprowadził coś jako adres e-mail
 *
C     AUTLENIN      IFGT      *ZERO                                Wprowadzony adres e-mail
 *
 * Sprawdzanie, czy adres e-mail jest poprawny
 *
C                   Z-ADD     0             i                 3 0
C     '@'           SCAN      AUTIN:1       i                    Poprawny adres e-mail
 *                                                                    zawiera znak @
 *
C     i             IFGT      0                                  Znaleziono @
C     AUTLENIN      SUBST(P)  AUTIN:1       Email            30
C                   Z-ADD     5             RETCDOUT             Akceptacja logowania
 *
 * Zaprotokołowanie anonimowego logowania przez FTP do kolejki komunikatów QSYSOPR
 * (Protokołowanie powinno być wykonywane w chronionym zbiorze fizycznym!!!!!!!)
 *
C     Text1         CAT(p)    Email:0       Message          43
C     Message       CAT(p)    Text2:0       Message
C     Message       DSPLY     'QSYSOPR'
 *
C                   ELSE                                         Niepoprawny adres e-mail
C                   Z-ADD     0             RETCDOUT             Odrzucenie próby logowania
C                   ENDIF
 *
C                   ELSE                                         Brak adresu e-mail
C                   Z-ADD     0             RETCDOUT             Odrzucenie próby logowania
C                   ENDIF
 *
C                   ELSE
 *
 * Inni użytkownicy: wykonanie normalnego przetwarzania logowania, ale adres klienta nie może
 *                    należeć do sieci 10.xxx.xxx.xxx
 *
C     3             SUBST     IPADDRIN:1    TheNet            3
C     TheNet        IFEQ      InvalidNet                         Błędna sieć
C                   Z-ADD     0             RETCDOUT             Odrzucenie próby logowania
C                   ELSE                                         Poprawna sieć
C                   Z-ADD     1             RETCDOUT             Kontynuacja logowania
C                   ENDIF
 *
C                   ENDIF
 *
C                   EVAL      *INLR = *ON
C                   RETURN
```

Format TCPL0100 punktu wyjścia:

Punktem wyjścia logowania do serwera FTP jest QIBM_QTMF_SVR_LOGON. Punktem wyjścia logowania do serwera REXEC jest QIBM_QTMX_SVR_LOGON. Jednym z interfejsów sterujących formatem parametrów dla tych punktów wyjścia jest TCPL0100. W tym temacie opisano parametry formatu punktu wyjścia TCPL0100.

To jest grupa wymaganych parametrów dla formatu punktu wyjścia TCPL0100.

Parametr	Opis	Wejściowy lub wyjściowy	Typ i długość
1	Identyfikator aplikacji	Wejściowy	Binary(4)
2	Identyfikator użytkownika	Wejściowy	Char(*)
3	Długość identyfikatora użytkownika	Wejściowy	Binary(4)
4	Łańcuch uwierzytelniający	Wejściowy	Char(*)
5	Długość łańcucha uwierzytelniającego	Wejściowy	Binary(4)

Parametr	Opis	Wejściowy lub wyjściowy	Typ i długość
6	Adres IP klienta	Wejściowy	Char(*)
7	Długość adresu IP klienta	Wejściowy	Binary(4)
8	Kod powrotu	Wyjściowy	Binary(4)
9	Profil użytkownika	Wyjściowy	Char(10)
10	Hasło	Wyjściowy	Char(10)
11	Początkowa biblioteka bieżąca	Wyjściowy	Char(10)

Opisy parametrów

Identyfikator aplikacji
INPUT; BINARY(4) Identyfikuje odpowiedni serwer aplikacji. Poprawnymi wartościami są:

1 program serwera FTP

2 program serwera REXEC

Identyfikator użytkownika
Wejściowy; Char(*) Identyfikator użytkownika podawany przez program klienta. Dla serwera FTP parametr ten zawiera pole danych komendy USER.

Długość identyfikatora użytkownika
Wejściowy; Binary(4) Długość (w bajtach) łańcucha identyfikatora użytkownika.

Łańcuch uwierzytelniający
Wejściowy; Char(*) Łańcuch (podobnie jak hasło) podawany przez program klienta.

Dla serwera FTP parametr ten zawiera pole danych komendy PASS (hasło). Podczas rozpoczynania pracy z systemem V5R1, jeśli uwierzytelnianie użytkownika zostało wykonane przez certyfikat klienta, parametr nie zawiera żadnych danych.

Długość łańcucha uwierzytelniającego
Wejściowy; Binary(4) Długość (w bajtach) łańcucha uwierzytelniającego.

Uwaga: Dla serwera FTP: jeśli uwierzytelnianie użytkownika zostało wykonane przez certyfikat klienta, parametr przyjmuje wartość 0.

Adres IP klienta
Wejściowy; Char(*) Adres IP inicjowanej sesji. Łańcuch jest w formacie dziesiętnym, wyrównany w lewo.

Długość adresu IP klienta
Wejściowy; Binary(4) Długość (w bajtach) adresu IP klienta.

Kod powrotu
OUTPUT; BINARY(4) Określa, czy operacja logowania się ma być zaakceptowana, czy odrzucona oraz czy hasło ma być autoryzowane, a początkowa biblioteka bieżąca ma być zastąpiona inną. Poprawnymi wartościami są:

0 Odrzucenie operacji logowania. Parametry wyjściowe profilu użytkownika, hasła i początkowej biblioteki bieżącej są ignorowane.

1 Kontynuacja operacji logowania z podanym identyfikatorem użytkownika, łańcuchem uwierzytelniającym i początkową biblioteką bieżącą określoną przez profil użytkownika. Identyfikator użytkownika staje się profilem użytkownika, a łańcuch uwierzytelniający staje się hasłem. Program ignoruje parametry wyjściowe profilu użytkownika, hasła i początkowej biblioteki bieżącej.

Uwaga: Aby logowanie zakończyło się pomyślnie, łańcuch uwierzytelniający musi zgadzać się z hasłem określonym w profilu użytkownika.

2 Kontynuacja operacji logowania z podanym identyfikatorem użytkownika, łańcuchem uwierzytelniającym i początkową biblioteką bieżącą określoną przez parametr początkowy biblioteki bieżącej. Identyfikator użytkownika jest jego profilem. Hasłem jest łańcuch uwierzytelniający. Należy podać parametr wyjściowy początkowej biblioteki bieżącej. Program ignoruje parametry wyjściowe profilu użytkownika i hasła.

Uwaga: Aby logowanie zakończyło się pomyślnie, łańcuch uwierzytelniający musi zgadzać się z hasłem określonym w profilu użytkownika.

3 Kontynuacja operacji logowania. Profil użytkownika i hasło są przesłaniane przez odpowiednie parametry wyjściowe zwrócone przez program obsługi wyjścia. Należy użyć początkowej biblioteki bieżącej podanej dla profilu użytkownika przez program obsługi wyjścia. Program ten pomija parametr wyjściowy początkowej biblioteki bieżącej.

Uwaga: Aby logowanie zakończyło się pomyślnie, hasło musi zgadzać się z hasłem określonym w profilu użytkownika.

Uwaga! Firma IBM zdecydowanie zaleca, aby hasło nie było **nigdy** kodowane bezpośrednio w programie obsługi wyjścia. Szyfrowanie, na przykład, umożliwia algorytmiczne rozpoznawanie hasła.

4 Kontynuacja operacji logowania; profil użytkownika, hasło oraz początkowa biblioteka bieżąca są przesłaniane przez odpowiednie parametry wyjściowe zwrócone przez program obsługi wyjścia.

Uwaga: Aby logowanie zakończyło się pomyślnie, hasło musi zgadzać się z hasłem określonym w profilu użytkownika.

Uwaga! Firma IBM zdecydowanie zaleca, aby hasło nie było **nigdy** kodowane bezpośrednio w programie obsługi wyjścia. Szyfrowanie, na przykład, umożliwia algorytmiczne rozpoznawanie hasła.

5 Akceptacja operacji logowania. Profil użytkownika jest przesłaniany przez parametr wyjściowy profilu użytkownika zwrócony przez program obsługi wyjścia. Należy użyć początkowej biblioteki bieżącej podanej w profilu użytkownika zwróconym przez program obsługi wyjścia. Program ignoruje parametry wyjściowe początkowej biblioteki bieżącej i hasła.

Uwaga: Określenie tej wartości przesłoni normalne przetwarzanie hasła w systemie i5/OS. Jest to jedyne uwierzytelnianie hasła.

6 Akceptacja operacji logowania. Profil użytkownika oraz początkowa biblioteka bieżąca są przesłaniane przez odpowiednie parametry wyjściowe zwrócone przez program obsługi wyjścia. Parametr wyjściowy hasła jest ignorowany.

Uwaga: Określenie tej wartości przesłoni normalne przetwarzanie hasła w systemie i5/OS. Jest to jedyne uwierzytelnianie hasła.

Profil użytkownika
Wyjściowy; Char(10) Profil użytkownika, który ma zostać użyty w tej sesji. Parametr ten musi być wyrównany w lewo i dopełniony znakami pustymi.

Hasło Wyjściowy; Char(10) Hasło, które ma zostać użyte w tej sesji. Parametr ten musi być wyrównany w lewo i dopełniony znakami pustymi.

Początkowa biblioteka bieżąca
Wyjściowy; Char(10) Początkowa biblioteka bieżąca ustalana dla tej sesji. Parametr ten musi być wyrównany w lewo i dopełniony znakami pustymi.

Odsyłacze pokrewne

"Format TCPL0200 punktu wyjścia" na stronie 125
Punktem wyjścia logowania do serwera FTP jest QIBM_QTMF_SVR_LOGON. Jednym z interfejsów sterujących formatem parametrów dla tych punktów wyjścia jest TCPL0200. W tym temacie opisano parametry formatu punktu wyjścia TCPL0200.

"Format TCPL0300 punktu wyjścia" na stronie 129
Punktem wyjścia logowania do serwera FTP jest QIBM_QTMF_SVR_LOGON. Punktem wyjścia logowania do serwera REXEC jest QIBM_QTMX_SVR_LOGON. Jednym z interfejsów sterujących formatem parametrów dla tych punktów wyjścia jest TCPL0300. W tym temacie opisano parametry formatu punktu wyjścia TCPL0300.

Uwagi dotyczące używania formatu TCPL0100:

TCPL0100 jest jednym z formatów punktu wyjścia używanych zarówno przez punkt wyjścia logowania do serwera FTP, jak i przez punkt wyjścia sprawdzania logowania do serwera REXEC.

W ramach protokołu FTP, jeśli którykolwiek ze zwróconych parametrów wyjściowych jest niepoprawny, serwer FTP nie pozwoli na kontynuowanie operacji. W tym wypadku serwer FTP wysyła do protokołu zdania komunikat Data from exit program for exit point &1 is missing or not valid (Dane z programu obsługi wyjścia 1 nie zostały przesłane do punktu wyjścia lub są niepoprawne).

W ramach protokołu FTP, jeśli wystąpi jakikolwiek wyjątek podczas wywoływania programu obsługi wyjścia, serwer FTP wyśle następujący komunikat: Exception encountered for FTP exit program &1 in library &2 for exit point &3 (Wystąpił wyjątek dla serwera FTP w programie obsługi wyjścia 1, w bibliotece 2 dla punktu wyjścia 3)

Poniższa tabela opisuje pokrótce, jakie czynności wykona serwer FTP w zależności od wartości kodu powrotu (parametr 8) zwracanego do serwera FTP przez program obsługi wyjścia.

Uwaga: Wartość w polu ″Kod powrotu″ oznacza, że program obsługi wyjścia musi określić odpowiednią dla tego parametru wyjściowego wartość. Ta wartość zostanie następnie użyta przez serwer FTP w celu przetworzenia żądania logowania się.

Kod powrotu	Profil użytkownika (9)	Hasło (10)	Biblioteka początkowa (11)
0	Ignorowany	Ignorowany	Ignorowany
1	(Identyfikator użytkownika, parametr 2)	(Hasło, parametr 4)	(Z profilu użytkownika)
2	(Identyfikator użytkownika, parametr 2)	(Hasło, parametr 4)	Wartość zwracana
3	Wartość zwracana	Wartość zwracana	(Z profilu użytkownika)
4	Wartość zwracana	Wartość zwracana	Wartość zwracana
5	Wartość zwracana	Ignorowany	(Z profilu użytkownika)
6	Wartość zwracana	Ignorowany	Wartość zwracana

W powyższej tabeli wartości ujęte w nawiasy wskazują, jakie informacje wykorzystuje aplikacja TCP/IP, gdy wartość wyjściowa została zignorowana. Zapis Ignorowany oznacza, że aplikacja ta nie użyła żadnych danych, dlatego dla tej wartości kodu powrotu nie zwróci ona żadnych danych.

W przypadku serwera FTP (punkt wyjścia QIBM_QTMF_SVR_LOGON, identyfikator aplikacji 1): jeśli identyfikatorem użytkownika jest ANONYMOUS i punkt wyjścia dodaje program obsługi wyjścia, serwer FTP wysyła specjalną odpowiedź podczas żądania hasła: 331 Guest logon in process, send complete e-mail address as password (331 Logowanie gościa w toku, prześlij jako hasło pełny adres poczty elektronicznej). Aplikacja wysyła ten program przed wywołaniem programu obsługi wyjścia.

Gdy aplikacja zaakceptuje logowanie na serwerze FTP, serwer FTP wysyła następujący komunikat: 230 Guest logon accepted, access restrictions apply (230 Logowanie gościa zaakceptowane, nadane ograniczenia dostępu).

Serwer REXEC (identyfikator aplikacji 2):

1. Jeśli parametr wyjściowy zezwolenia na operację nie jest poprawny, to serwer REXEC nie zezwoli na operację. Serwer REXEX wyśle do protokołu zadania komunikat ″Data from exit program for exit point &1 is missing or not valid″ (″Dane z programu obsługi wyjścia dla punktu wyjścia 1 nie zostały podane lub są niepoprawne″).
2. Jeśli podczas wywołania programu obsługi wyjścia wystąpi jakikolwiek wyjątek, to serwer REXEC nie zezwoli na operację. Wyśle on do protokołu zdania komunikat ″Exception encountered for REXEC exit program &1 in library &2 for exit point &3.″ (″Wystąpił wyjątek dla serwera REXEC w programie obsługi wyjścia 1, w bibliotece 2 dla punktu wyjścia 3.).

Format TCPL0200 punktu wyjścia:

Punktem wyjścia logowania do serwera FTP jest QIBM_QTMF_SVR_LOGON. Jednym z interfejsów sterujących formatem parametrów dla tych punktów wyjścia jest TCPL0200. W tym temacie opisano parametry formatu punktu wyjścia TCPL0200.

Grupa wymaganych parametrów.

Parametr	Opis	Wejściowy lub wyjściowy	Typ i długość
1	Identyfikator aplikacji	Wejściowy	Binary(4)
2	Identyfikator użytkownika	Wejściowy	Char(*)
3	Długość identyfikatora użytkownika	Wejściowy	Binary(4)
4	Łańcuch uwierzytelniający	Wejściowy	Char(*)
5	Długość łańcucha uwierzytelniającego	Wejściowy	Binary(4)
6	Adres IP klienta	Wejściowy	Char(*)
7	Długość adresu IP klienta	Wejściowy	Binary(4)
8	Pozwolenie na logowanie	Wyjściowy	Binary(4)
9	Profil użytkownika	Wyjściowy	Char(10)
10	Hasło	Wyjściowy	Char(10)
11	Początkowa biblioteka bieżąca	Wejściowy/wyjściowy	Char(10)
12	Początkowy katalog osobisty	Wyjściowy	Char(*)
13	Długość początkowego katalogu osobistego	Wejściowy/wyjściowy	Binary(4)
14	Informacje właściwe dla aplikacji	Wejściowy/wyjściowy	Char(*)
15	Długość informacji właściwych dla aplikacji	Wejściowy	Binary(4)

Opisy parametrów

Identyfikator aplikacji

Wejściowy; Binary(4) Identyfikuje serwer aplikacji, z którego zostało wysłane żądanie. Poprawnymi wartościami są:

1 program serwera FTP

Identyfikator użytkownika

Wejściowy; Char(*) Identyfikator użytkownika podawany przez program klienta. Dla serwera FTP parametr ten zawiera pole danych komendy USER.

Długość identyfikatora użytkownika
Wejściowy; Binary(4) Długość (w bajtach) łańcucha identyfikatora użytkownika.

Łańcuch uwierzytelniający
Wejściowy; Char(*) Łańcuch (podobnie jak hasło) podawany przez program klienta.

Dla serwera FTP parametr ten zawiera pole danych komendy PASS (hasło). Podczas rozpoczynania pracy z systemem V5R1, jeśli uwierzytelnianie użytkownika zostało wykonane przez certyfikat klienta, parametr nie zawiera żadnych danych.

Długość łańcucha uwierzytelniającego
Wejściowy; Binary(4) Długość (w bajtach) łańcucha uwierzytelniającego.

Uwaga: Dla serwera FTP: jeśli uwierzytelnianie użytkownika zostało wykonane przez certyfikat klienta, parametr przyjmuje wartość 0.

Adres IP klienta
Wejściowy; Char(*) Adres IP inicjowanej sesji. Ten łańcuch ma postać dziesiętną z kropkami i jest wyrównany do lewej strony.

Długość adresu IP klienta
Wejściowy; Binary(4) Długość (w bajtach) adresu IP klienta.

Pozwolenie na logowanie
Wejściowy; Binary(4) Wskazuje, czy operacja logowania powinna zostać zaakceptowana, czy odrzucona oraz jak powinna zostać przeprowadzona operacja uwierzytelnienia hasła. Poprawnymi wartościami są:

0 Odrzucenie operacji logowania. Wszystkie pozostałe parametry wyjściowe zostaną zignorowane.

1 Kontynuacja operacji logowania z podanym identyfikatorem użytkownika i łańcuchem uwierzytelniającym. Identyfikator użytkownika jest profilem użytkownika, a łańcuch uwierzytelniający jest hasłem. Bieżąca biblioteka i katalog roboczy zależą od ustawień odpowiednich parametrów wyjściowych. Aplikacja ignoruje parametry wyjściowe profilu użytkownika i hasła.

Uwaga: Aby logowanie zakończyło się pomyślnie, łańcuch uwierzytelniający musi zgadzać się z hasłem określonym w profilu użytkownika.

2 Kontynuacja operacji logowania. Profil użytkownika i hasło są przesłaniane przez odpowiednie parametry wyjściowe zwrócone przez program obsługi wyjścia. Aplikacja inicjuje bieżącą bibliotekę i katalog roboczy.

Uwaga: Aby logowanie zakończyło się pomyślnie, hasło musi zgadzać się z hasłem określonym w profilu użytkownika.

Uwaga! Firma IBM zdecydowanie zaleca, aby hasło nie było **nigdy** kodowane bezpośrednio w programie obsługi wyjścia. Szyfrowanie, na przykład, umożliwia algorytmiczne rozpoznawanie hasła.

3 Akceptacja operacji logowania. Profil użytkownika jest przesłaniany przez parametr wyjściowy profilu użytkownika zwrócony przez program obsługi wyjścia. Program inicjuje bieżącą bibliotekę i katalog roboczy na podstawie ustawień odpowiednich parametrów wyjściowych. Parametry wyjściowe hasła są ignorowane.

Uwaga: Jeśli system działa na poziomie ochrony 20 lub wyższym, podanie tej wartości spowoduje zastąpienie normalnego przetwarzania haseł w systemie i5/OS. Jest to jedyne uwierzytelnianie hasła.

Profil użytkownika
Wyjściowy; Char(10) Profil użytkownika, który ma zostać użyty w tej sesji. Jeśli parametr ten jest wymagany, to musi on być wyrównany w lewo i dopełniony znakami pustymi.

Hasło Wyjściowy; Char(10) Hasło, które ma zostać użyte w tej sesji. Jeśli parametr ten jest wymagany, to musi on być wyrównany w lewo i dopełniony znakami pustymi.

Początkowa biblioteka bieżąca
Wyjściowy; Char(10) Biblioteka bieżąca ustalana dla tej sesji. Jeśli parametr ten jest wymagany, to musi on być wyrównany w lewo i dopełniony znakami pustymi. Parametr ten jest ustawiany podczas wywołania programu obsługi wyjścia na poniższą wartość specjalną.

***CURLIB**
Należy użyć biblioteki bieżącej, określonej przez profil użytkownika.

Początkowy katalog osobisty
Wyjściowy; Char(*) Katalog osobisty, który ma zostać użyty w tej sesji. Jeśli parametr ten został podany, musi on zawierać bezwzględną nazwę ścieżki, a długość parametru początkowego katalogu osobistego musi być ustawiona tak, aby miała prawidłową wartość.

Długość początkowego katalogu osobistego
Wejściowy/Wyjściowy; Binary(4) Długość parametru początkowego katalogu osobistego zwracana przez program obsługi wyjścia. Parametr ten jest inicjowany dla wartości zerowej, gdy aplikacja wywoła program obsługi wyjścia. Jeśli program obsługi wyjścia nie zmienia wartości parametru, to katalog osobisty jest inicjowany wartością katalogu osobistego z profilu użytkownika.

Informacje właściwe dla aplikacji
Wejściowy/Wyjściowy; Char(*) Informacja wykorzystywana do przesyłania ustawień logowania właściwych dla aplikacji. Więcej informacji na temat poprawnego formatu zawiera sekcja Format parametru informacji właściwej dla aplikacji.

Długość informacji właściwych dla aplikacji
Wejściowy; Binary(4) Długość (w bajtach) informacji właściwej dla aplikacji.

Zadania pokrewne

“Konfigurowanie serwerów FTP w celu współpracy z klientami FTP z interfejsem graficznym oraz narzędziami WWW” na stronie 8
Serwery FTP w systemie operacyjnym i5/OS obsługują klienty FTP z interfejsem graficznym, przeglądarki WWW oraz narzędzia WWW. Ponieważ większość klientów FTP z interfejsem graficznym używa formatu listingu przypominającego system UNIX oraz pliku ścieżek jako formatu nazw plików, serwer FTP musi być tak skonfigurowany, aby obsługiwał te formaty.

Odsyłacze pokrewne

“Format TCPL0100 punktu wyjścia” na stronie 121
Punktem wyjścia logowania do serwera FTP jest QIBM_QTMF_SVR_LOGON. Punktem wyjścia logowania do serwera REXEC jest QIBM_QTMX_SVR_LOGON. Jednym z interfejsów sterujących formatem parametrów dla tych punktów wyjścia jest TCPL0100. W tym temacie opisano parametry formatu punktu wyjścia TCPL0100.

Format parametru informacji właściwej dla aplikacji:

Jeśli identyfikator aplikacji wskazuje na program serwera FTP, to parametr informacji właściwej dla aplikacji ma następujące pola.

Przesunięcie dziesiętnie	Przesunięcie szesnastkowo	Typ	Pole
0	0	BINARY(4)	Początkowy format nazwy
4	4	BINARY(4)	Początkowy bieżący katalog roboczy
8	8	BINARY(4)	Początkowy format listy plików
12	C	BINARY(4)	Mechanizm ochrony sterowania połączeniem
16	10	BINARY(4)	Opcja szyfrowania połączenia danych

Przesunięcie dziesiętnie	Przesunięcie szesnastkowo	Typ	Pole
20	14	BINARY(2)	Zestaw algorytmów szyfrowania połączenia kontrolnego
22	16	BINARY(2)	Zestaw algorytmów szyfrowania połączenia danych

Opisy pół

Początkowy format nazwy

Identyfikuje początkowe ustawienie formatu nazw plików dla danej sesji. Podczas wywołania programu obsługi wyjścia wartość tego pola jest ustawiana zgodnie z wartością znajdującą się w pliku konfiguracyjnym serwera FTP. Jest ona określona przez parametr NAMEFMT. Poprawnymi wartościami są:

0 Użyj formatu nazwy LIBRARY/FILE.MEMBER. Ustawienie to odpowiada opcji NAMEFMT(*LIB) komendy CHGFTPA i jest równoważne wykonaniu komendy SITE NAMEFMT 0 na serwerze FTP.

1 Użyj formatu nazewnictwa ścieżek. Ustawienie to odpowiada opcji NAMEFMT(*PATH) komendy CHGFTPA i jest równoważne z wykonaniem komendy SITE NAMEFMT na serwerze FTP.

Początkowy bieżący katalog roboczy

Określa początkowe ustawienia bieżącego katalogu roboczego na serwerze FTP, który jest domyślnym katalogiem wykorzystywanym przez działania na plikach i listach. Podczas wywołania programu obsługi wyjścia wartość tego pola jest ustawiana zgodnie z wartościami konfiguracyjnymi serwera FTP określanymi przez parametry CURDIR. Poprawnymi wartościami są:

0 Jako bieżący katalog roboczy serwera FTP używana jest biblioteka bieżąca. To ustawienie odpowiada opcji CURDIR(*CURLIB) komendy CHGFTPA.

1 Jako początkowy bieżący katalog roboczy serwera FTP używany jest katalog osobisty. To ustawienie odpowiada opcji CURDIR(*HOMEDIR) komendy CHGFTPA.

Uwaga: Jeśli w pole to zostanie wpisana wartość 1, to należy także ustawić pole formatu nazwy na 1.

Początkowy format listy plików

Identyfikuje początkowe ustawienie formatu listy plików dla danej sesji. Podczas wywołania programu obsługi wyjścia wartość tego pola jest ustawiana zgodnie z wartością znajdującą się w konfiguracji serwera FTP. Jest ona określona przez parametr LISTFMT. Poprawnymi wartościami są:

0 Użyj formatu listy plików systemu i5/OS. Ustawienie to odpowiada opcji LISTFMT(*DFT) komendy CHGFTPA i jest równoważne wykonaniu komendy SITE LISTFMT 0 na serwerze FTP.

1 Użyj formatu listy plików UNIX. Ustawienie to odpowiada opcji LISTFMT(*UNIX) komendy CHGFTPA i jest równoważne wykonaniu komendy SITE LISTFMT 1 na serwerze FTP.

Mechanizm ochrony sterowania połączeniem

Określa mechanizm ochrony używany do sterowania połączeniem dla danej sesji FTP. Poprawnymi wartościami są:

0 Sterowanie połączeniem nie jest chronione.

1 Sterowanie połączeniem jest chronione przez warstwę SSL; mechanizm określony przez klienta FTP w podkomendzie AUTH to TLS-C lub TLS.

2 Sterowanie połączeniem jest chronione przez warstwę SSL; mechanizm określony przez klienta FTP w komendzie AUTH to TLS-C lub TLS.

Uwagi:

- Jest to tylko pole wejściowe dla programu obsługi wyjścia. Zmiany wprowadzone przez program obsługi wyjścia są ignorowane.

- Wartość ustawiana jest na 1 dla sesji podłączonych do chronionego portu FTP. Połączenia do chronionego portu FTP zachowują się tak, jakby do serwera FTP została wysłana niejawna komenda SSL.

Opcja szyfrowania połączenia danych

Określa, czy połączenie FTP danych dla sesji FTP ma być szyfrowane. Poprawnymi wartościami są:

-1 Nie jest dozwolone szyfrowanie połączeń FTP danych dla tej sesji FTP.

0 Dozwolone (ale nie wymagane) jest szyfrowanie połączeń FTP danych dla tej sesji FTP.

1 Wymagane jest szyfrowanie połączeń FTP danych dla tej sesji FTP.

Uwagi:

- Jeśli wartość dla mechanizmu ochrony sterowania połączeniem jest równa 1, ustawienie opcji szyfrowania połączenia danych na -1 będzie wymagało dodatkowych komend FTP od klienta FTP, aby pomyślnie przesłać dane. (Mechanizm ochrony TLS-P lub SSL domyślnie szyfruje połączenia danych.)
- Jeśli wartość dla mechanizmu ochrony sterowania połączeniem jest równa 2, ustawienie opcji szyfrowania połączenia danych na 1 będzie wymagało dodatkowych komend FTP od klienta FTP, aby pomyślnie przesłać dane. (Mechanizm ochrony TLS-C lub TLS nie szyfruje domyślnie połączeń danych.)

Zestaw algorytmów szyfrowania połączenia kontrolnego

Określa zestaw algorytmów szyfrowania SSL używanych do szyfrowania sterowania połączeniem dla sesji FTP. Wartości zestawu algorytmów szyfrowania są definiowane w funkcjach API protokołu SSL (Secure Sockets Layer).

Uwagi:

- Jest to tylko pole wejściowe dla programu obsługi wyjścia. Zmiany wprowadzone przez program obsługi wyjścia są ignorowane.
- Wartość jest poprawna tylko wtedy, gdy wartość mechanizmu sterowania połączeniem jest równa 1 lub 2.

Zestaw algorytmów szyfrowania połączenia danych

Określa zestaw algorytmów szyfrowania SSL używanych do szyfrowania danych w połączeniu danych dla sesji FTP. Gdy wywoływany jest program obsługi wyjścia, wartość ta ustawiana jest na 0, co umożliwia obsłudze warstwy SSL negocjowanie, jaki zestaw algorytmów szyfrowania będzie używany. Jeśli program obsługi wyjścia zmieni to pole, musi zostać podana poprawna wartość zestawu algorytmów szyfrowania. Wartości zestawu algorytmów szyfrowania są definiowane w funkcjach API protokołu SSL (Secure Sockets Layer).

Uwagi:

- Pole to jest ignorowane, jeśli mechanizm ochrony sterowania połączeniem ma wartość 0 lub opcja szyfrowania połączenia ma wartość -1.
- Określenie dla tego pola wartości innej niż 0 lub wartości określonej w polu zestawu algorytmów szyfrowania sterowania połączeniem może być przyczyną błędów podczas próby nawiązania połączenia SSL pomiędzy serwerem FTP a klientem FTP, ponieważ podany zestaw algorytmów szyfrowania może nie być obsługiwany przez klienta FTP.

Odsyłacze pokrewne

Funkcje API warstwy SSL (Secure Sockets Layer)

Format TCPL0300 punktu wyjścia:

Punktem wyjścia logowania do serwera FTP jest QIBM_QTMF_SVR_LOGON. Punktem wyjścia logowania do serwera REXEC jest QIBM_QTMX_SVR_LOGON. Jednym z interfejsów sterujących formatem parametrów dla tych punktów wyjścia jest TCPL0300. W tym temacie opisano parametry formatu punktu wyjścia TCPL0300.

Grupa wymaganych parametrów.

Parametr	Opis	Wejściowy lub wyjściowy	Typ i długość
1	Identyfikator aplikacji	Wejściowy	Binary(4)
2	Identyfikator użytkownika	Wejściowy	Char(*)
3	Długość identyfikatora użytkownika	Wejściowy	Binary(4)
4	Łańcuch uwierzytelniający	Wejściowy	Char(*)
5	Długość łańcucha uwierzytelniającego	Wejściowy	Binary(4)
6	Identyfikator CCSID łańcucha uwierzytelniającego	Wejściowy	Binary(4)
7	Adres IP klienta	Wejściowy	Char(*)
8	Długość adresu IP klienta	Wejściowy	Binary(4)
9	Pozwolenie na logowanie	Wyjściowy	Binary(4)
10	Profil użytkownika	Wyjściowy	Char(10)
11	Hasło	Wyjściowy	Char(*)
12	Długość hasła	Wyjściowy	Binary(4)
13	Identyfikator CCSID hasła	Wyjściowy	Binary(4)
14	Początkowa biblioteka bieżąca	Wejściowy/wyjściowy	Char(10)
15	Początkowy katalog osobisty	Wyjściowy	Char(*)
16	Długość początkowego katalogu osobistego	Wejściowy/wyjściowy	Binary(4)
17	Identyfikator CCSID początkowego katalogu osobistego	Wejściowy/wyjściowy	Binary(4)
18	Informacje właściwe dla aplikacji	Wejściowy/wyjściowy	Char(*)
19	Długość informacji właściwych dla aplikacji	Wejściowy	Binary(4)

Opisy parametrów

Identyfikator aplikacji

Wejściowy; Binary(4) Identyfikuje serwer aplikacji, z którego zostało wysłane żądanie. Poprawnymi wartościami są:

1 program serwera FTP

2 program serwera REXEC

Identyfikator użytkownika

Wejściowy; Char(*) Identyfikator użytkownika podawany przez program klienta.

Dla serwera FTP parametr ten zawiera pole danych komendy USER.

Długość identyfikatora użytkownika

Wejściowy; Binary(4) Długość (w bajtach) łańcucha identyfikatora użytkownika.

Łańcuch uwierzytelniający

Wejściowy; Char(*) Łańcuch (podobnie jak hasło) podawany przez program klienta.

Dla serwera FTP parametr ten zawiera pole danych podkomendy PASS (hasło), chyba że uwierzytelnianie użytkownika zostało wykonane za pomocą certyfikatu klienta. W takim wypadku dla tego parametru dostarczany jest certyfikat klienta.

Długość łańcucha uwierzytelniającego
Wejściowy; Binary(4) Długość (w bajtach) łańcucha uwierzytelniającego.

Identyfikator CCSID łańcucha uwierzytelniającego
Wejściowy; Binary(4) Identyfikator CCSID parametru łańcucha uwierzytelniającego. Dla serwera FTP: jeśli uwierzytelnianie użytkownika zostało wykonane przez certyfikat klienta, parametr przyjmuje wartość -2.

Adres IP klienta
Wejściowy; Char(*) Adres IP inicjowanej sesji. Ten łańcuch ma postać dziesiętną z kropkami i jest wyrównany do lewej strony.

Długość adresu IP klienta
Wejściowy; Binary(4) Długość (w bajtach) adresu IP klienta.

Pozwolenie na logowanie
Wejściowy; Binary(4) Wskazuje, czy operacja logowania powinna zostać zaakceptowana, czy odrzucona oraz jak powinna zostać przeprowadzona operacja uwierzytelnienia hasła. Poprawnymi wartościami są:

0 Odrzucenie operacji logowania. Wszystkie pozostałe parametry wyjściowe zostaną zignorowane.

1 Kontynuacja operacji logowania z podanym identyfikatorem użytkownika i łańcuchem uwierzytelniającym. Identyfikator użytkownika jest profilem użytkownika, a łańcuch uwierzytelniający jest hasłem. Bieżąca biblioteka i katalog roboczy zależą od ustawień odpowiednich parametrów wyjściowych. Aplikacja ignoruje parametry wyjściowe profilu użytkownika i hasła.

Uwaga: Aby logowanie zakończyło się pomyślnie, łańcuch uwierzytelniający musi zgadzać się z hasłem określonym w profilu użytkownika.

2 Kontynuacja operacji logowania. Profil użytkownika i hasło są przesłaniane przez odpowiednie parametry wyjściowe zwrócone przez program obsługi wyjścia. Aplikacja inicjuje bieżącą bibliotekę i katalog roboczy.

Uwaga: Aby logowanie zakończyło się pomyślnie, hasło musi zgadzać się z hasłem określonym w profilu użytkownika.

Uwaga! Firma IBM zdecydowanie zaleca, aby hasło nie było **nigdy** kodowane bezpośrednio w programie obsługi wyjścia. Szyfrowanie, na przykład, umożliwia algorytmiczne rozpoznawanie hasła.

3 Akceptacja operacji logowania. Profil użytkownika jest przesłaniany przez parametr wyjściowy profilu użytkownika zwrócony przez program obsługi wyjścia. Program inicjuje bieżącą bibliotekę i katalog roboczy na podstawie ustawień odpowiednich parametrów wyjściowych. Parametry wyjściowe hasła są ignorowane.

Uwaga: Jeśli system działa na poziomie ochrony 20 lub wyższym, podanie tej wartości spowoduje zastąpienie normalnego przetwarzania haseł w systemie i5/OS. Jest to jedyne uwierzytelnianie hasła.

Profil użytkownika
Wyjściowy; Char(10) Profil użytkownika, który ma zostać użyty w tej sesji. Jeśli parametr ten jest wymagany, to musi on być wyrównany w lewo i dopełniony znakami pustymi.

Hasło Wyjściowy; Char(*) Hasło, które ma zostać użyte w tej sesji. Jeśli jest to konieczne, muszą zostać podane parametry: Długość hasła i Identyfikator CCSID hasła; parametry te muszą być wyrównane do lewej strony. Jeśli dla wartości systemowej QPWDLVL określono wartość 0 lub 1, można podać do 10 znaków; jeśli dla wartości systemowej QPWDLVL określono wartość 2 lub 3, można podać do 128 znaków.

Długość hasła
Wyjściowy; Binary(4) Długość hasła (w bajtach). Poprawny zakres to od 1 do 512 bajtów.

Identyfikator CCSID hasła
Wyjściowy; Binary(4) CCSID hasła. Parametr ten musi zostać ustawiony przez program obsługi wyjścia podczas określania parametru. Poprawnymi wartościami są:

0 CCSID zadania jest używany do określenia CCSID przekształcanych danych. Jeśli identyfikatorem CCSID zadania jest 65535, to używany jest identyfikator CCSID z domyślnego identyfikatora CCSID (DFTCCSID) dla atrybutu zadania.

1-65533
Jest to zakres, w którym identyfikator CCSID jest poprawny.

Początkowa biblioteka bieżąca
Wyjściowy; Char(10) Biblioteka bieżąca ustalana dla tej sesji. Jeśli parametr ten jest wymagany, to musi on być wyrównany w lewo i dopełniony znakami pustymi. Parametr ten podczas wywołania programu obsługi wyjścia ma ustawianą następującą wartość specjalną : *CURLIB- Korzystanie z bieżącej biblioteki określanej przez profil użytkownika.

Początkowy katalog osobisty
Wyjściowy; Char(*) Katalog osobisty, który ma zostać użyty w tej sesji. Jeśli parametr ten został podany, musi zawierać bezwzględną nazwę ścieżki, a parametr długość początkowego katalogu osobistego i parametr identyfikatora CCSID początkowego katalogu osobistego muszą być ustawione na prawidłową wartość.

Długość początkowego katalogu osobistego
Wejściowy/Wyjściowy; Binary(4) Długość parametru początkowego katalogu osobistego zwracana przez program obsługi wyjścia. Parametr ten jest inicjowany dla wartości zerowej, gdy aplikacja wywoła program obsługi wyjścia. Jeśli program obsługi wyjścia nie zmienia wartości parametru, to katalog osobisty jest inicjowany wartością katalogu osobistego z profilu użytkownika.

Identyfikator CCSID początkowego katalogu osobistego
OUTPUT; BINARY(4) Identyfikator CCSID początkowego katalogu osobistego. Parametr ten musi zostać ustawiony przez program obsługi wyjścia podczas określania początkowego katalogu osobistego. Poprawnymi wartościami są:

0 CCSID zadania jest używany do określenia CCSID przekształcanych danych. Jeśli identyfikatorem CCSID zadania jest 65535, to używany jest identyfikator CCSID z domyślnego identyfikatora CCSID (DFTCCSID) dla atrybutu zadania.

1-65533
Jest to zakres, w którym identyfikator CCSID jest poprawny.

Informacje właściwe dla aplikacji
Wejściowy/Wyjściowy; Char(*) Informacja wykorzystywana do przesyłania ustawień logowania właściwych dla aplikacji. Więcej informacji na temat poprawnego formatu zamieszczono w sekcji “Format parametru informacji właściwej dla aplikacji” na stronie 127.

Długość informacji właściwych dla aplikacji
Wejściowy; Binary(4) Długość (w bajtach) informacji właściwej dla aplikacji.

Zadania pokrewne

“Konfigurowanie serwerów FTP w celu współpracy z klientami FTP z interfejsem graficznym oraz narzędziami WWW” na stronie 8
Serwery FTP w systemie operacyjnym i5/OS obsługują klienty FTP z interfejsem graficznym, przeglądarki WWW oraz narzędzia WWW. Ponieważ większość klientów FTP z interfejsem graficznym używa formatu listingu przypominającego system UNIX oraz pliku ścieżek jako formatu nazw plików, serwer FTP musi być tak skonfigurowany, aby obsługiwał te formaty.

Odsyłacze pokrewne

“Format TCPL0100 punktu wyjścia” na stronie 121
Punktem wyjścia logowania do serwera FTP jest QIBM_QTMF_SVR_LOGON. Punktem wyjścia logowania do

serwera REXEC jest QIBM_QTMX_SVR_LOGON. Jednym z interfejsów sterujących formatem parametrów dla tych punktów wyjścia jest TCPL0100. W tym temacie opisano parametry formatu punktu wyjścia TCPL0100.

Usuwanie programu obsługi wyjścia

Kiedy program obsługi wyjścia nie jest już dłużej potrzebny, można go usunąć za pomocą ekranu Praca z programem obsługi wyjścia (Work with Exit Program).

Aby usunąć zainstalowany program obsługi wyjścia, wykonaj następujące czynności:

1. W wierszu komend wpisz komendę WRKREGINF.
2. Przejdź na następną stronę do punktu wyjścia logowania do serwera FTP:

```
QIBM_QTMF_SERVER_REQ  VLRQ0100
QIBM_QTMF_SVR_LOGON   TCPL0100
QIBM_QTMF_SVR_LOGON   TCPL0200
QIBM_QTMF_SVR_LOGON   TCPL0300
```

3. Wprowadź 8 w polu opcji (Opt) z lewej strony wpisu punktu wyjścia i naciśnij klawisz Enter.
4. Na ekranie Praca z programem obsługi wyjścia (Work with Exit Program) wpisz wartość 4 (Usuń) (Remove).
5. Wpisz nazwę programu obsługi wyjścia w polu **Program obsługi wyjścia**.
6. W polu Biblioteka wpisz nazwę biblioteki zawierającej program obsługi wyjścia.
7. Naciśnij klawisz Enter.
8. Po zakończeniu usuwania punktów wyjścia zatrzymaj i zrestartuj serwer FTP.

Pojęcia pokrewne

"Zarządzanie dostępem za pomocą programów obsługi wyjścia FTP" na stronie 23
Dodatkowe bezpieczeństwo można zapewnić, dodając programy obsługi wyjścia FTP do punktów wyjścia serwera i klienta FTP, które oferują więcej możliwości ograniczenia dostępu do systemu.

Zadania pokrewne

"Instalowanie i rejestrowanie programów obsługi wyjścia" na stronie 15
Istnieje możliwość utworzenia bibliotek zawierających programy obsługi wyjścia i ich protokoły, a następnie skompilowania i zarejestrowania tych programów jako programów używanych przez serwer FTP.

"Uruchamianie i zatrzymywanie serwera FTP" na stronie 26
Serwer FTP można uruchamiać i zatrzymywać za pomocą programu System i Navigator.

Metody przesyłania danych

Przed rozpoczęciem przesyłania plików należy wybrać właściwy format ich przesyłania. Można użyć domyślnego formatu ASCII lub podać inny format, na przykład EBDCIC lub BINARY.

ASCII jest standardem kodowania znaków w sieci Internet. Format EBCDIC jest standardowym formatem systemu operacyjnego i5/OS. Należy wybrać odpowiedni typ zgodnie z następującymi wskazówkami:

- Format ASCII służy do przesyłania plików, które zawierają tylko tekst (pliki tekstowe).
- Format EBCDIC służy do przesyłania danych EBCDIC pomiędzy systemami obsługującymi kod EBCDIC. Używanie tego formatu pozwoli uniknąć, w obu systemach, wykonywania konwersji danych pomiędzy formatem EBCDIC a ASCII.
- Format BINARY służy do przesyłania plików niebędących plikami tekstowymi, takich jak binarne pliki danych numerycznych, pliki graficzne i zbiory składowania systemu i5/OS.

Po wybraniu formatu przesyłania plików można rozpocząć przesyłanie plików za pomocą protokołu FTP.

Zadania pokrewne

"Przesyłanie plików za pomocą protokołu FTP" na stronie 31
Protokół FTP umożliwia wysyłanie i odbieranie plików.

Odsyłacze pokrewne

"ASCII (Zmiana typu pliku na ASCII - Change File Type to ASCII)" na stronie 63
Podkomenda ASCII klienta FTP i5/OS służy doustawiania typu przesyłania plików na format ASCII.

"EBCDIC (Zmiana typu pliku na EBCDIC - Change File Type to EBCDIC)" na stronie 69
Podkomenda EBCDIC klienta FTP i5/OS służy do ustawiania typu przesyłania plików na format EBCDIC. Typ przesyłania EBCDIC jest przydatny podczas przesyłania plików do lub z innego systemu EBCDIC, ponieważ pozwala uniknąć konwersji między formatami ASCII i EBCDIC w obu systemach.

"BINARY (Ustawienie typu przesyłania dla obrazu - Set Transfer Type to Image)" na stronie 64
Podkomenda BINARY klienta FTP i5/OS służy do ustawiania typu przesyłania plików na format BINARY.

Przesyłanie plików zawierających upakowane dane dziesiętne między platformami System i

Przesyłanie upakowanych lub nieupakowanych danych dziesiętnych jest obsługiwane między platformami System i. Wykonanie takiego przesyłania wymaga użycia typu przesyłania TYPE I (BINARY) lub TYPE E (EBCDIC) w trybie transmisji BLOCK.

W typie przesyłania BINARY lub EDCDIC dane są przesyłane bez jakiejkolwiek konwersji. Wyniki innych rodzajów przesyłania są nieprzewidywalne.

Podczas przesyłania upakowanych lub nieupakowanych danych w zewnętrznie opisanym pliku systemu plików QSYS.LIB plik docelowy powinien zostać utworzony wcześniej w taki sam sposób, jak plik źródłowy. To ograniczenie stosowane jest do danych zawierających specjalny format liczbowy lub gdy wymagany jest dostęp za pomocą klucza.

Podczas przesyłania danych, w trybie przesyłania binarnego, długość rekordu w pliku docelowym musi być taka sama, jak długość rekordu w pliku źródłowym.

Przed przesłaniem upakowanych lub nieupakowanych danych dziesiętnych do lub z systemów o innej architekturze (takich jak S/390 lub UNIX), należy wykonać konwersję danych do postaci nadającej się do wydruku.

Przesyłanie zbiorów *SAVF

Zbiory *SAVF muszą być wysyłane jako obrazy, dlatego przed przesłaniem tego rodzaju zbiorów należy uruchomić podkomendę FTP BINARY.

Jeśli zbiór *SAVF jest przesyłany z użyciem formatu nazwy 0, w systemie odbierającym należy wcześniej utworzyć zbiór składowania. Aby zwiększyć wydajność i zachować integralność, zalecane jest również wcześniejsze utworzenie zbiorów w innych sytuacjach.

Przesyłanie zbioru składowania jest użyteczne tylko wtedy, gdy zarówno serwer nadający, jak i odbierający znajduje się na platformie System i, ponieważ jest to format zbioru właściwy dla systemu operacyjnego i5/OS. Zbiór składowania można jednak wysłać do systemu innego niż platforma System i i składować go tam w postaci kopii zapasowej. Taki zbiór składowania można przesłać później do platformy System i za pomocą protokołu FTP.

Przykład: przesyłanie zbioru *SAVF z maszyny wirtualnej do platformy System i

Poniższy przykład przedstawia sposób przesyłania zbioru *SAVF z maszyny wirtualnej do platformy System i przy użyciu formatów NAMEFMT 0 i NAMEFMT 1.

Sesja FTP została już zainicjowana, podkomenda BINARY została wydana, a format NAMEFMT 0 został określony.

W pierwszej kolejności należy przesłać zbiór P162484 SAVF310L z dysku A maszyny wirtualnej do platformy System i. Usługa FTP maszyny wirtualnej wymaga wstawienia kropki pomiędzy nazwę zbioru a typ zbioru. Jako nazwę zbioru należy podać P162484 w bibliotece P162484 platformy System i i określić parametr REPLACE, tak jakby zbiór został wcześniej utworzony, nawet jeśli nie był przedtem używany. Należy pamiętać, że wcześniejsze utworzenie jest obowiązkowe w przypadku formatu NAMEFMT 0.

Format NAMEFMT zostanie zmieniony na 1 i całe przesyłanie zbioru jest powtarzane z nowym formatem nazwy. Po raz kolejny określ parametr REPLACE, ponieważ zbiór istnieje po wykonaniu poprzedniej czynności.

Uwagi:

- Jeśli przed przeprowadzeniem operacji przesyłania za pomocą formatu NAMEFMT 0 nie utworzono wcześniej zbioru na platformie System i, operacja przesyłania wyglądałaby na zakończoną pomyślnie. Jednak po sprawdzeniu zbioru na platformie System i okazałoby się, że utworzony został zbiór fizyczny (*PF), a nie zbiór składowania (*SAVF).
- W zależności od tego, w jaki sposób zbiór *SAVF został wcześniej wysłany do maszyny wirtualnej, konieczne może być wykonanie niektórych czynności z zakresu przetwarzania wstępnego w maszynie wirtualnej.
  - Jeśli zbiór *SAVF został wysłany do maszyny wirtualnej za pomocą protokołu FTP, można wydać podkomendę GET, aby przesłać go z powrotem do platformy System i.
  - Jeśli w celu wysłania zbioru *SAVF do maszyny wirtualnej użyto komendy Wysłanie zbioru sieciowego (Send Network File - SNDNETF), przed przesłaniem zbioru ponownie do platformy System i za pomocą protokołu FTP należy dokonać konwersji zbioru w maszynie wirtualnej z formatu rekordów o zmiennej długości (RECFM) na format RECFM o stałej długości. W tym celu należy w maszynie wirtualnej użyć komendy COPYFILE. Na przykład:

    ```
    COPYFILE P162484 SAVF310L A = = = (RECFM F REPLACE
    ```

```
 |
 > GET P162484.SAVF310L P162484/P162484 (REPLACE
  200 Żądanie portu poprawne.
  150 Wysyłanie pliku 'P162484.SAVF310L'
  250 Transfer zakończony pomyślnie.
  Przesłano 384912 bajtów w ciągu 3,625 sek. Szybkość przesyłania 106,183 kB/sek.   |

> namefmt 1
  202 Komenda SITE nie jest wymagana; można kontynuować
  Format zbiorów w stacji typu Klient - NAMEFMT 1.
> GET P162484.SAVF310L/QSYS.LIB/P162484.LIB/P162484.savf(REPLACE
  200 Żądanie portu poprawne.
  150 Wysyłanie pliku 'P162484.SAVF310L'
  250 Transfer zakończony pomyślnie.
  Przesłano 384912 bajtów w ciągu 3,569 sek. Szybkość przesyłania 107.839 kB/sek.   |
Wpisz podkomendę FTP.
===>
```

*Rysunek 9. Przesyłanie zbioru *SAVF z maszyny wirtualnej do platformy System i przy użyciu formatów NAMEFMT 0 i NAMEFMT 1*

Przesyłanie dokumentów QDLS

Podczas przesyłania dokumentu QDLS atrybut pozycji katalogu QDLS wskazujący domyślny typ dokumentu jest ustawiony na typ dokumentu PCFILE w systemie odbierającym dla wszystkich typów dokumentów z wyjątkiem dokumentów w formacie odwracalnym (RFT).

Dla dokumentów typu RFT wartością domyślną jest RFTDCA. Dokumenty typu RFTDCA można przeglądać i edytować za pomocą komendy CL WRKDOC. Dokumentów typu PCFILE nie można przeglądać ani edytować za pomocą komendy CL WRKDOC.

Przesyłanie plików w systemach plików root, QOpenSys, QLANSrv, QDLS i QOPT

Podczas przesyłania plików w systemach plików root, QOpenSys, QDLS i QOPT konieczne jest użycie trybu strumieniowego (MODE S) oraz struktury pliku (STRUCT F).

Systemy plików root, QOpenSys, QDLS i QOPT mogą istnieć w każdej poprawnej stronie kodowej.

Konwersja danych oraz przypisania identyfikatora CCSID zmieniają się w zależności od wybranego trybu (TYPE). Więcej informacji zawiera sekcja Znaczniki strony kodowej CCSID dla plików systemu i5/OS.

Podczas dopisywania danych do istniejącego pliku, znacznik identyfikatora CCSID tego pliku nie jest zmieniany. Podczas dopisywania danych do istniejącego pliku za pomocą trybu TYPE A, dane są przekształcane do strony kodowej tego pliku.

Odsyłacze pokrewne

“Znaczniki strony kodowej CCSID dla plików systemu i5/OS” na stronie 141
Nowe pliki tworzone przez protokół FTP w systemie operacyjnym i5/OS są znakowane identyfikatorem kodowanego zestawu znaków (CCSID) lub stroną kodową tego identyfikatora. Znakowanie stroną kodową CCSID identyfikuje dane znakowe w plikach.

Przesyłanie plików za pomocą systemu plików QfileSvr.400

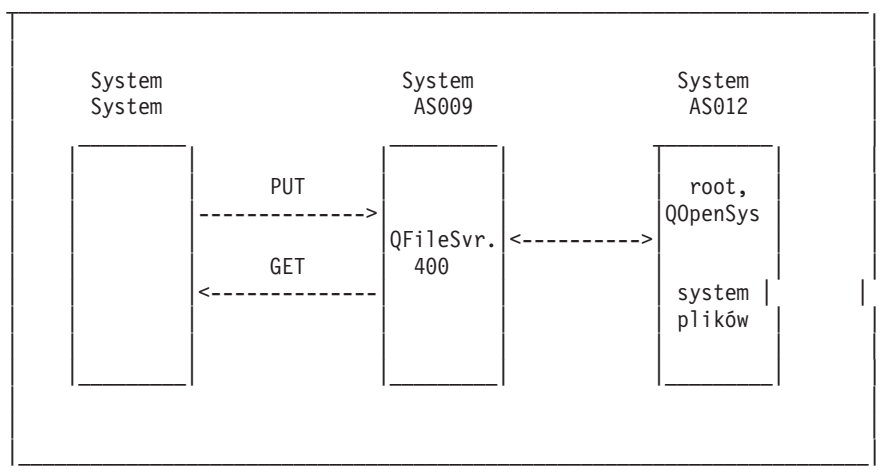
System plików QFileSvr.400 umożliwia dostęp do innych systemów plików w systemie zdalnym.

Umożliwia przesyłanie plików w systemach plików root, QOpenSys, QDLS i QOPT. Nie umożliwia natomiast przesyłania plików w systemie QSYS.LIB.

W czasie przesyłania plików konieczne jest użycie trybu strumieniowego (MODE S) oraz struktury pliku (STRUCT F). Na przykład na rysunku Rys. 10 przedstawiono przesyłanie pliku FILE.ABC do i z dwóch różnych systemów plików systemu AS012 za pomocą systemu plików QFileSvr.400 systemu AS009.

Po połączeniu z serwerem AS009 przesyłanie pliku jest realizowane za pomocą podkomend klienta FTP przedstawionych na rysunku Rys. 11 na stronie 137.

Uwaga: W systemach AS009 i AS012 identyfikator użytkownika oraz hasło muszą być takie same.



Rysunek 10. Przykład systemu plików QFileSvr.400

```
NAMEFMT  1
LCD  /CLIENTDIR1
CD  /QFileSvr.400/AS012/FLSDIR
PUT  FILE.ABC
GET  FILE.ABC  /CLIENTDIR2/FILE.ABC
CD  /QFileSvr.400/AS012/QOpenSys/FLSDIR
PUT  FILE.ABC
GET  FILE.ABC  /CLIENTDIR2/FILE.ABC (REPLACE
SYSCMD  RMVLNK  '/CLIENTDIR2/FILE.ABC'
DELETE  /QFileSvr.400/AS012/FLSDIR/FILE.ABC
DELETE  /QFileSvr.400/AS012/QOpenSys/FLSDIR/FILE.ABC
QUIT
```

Rysunek 11. Podkomendy do przesyłania plików za pomocą systemu plików QFileSvr.400

Przesyłanie zbiorów QSYS.LIB

W tym temacie omówiono operacje protokołu FTP w trybie przesyłania strumieniowego i w trybie przesyłania obrazów przeznaczone dla systemu plików QSYS.LIB.

Tabele Tabela 3 na stronie 138 i Tabela 4 na stronie 139 zawierają podsumowanie operacji FTP w trybie przesyłania strumieniowego i w trybie przesyłania obrazów dla systemu plików QSYS.LIB. Podczas korzystania z tych tabel należy uwzględnić następujące aspekty:

Zgodność długości rekordu i wielkości pliku

Podczas przesyłania danych do zbioru, który istnieje, wielkość rekordu i wielkość otrzymywanego zbioru muszą być zgodne z odpowiadającymi im wielkościami wysyłanego zbioru, w przeciwnym razie wystąpi błąd przesyłania. Zarówno wielkość rekordu jak i wielkość zbioru otrzymywanego musi być większa lub równa wielkości rekordu i wielkości zbioru źródłowego. Aby określić, czy wielkość istniejącego zbioru jest zgodna, należy sprawdzić liczbę rekordów, liczbę dozwolonych rozszerzeń oraz maksymalną dozwoloną wielkość rekordu. Informacje te można wyświetlić, wprowadzając komendę Wyświetlenie opisu zbioru (Display File Description - DSPFD).

Automatyczne tworzenie zbioru w systemie operacyjnym i5/OS

Jeśli zbiór fizyczny nie istnieje, system utworzy go automatycznie po otrzymaniu zbioru. Zaleca się jednak, aby wcześniej utworzyć zbiór w systemie.

Typ danych

Podczas przesyłania danych za pomocą TYPE I, dane te nie są przekształcane. Jeśli zbiór nie istnieje, to podczas tworzenia jest oznaczany numerem CCSID 65535.

Uwaga: Zaleca się, aby przed przesyłaniem zbiorów z wieloma podzbiorami, utworzyć zbiór za pomocą komend MGET i MPUT. Jeśli zbiór nie został wcześniej utworzony, usługa FTP utworzy taki zbiór, ustalając maksymalną długość rekordu równą najdłuższemu rekordowi pierwszego przetwarzanego podzbioru. Jeśli długość rekordu pozostałych podzbiorów jest dłuższa, pojawi się błąd przycięcia danych podczas przesyłania tych podzbiorów. Wcześniejsze utworzenie zbioru, z wielkością rekordu przystosowaną do wszystkich podzbiorów, zapobiegnie wystąpieniu takiego błędu.

Tabela 3. Tryb przesyłania strumieniowego dla systemu plików QSYS.LIB

Biblioteka istnieje	**Zbiór istnieje**	**Podzbiór istnieje**	**Wybrano zastąpienie**	**Długość rekordu jest zgodna**	**Wielkość zbioru jest zgodna**	**Rezultat**
Tak	Tak	Tak	Tak	Tak	Tak	Dane zapisane w podzbiorze.
Tak	Tak	Tak	Nie			Przesyłanie zostaje odrzucone i wysyłany jest komunikat.
Tak	Tak	Nie		Nie	Tak	Przesyłanie zbioru zostaje zakończone, rekordy zostają przycięte i wysyłany jest komunikat.
Tak	Tak	Nie	Tak	Nie	Tak	Przesyłanie zbioru zostaje zakończone, rekordy zostają przycięte i wysyłany jest komunikat.
Tak	Tak	Nie		Tak	Tak	Tworzony jest podzbiór, do którego zapisywane są dane.
Tak	Tak	Nie	Nie		Nie	Przesyłanie zostaje odrzucone i wysyłany jest komunikat.
Tak	Nie					Tworzony jest zbiór z długością rekordu równą maksymalnej długości rekordu przysłanego zbioru. Tworzony jest podzbiór, do którego zapisywane są dane.

Tabela 3. Tryb przesyłania strumieniowego dla systemu plików QSYS.LIB (kontynuacja)

Biblioteka istnieje	Zbiór istnieje	Podzbiór istnieje	Wybrano zastąpienie	Długość rekordu jest zgodna	Wielkość zbioru jest zgodna	Rezultat
Nie						Przesyłanie zostaje odrzucone i wysyłany jest komunikat. Należy użyć komendy Tworzenie biblioteki (Create Library - CRTLIB) w celu utworzenia biblioteki w systemie zdalnym.

Tabela 4. Tryb przesyłania obrazów dla systemu plików QSYS.LIB

Biblioteka istnieje	Zbiór istnieje	Podzbiór istnieje	Wybrano zastąpienie	Rezultat
Tak	Tak	Tak	Tak	Dane zapisane w podzbiorze.
Tak	Tak	Tak	Nie	Przesyłanie zostaje odrzucone i wysyłany jest komunikat.
Tak	Tak	Nie		Tworzony podzbiór i dane
Tak	Nie			
Nie				

Odsyłacze pokrewne

"Uwagi dotyczące tworzenia zbiorów przed przesłaniem ich do systemu plików QSYS.LIB" na stronie 140
Przed przesłaniem jakichkolwiek zbiorów do systemu plików QSYS.LUB zalecane jest ich utworzenie. Dzięki temu dane będą przesłane niezawodnie i efektywnie z zachowaniem optymalnej wydajności i integralności.

Odbieranie plików tekstowych w systemie plików QSYS.LIB:

System plików QSYS.LIB obsługuje wewnętrznie strukturę rekordu. W związku z tym protokół FTP i5/OS dokonuje konwersji plików odbieranych na platformie System i na strukturę rekordu, a plików wysyłanych z platformy System i na strukturę pliku protokołu FTP.

Pliki tekstowe odebrane na platformie System i za pomocą protokołu FTP są konwertowane na strukturę rekordu w następujący sposób:

- Kiedy serwer FTP odbiera plik, który już istnieje w systemie, jest stosowana długość rekordu istniejącego pliku.
- Kiedy serwer FTP tworzy nowy plik w systemie, jako długość pliku jest stosowana długość najdłuższego wiersza lub rekordu pliku (wykluczając końcowe odstępy).

Pliki tekstowe wysyłane z platformy System i za pomocą protokołu FTP są konwertowane na strukturę pliku przez usunięcie końcowych odstępów z każdego wiersza lub rekordu i wysłanie obciętego rekordu.

Uwagi dotyczące tworzenia zbiorów przed przesłaniem ich do systemu plików QSYS.LIB

Przed przesłaniem jakichkolwiek zbiorów do systemu plików QSYS.LUB zalecane jest ich utworzenie. Dzięki temu dane będą przesłane niezawodnie i efektywnie z zachowaniem optymalnej wydajności i integralności.

Należy się upewnić, że dla całego zbioru przydzielono wystarczającą ilość rekordów. W systemie i5/OS należy w tym celu użyć parametru SIZE komendy Tworzenie zbioru fizycznego (Create Physical File - CRTPF).

Należy się upewnić, że parametr RCDLEN komendy Tworzenie zbioru fizycznego (Create Physical File - CRTPF) ma wartość odpowiednią na ulokowanie maksymalnej, oczekiwanej długości rekordu.

Uwaga: Zbiory w systemie serwera FTP można tworzyć za pomocą podkomendy QUOTE. Natomiast zbiory w systemie klienta FTP można tworzyć za pomocą podkomendy SYSCMD.

Odsyłacze pokrewne

"Przesyłanie zbiorów QSYS.LIB" na stronie 137
W tym temacie omówiono operacje protokołu FTP w trybie przesyłania strumieniowego i w trybie przesyłania obrazów przeznaczone dla systemu plików QSYS.LIB.

Konwersje identyfikatora kodowanego zestawu znaków

W systemie operacyjnym i5/OS informacje o identyfikatorze kodowanego zestawu znaków (CCSID) służą do interpretowania danych wejściowych i wyświetlania danych wyjściowych w poprawnym formacie. Dane wejściowe mogą być w formacie ASCII lub EBCDIC.

Szczegółowe informacje dotyczące konwersji CCSID znajdują się w następujących tematach.

Określanie tabel odwzorowań:

Tabele odwzorowań ASCII dla klienta FTP określane są w komendzie FTP. Dla serwera FTP służy do tego komenda Zmiana atrybutów FTP (Change FTP Attributes - CHGFTPA).

Aby określić tabele odwzorowań klienta FTP:

1. Wpisz komendę FTP.
2. Naciśnij klawisz F4. Zostanie wyświetlony ekran **Uruchomienie przesyłania plików TCP/IP**.
3. Naciśnij klawisz F10. Wyświetlą się podpowiedzi dla wychodzących i przychodzących tabel ASCII/EBCDIC.

```
                     Uruchomienie przesyłania plików TCP/IP (FTP)
                   (Start TCP/IP File Transfer (FTP))

Wpisz opcje i naciśnij klawisz Enter.

System zdalny  . . . . . .



Adres internetowy . . . . . .
Identyfikator kodowanego zestawu znaków     *DFT          1-65533, *DFT

                           Parametry dodatkowe

Tabela danych wychodzących EBCDIC/ASCII  . .   *CCSID        Nazwa, *CCSID,*DFT
  Biblioteka  . . . . . .                         Nazwa, *LIBL,*CURLIB
Tabela danych przychodzących ASCII/EBCDIC  . .   *CCSID        Nazwa, *CCSID,*DFT
  Biblioteka  . . . . . .                         Nazwa, *LIBL,*CURLIB


                                                                        Koniec
 F3=Wyjście F4=Podpowiedź F5=Odśwież F12=Anuluj F13=Jak używać ekranu
 F24=Inne klawisze
```

*Rysunek 12. Określanie tabel odwzorowań ASCII za pomocą wartości *CCSID*

Należy podać wartość CCSID (i stąd tabele odwzorowań), która ma być używana przez klienta FTP. Jeśli wartość *DFT nie zostanie zmieniona, używana jest wartość CCSID 00819 (ISO 8859-1 8-bitowy kod ASCII). Można również określić określoną wartość CCSID dla transferów przychodzących i wychodzących. Zastosowanie identyfikatorów CCSID zostało omówione w sekcji Uwagi dotyczące protokołu FTP w zakresie obsługi języków narodowych.

Uwagi:

- Dla parametru CCSID komendy CHGFTPA wartości CCSID zestawu znaków dwubajtowych (DBCS) są niedopuszczalne. Wartości CCSID DBCS mogą być określone za pomocą podkomendy TYPE (Określenie typu przesyłania plików - Specify File Transfer Type).
- IBM dołącza obsługę odwzorowań do usługi FTP, aby zapewnić kompatybilność z wersjami wcześniejszymi niż V3R1. Użycie tabel odwzorowań dla przychodzących przesyłań plików TYPE A, wynika z utraty znakowania CCSID, kiedy tworzony jest plik docelowy. IBM zdecydowanie zaleca stosowanie obsługi CCSID dla normalnych operacji.

Odsyłacze pokrewne

“Uwagi dotyczące obsługi języków narodowych przez protokół FTP” na stronie 142
Ten rozdział przedstawia szereg aspektów, na które należy zwrócić uwagę przy stosowaniu protokołu FTP w środowisku z różnymi językami podstawowymi.

“TYPE (Określenie typu przesyłania plików - Specify File Transfer Type)” na stronie 92
Podkomenda TYPE klienta FTP i5/OS służy do określania typu przesyłania plików lub reprezentacji, w jakiej odbywa się przesyłanie.

Znaczniki strony kodowej CCSID dla plików systemu i5/OS:

Nowe pliki tworzone przez protokół FTP w systemie operacyjnym i5/OS są znakowane identyfikatorem kodowanego zestawu znaków (CCSID) lub stroną kodową tego identyfikatora. Znakowanie stroną kodową CCSID identyfikuje dane znakowe w plikach.

Podczas zastępowania lub dopisywania danych do istniejącego pliku, znacznik pliku nie jest zmieniany.

W poniższej tabeli przedstawiono, w jaki sposób protokół FTP przypisuje te wartości różnym systemom plików i różnym rodzajom przesyłania.

Tabela 5. Znaczniki strony kodowej CCSID dla plików systemu i5/OS

Pobieranie systemu plików	Rodzaj przesyłania Type A (ASCII)	Rodzaj przesyłania type C ('ccsid')	Rodzaj przesyłania type E (EBCDIC)	Rodzaj przesyłania Type I (Image/Binary)
QSYS.LIB	Identyfikator CCSID określony przez identyfikator CCSID równy EBCDIC dla nowej bazy danych zbiorów (CRTCCSID).	'ccsid' jeśli EBCDIC CCSID. Jeśli identyfikator ccsid jest typu ASCII, wtedy odpowiednio domyślnie EBCDIC CCSID.	65535	65535
″root″, QOpenSys, QDLS, QOPT	Domyślny identyfikator CCSID równy ASCII.	Wartość 'ccsid' określona w komendzie TYPE C numer_ccsid.	Identyfikator CCSID zadania jeśli nie jest to 65535. Jeśli identyfikator CCSID zadania to 65535, przypisywany jest domyślny CCSID zadania.	Domyślny identyfikator CCSID równy ASCII.
Uwaga: Domyślny identyfikator CCSID ASCII jest definiowany po uruchomieniu zadania FTP. Dla klienta jest to parametr CCSID komendy STRTCPFTP (i FTP). Dla serwera, parametr CCSID atrybutów konfiguracji FTP, które mogą być zmienione za pomocą komendy CHGFTPA. Przypisania pliku w systemie QFileSvr.400 zależą od systemu plików otrzymującego ten plik.				

Odsyłacze pokrewne

"Przesyłanie plików w systemach plików root, QOpenSys, QLANSrv, QDLS i QOPT" na stronie 135
Podczas przesyłania plików w systemach plików root, QOpenSys, QDLS i QOPT konieczne jest użycie trybu strumieniowego (MODE S) oraz struktury pliku (STRUCT F).

Uwagi dotyczące obsługi języków narodowych przez protokół FTP:

Ten rozdział przedstawia szereg aspektów, na które należy zwrócić uwagę przy stosowaniu protokołu FTP w środowisku z różnymi językami podstawowymi.

- Jeśli dane są przesyłane z użyciem trybu TYPE E (lub kodu EBCDIC), są one składowane w niezmienionej postaci, więc będą miały stronę kodową EBCDIC pliku, z którego pochodzą. Może to spowodować, że zapisany plik będzie zawierał znaczniki z nieodpowiednią wartością CCSID, jeśli język podstawowy dwóch systemów nie będzie taki sam.

  Na przykład, jeśli dane w stronie kodowej 237 wysyłane są przy użyciu TYPE E do systemu plików QSYS.LIB, w komputerze, gdzie taki zbiór nie istnieje, są składowane w niezmienionej postaci, w nowym zbiorze z identyfikatorem CCSID równym 65535. Jeśli zbiór odbierający już istnieje, dane zostaną zapisane w niezmienionej postaci i oznaczone wartością CCSID istniejącego zbioru, która nie może być wartością 237.

  Aby uniknąć nieprawidłowego przypisania CCSID, można skorzystać z komendy TYPE C CCSID (na przykład TYPE C 237) do określenia wartości CCSID przesyłanych danych. Kiedy podczas przesyłania wartość CCSID zostaje określona, a dane zostają zapisane do istniejącego zbioru, następuje przekształcenie danych do CCSID istniejącego zbioru. Jeśli zbiór docelowy nie istnieje, jest tworzony z podanym identyfikatorem CCSID.

  Jak podano we wcześniejszym przykładzie, jeśli zbiór docelowy nie istnieje, to w systemie otrzymującym dane tworzony jest zbiór z identyfikatorem CCSID 237. Natomiast jeśli zbiór docelowy istnieje, dane są przekształcane do identyfikatora CCSID tego zbioru.
- Podczas uruchamiania klienta FTP może pojawić się komunikat: Unable to convert data from CCSID &1 to CCSID &2 (Konwersja z indentyfikatora CCSID 1 na identyfikator CCSID 2 jest niemożliwa). Wyświetla się on w momencie, kiedy pomiędzy identyfikatorem CCSID EBCDIC określonym dla zadania, a identyfikatorem CCSID ASCII określonym dla danej sesji FTP nie jest możliwa konwersja znaków.

  Identyfikator CCSID ASCII można zmienić, podając wartość parametru identyfikatora CCSID komendy CL STRTCPFTP. Identyfikatorem CCSID 850, który zawiera kodowany zestaw znaków IBM Personal Computer Latin-1, jest identyfikator ASCII CCSID, dla którego dostępne są konwersje znaków dla wszystkich poprawnych wartości CCSID zadania.

- Podczas korzystania z FTP w trybie ASCII, pomiędzy dwoma systemami EBCDIC w systemie wysyłającym dane są one przekształcane ze strony kodowej EBCDIC na ASCII, a następnie z ASCII na EBCDIC w systemie otrzymującym dane. Zazwyczaj nie stanowi to problemu, ponieważ 7-bitowa strona kodowa ASCII używana przez oba systemy jest taka sama, chyba że znaki EBCDIC w systemie wysyłającym nie są zdefiniowane w stronie kodowej ASCII. Ponadto niektóre znaki strony kodowej ASCII pomiędzy dwoma różnymi stronami kodowymi EBCDIC mogą być odwzorowane inaczej. Może się tak zdarzyć, jeśli niektóre znaki ASCII są zmienne (znaki zajmujące różne szesnastkowe punkty kodowe w stronie kodowej EBCDIC). Znak zmienny może być odmiennie interpretowany przez system otrzymujący dane, jeśli strona kodowa EBCDIC jest inna niż strona określona dla systemu wysyłającego zbiór.

  Odsyłacze pokrewne

  “Określanie tabel odwzorowań” na stronie 140
  Tabele odwzorowań ASCII dla klienta FTP określane są w komendzie FTP. Dla serwera FTP służy do tego komenda Zmiana atrybutów FTP (Change FTP Attributes - CHGFTPA).

Systemy plików i konwencje nazewnictwa

Serwer FTP organizuje jednostki informacji systemu plików w struktury wielowarstwowe, podobne do drzewa.

W zależności od wersji systemu operacyjnego i5/OS można w nim używać z protokołem FTP różnych systemów plików. Systemy plików w systemie operacyjnym i5/OS mogą używać różnych terminów dla danych i ich struktur hierarchicznych.

Konwencje nazewnictwa

W każdym systemie plików i5/OS istnieje inny zestaw reguł dotyczących nazewnictwa plików. Format nazwy pliku musi odpowiadać konwencji nazewnictwa systemu plików, w którym plik ten się znajduje. Formaty i przykłady nazw plików dla systemów plików i5/OS, które są obsługiwane przez protokół FTP, opisano w kolekcji tematów Zintegrowany system plików. System udostępnia informacje dotyczące nazewnictwa plików w innych systemach operacyjnych po użyciu komendy QUOTE HELP.

Parametr NAMEFMT serwera FTP

Kiedy uruchamiana jest sesja serwera FTP, parametr NAMEFMT przyjmuje wartość 0. Wartość parametru NAMEFMT można zmienić za pomocą podkomendy SITE.

Serwer FTP automatycznie przełącza wartość domyślną parametru NAMEFMT z 0 na 1, kiedy pierwszy parametr pliku lub nazwy ścieżki otrzymany z podkomendą:

- zaczyna się znakiem ukośnika (/) lub tyldy (~)

lub

- jest pusty (z wyjątkiem komend LIST i NLST).

Późniejsze komendy serwera, zawierające parametr pliku lub nazwy ścieżki, nie wpłyną na wartość parametru NAMEFMT. Oprócz zmiany wartości parametru NAMEFMT, odpowiedź serwera FTP na podkomendę będzie zawierała instrukcję informującą o zmianie tej wartości.

Na przykład wartość parametru NAMEFMT serwera FTP zostanie zmieniona na ″1″, jeśli pierwszą podkomendą serwera zawierającą plik lub nazwę ścieżki będzie:

```
CWD  /DIR1/DIR2A
```

Odpowiedź serwera FTP będzie miała postać:

```
250-NAMEFMT ustawione na 1.
250 Bieżący katalog został zmieniony na /DIR1/DIR2A.
```

Uwaga: Umożliwia to typowej przeglądarce WWW, która wymaga określenia wartości ″1″ dla parametru NAMEFMT, współdziałanie z serwerami FTP i5/OS bez potrzeby uruchamiania podkomendy SITE NAMEFMT 1.

Pojęcia pokrewne

Zintegrowany system plików

Zbiory i systemy plików

Odsyłacze pokrewne

“NAMEFMT (Wybranie formatu nazw plików - Select File Naming Format)” na stronie 79
Podkomenda NAMEFMT klienta FTP i5/OS służy do wybierania formatu nazw plików, który będzie używany w systemie lokalnym i zdalnym.

“QUOTE (Wysłanie komendy do serwera FTP - Send a Subcommand to an FTP Server)” na stronie 83
Podkomenda QUOTE klienta FTP i5/OS służy do wysyłania podkomendy do serwera FTP.

Systemy plików i5/OS obsługiwane przez protokół FTP

Systemy plików, których można używać z protokołem FTP są zależne od poziomu wersji systemu operacyjnego.

System plików biblioteki QSYS.LIB - biblioteki, zbiory, podzbiory
FTP obsługuje przesyłanie zbiorów składowania i podzbiorów zbiorów fizycznych, logicznych, zbiorów DDM i źródłowych zbiorów fizycznych. Dla zbiorów fizycznych systemu plików QSYS.LIB przesyłane dane to podzbiory zbiorów znajdujących się w bibliotekach.

Usługi biblioteki dokumentów QDLS - foldery i dokumenty
Dla systemu plików usług biblioteki dokumentów (Document Library Services - QDLS) przesyłane dane zazwyczaj noszą nazwę dokumentów. Dokumenty QDLS znajdują się w katalogach nazywanych folderami.

″katalog główny″
System plików /. Ten system plików wykorzystuje w pełni możliwość obsługi plików strumieniowych i hierarchiczną strukturę katalogów zintegrowanego systemu plików. Ma charakterystykę systemów plików DOS i OS/2.

QOpenSys
System plików systemów otwartych. Ten system plików jest zgodny ze standardami systemów otwartych opartych na systemach UNIX(R), takich jak POSIX czy XPG. Tak jak bazowy system plików, wykorzystuje on zalety plików strumieniowych i obsługi katalogów zapewnianych przez zintegrowany system plików. Obsługuje on nazwy z rozróżnieniem wielkości liter.

QOPT System plików nośników optycznych QOPT. Zapewnia dostęp do strumienia danych, który jest przechowywany na nośniku optycznym.

System plików QFileSvr.400
System plików serwera plików i5/OS. Ten system plików umożliwia dostęp do innych systemów plików rezydujących w systemach zdalnych. Protokół FTP nie umożliwia dostępu do bibliotek QSY.LIB, QDLS ani QOPT, które używają systemu plików QFileSvr.400.

Pojęcia pokrewne

Zintegrowany system plików

Komunikaty o statusie z serwera FTP

Po wpisaniu podkomendy podczas trwania sesji klienta FTP komunikaty o statusie zwracane są przez serwer za pomocą 3-cyfrowego kodu: *xyz*. Do każdej cyfry przypisane są pewne wartości wskazujące różne statusy.

Pierwsza cyfra (x) oznacza, że odpowiedź jest dobra, zła lub niekompletna. Pierwsza cyfra może mieć pięć wartości:

- 1yz = Dobra. Żądane działanie jest inicjowane; spodziewana jest kolejna odpowiedź.
- 2yz = Dobra. Żądane działanie zostało wykonane pomyślnie; można wysłać nowe żądanie.
- 3yz = Niepełna. Podkomenda została zaakceptowana, ale żądane działanie oczekuje na dostarczenie dodatkowych informacji.

- 4yz = Niepełna. Serwer FTP nie przyjął podkomendy. Żądane działanie nie zostało wykonane. Jest to chwilowy błąd i można ponowić żądanie.
- 5yz = Zła. Komenda nie została zaakceptowana i żądanie nie zostało wykonane.

Druga cyfra (y) oznacza kategorię funkcjonalną odpowiedzi.

- x0z=Składnia. Oznacza błędy składni lub informuje, że użyte komendy są nieodpowiednie lub niepotrzebne.
- x1z=Informacja. Odnosi się do żądań podania informacji takich jak status lub pomoc.
- x2z=Połączenia. Odnosi się do połączeń kontrolnych lub połączeń danych.
- x3z=Uwierzytelnianie. Odnosi się do procesu logowania się.
- x5z=System plików. Odnosi się do statusu serwera FTP w stosunku do żądania przesyłania plików.

Trzecia cyfra (z) określa wyższy poziom szczegółów informacji o kategorii funkcjonalnej.

W poniższej tabeli przedstawiono najczęściej spotykane kody odpowiedzi i ich znaczenie. Tekst komunikatu może się różnić w zależności od systemu.

Kod	**Znaczenie**
110	Zrestartuj odpowiedź znacznika
120	Usługa będzie gotowa w przeciągu nnn minut
125	Połączenie danych jest już otwarte; rozpoczyna się przesyłanie
150	Uruchomienie pliku OK; nastąpi otworzenie łącza danych
200	Komenda OK
202	Komenda nie została zaimplementowana; nie jest używana w tym systemie
211	Status systemu lub odpowiedź pomocy systemu
212	Status katalogu
213	Status pliku
214	Komunikat pomocy
220	Usługa oczekuje na nowego użytkownika
226	Trwa zamykanie łącza danych; działanie na pliku zostało zakończone pomyślnie
230	Użytkownik zalogowany
250	Żądane działanie na pliku zostało zakończone pomyślne; działanie zakończone
257	Utworzono nazwę ścieżki
331	Wymagane hasło
332	Wymagane konto
425	Nie można otworzyć połączenia danych
426	Połączenie zamknięte; przesyłanie nie powiodło się
450	Żądane działanie na pliku nie zostało podjęte; plik jest zajęty
451	Żądane działanie zostało zakończone nieprawidłowo; lokalny błąd przetwarzania
452	Żądane działanie nie zostało podjęte; brak pamięci w systemie
500	Błąd składni; komenda nie została rozpoznana
501	Błąd składni parametrów lub argumentów
502	Komenda nie została zaimplementowana

Kod	Znaczenie
503	Nieprawidłowa sekwencja komend
504	Komenda nie została zaimplementowana dla tego parametru
530	Próba zalogowania się do systemu została odrzucona
532	Do przechowywania plików wymagane jest konto
550	Żądane działanie nie zostało podjęte; plik nie został znaleziony (lub brak dostępu)
551	Żądane działanie zostało zakończone nieprawidłowo; nieznany typ strony
552	Żądane działanie zostało zakończone nieprawidłowo; przekroczono przypisaną pojemność pamięci
553	Żądane działanie nie zostało podjęte; niedozwolona nazwa pliku

Odsyłacze pokrewne

“Podkomendy serwera FTP” na stronie 41
Poniższe podkomendy przedstawiają komunikację pomiędzy klientem FTP a serwerem FTP. W tym temacie opisano podkomendy odpowiadające komendom CL w systemie i5/OS, które są unikalne dla serwera FTP i5/OS.

“Podkomendy klienta FTP” na stronie 60
Za pomocą podkomend klienta FTP można nawiązywać połączenia ze zdalnymi serwerami FTP, przechodzić do bibliotek i katalogów oraz tworzyć, usuwać i przesyłać pliki.

Konwencje składni komend serwera FTP

Podczas stosowania podkomend serwera FTP należy przestrzegać następujących konwencji składni.

Wielkie litery
Należy wpisywać wielkie litery dokładnie tak, jak to podano w definicjach składni komend. Litery te można wisywać wielkimi bądź małymi literami.

Słowa pisane małymi literami lub terminy łączone
Słowa pisane małymi literami, terminy łączone myślnikiem lub podkreśleniem, jak na przykład plik_zdalny i informacje-konta, reprezentują zmienne, które należy zastąpić konkretnymi informacjami.

Nawiasy kwadratowe [ ]
Słowa, symbole lub frazy ujęte w nawiasy można traktować jako opcjonalne.

Nawias otwierający (i gwiazdka *
Nawias otwierający i gwiazdkę należy wpisywać dokładnie tak, jak to podano w definicjach składni.

Nawiasy klamrowe { }
Klamry obejmują grupę parametrów, wartości lub zmiennych, które można powtarzać.

Wielokropek ...
Wielokropek wskazuje, że w nawiasach można dodać dowolną liczbę powtórzeń poprzedniej zmiennej.

Kreska pionowa |
Kreska pionowa między parametrami lub wartościami wskazuje, że można podać pierwszą lub drugą wartość, lecz nie obie naraz. Pionowe kreski umieszczane są w nawiasach lub klamrach.

Konwencje składni komend klienta FTP

Podczas stosowania podkomend klienta FTP należy przestrzegać następujących konwencji składni.

Wielkie litery
Wielkie litery widoczne w definicjach składni komend klienta są minimalną liczbą liter, których wpisanie jest wymagane. Komendy klienta FTP można wpisywać wielkimi bądź małymi literami.

Słowa pisane małymi literami lub terminy łączone
Słowa pisane małymi literami lub terminy łączone myślnikiem, na przykład nazwa lub plik_zdalny reprezentują zmienne, które należy zastąpić konkretnymi informacjami.

Nawiasy kwadratowe[ ]
Słowa, symbole lub frazy ujęte w nawiasy można traktować jako opcjonalne.

Nawias otwierający (i gwiazdka *
Nawias otwierający i gwiazdkę należy wpisywać dokładnie tak, jak umieszczone są w definicjach składni.

Nawiasy klamrowe { }
Klamry obejmują grupę parametrów, wartości lub zmiennych, które można powtarzać.

Wielokropek ...
Wielokropek wskazuje, że w nawiasach można dodać dowolną liczbę powtórzeń poprzedniej zmiennej.

Kreska pionowa |
Kreska pionowa między parametrami lub wartościami wskazuje, że można podać pierwszą lub drugą wartość, lecz nie obie naraz. Pionowe kreski umieszczane są w zestawach kilku nawiasów lub klamr.

Ujmowanie parametrów podkomend w cudzysłowy lub apostrofy

Parametry podkomend można ująć w znaki apostrofu (') lub cudzysłowu (″).

Aby umieścić apostrof w parametrze ujętym w apostrofy, należy go wprowadzić jako dwa następujące po sobie apostrofy (''). Aby umieścić apostrof w parametrze ujętym w cudzysłowy (″), należy go wprowadzić jako apostrof.

Podobnie, jeśli cudzysłów (″) ma znajdować się w parametrze, należy wpisać go w jeden z następujących sposobów:

- znak cudzysłowu (″) w parametrze ujętym w apostrofy.
- dwa następujące po sobie znaki cudzysłowu (″″) w parametrze ujętym w cudzysłowy.

Apostrofu lub cudzysłowu można używać w jeden z następujących sposobów:

1. Jeśli apostrofy lub cudzysłowy w parametrze są takie same jak ogranicznik początkowy i końcowy, należy powtórzyć ten znak wewnątrz parametru. Na przykład:

```
'ABCD''12345'
   oznacza   ABCD'12345
"ABCD""12345"
   oznacza  ABCD"12345
```

2. Jeśli początkowy i końcowy znak są inne niż znak wewnątrz parametru, nie należy powtarzać znaku. Na przykład:

```
"ABCD'12345"
   oznacza   ABCD'12345
'ABCD"12345'
   oznacza  ABCD"12345
```

3. Jeśli wewnątrz parametru znajdują się zarówno apostrofy, jak i znaki cudzysłowu, jako ogranicznik należy wybrać jeden z tych symboli. Na przykład:

```
"ABC'12""345"  lub  'ABC'12"345'
   oznacza   ABC'12"345
```

Odsyłacze pokrewne

"GET (Kopiowanie pliku z systemu zdalnego do lokalnego - Copy a File from a Remote System to the Local System)" na stronie 69
Podkomenda GET klienta FTP i5/OS służy do kopiowania pliku z systemu zdalnego do systemu lokalnego.

"PUT (Kopiowanie podzbioru zbioru z systemu lokalnego do pliku w systemie zdalnym - Copy a File Member from the Local System to a File on a Remote System)" na stronie 81
Podkomenda PUT klienta FTP i5/OS służy do kopiowania lokalnego podzbioru zbioru do systemu zdalnego.

"Nazwy plików dla podkomend klienta służących do przesyłania danych" na stronie 148
W przypadku niektórych podkomend można używać domyślnych nazw plików źródłowych i docelowych; należy jednak określić nazwę pliku dla pozostałych podkomend.

“Nazwy plików do przesyłania” na stronie 150
Podkomendy klienta FTP używane do przesyłania danych mogą zawierać parametr **plik_lokalny**, **plik_zdalny** lub oba te parametry. Można ich użyć do nazwania danych, które mają być przesłane.

Nazwy plików dla podkomend klienta służących do przesyłania danych

W przypadku niektórych podkomend można używać domyślnych nazw plików źródłowych i docelowych; należy jednak określić nazwę pliku dla pozostałych podkomend.

Jeśli nazwa pliku docelowego dla komend PUT, APPEND i GET nie zostanie podana, klient FTP używa domyślnych nazw plików. Ponieważ w podkomendach MPUT i MGET można podać nazwy plików źródłowych, serwer FTP tworzy także nazwy plików docelowych dla podkomend MPUT i MGET. Informacje na temat składni tych podkomend zamieszczone zostały w tabeli Komendy służące do przesyłania danych. Kolumna tabeli z nagłówkiem *Docelowy* jest parametrem, dla którego nadawana jest domyślna nazwa.

Podkomenda	Plik źródłowy	Plik docelowy	Inne informacje
APPEND	nazwa pliku lokalnego	[nazwa pliku na serwerze]	
PUT	nazwa pliku lokalnego	[nazwa pliku na serwerze]	
GET	nazwa pliku na serwerze	[nazwa pliku lokalnego]	[(Replace]
MPUT	nazwa pliku lokalnego		
MGET	nazwa pliku na serwerze		[(Replace]

Podkomendy PUT i APPEND

Zasady tworzenia nazw domyślnych dla podkomend PUT i APPEND dzielą się na dwie kategorie:

- W przypadku korzystania z platformy System i należy uwzględnić następujące reguły:
  - Jeśli docelowy system plików jest systemem plików zawierającym biblioteki lub biblioteki dokumentów, domyślna nazwa jest zgodna z regułami nazewnictwa obowiązującymi w systemach tego rodzaju, w tym z formatem nazw.
  - Jeśli docelowy system plików nie jest systemem plików zawierającym biblioteki lub dokumenty, nazwa domyślna jest jedną z następujących nazw:
    - Nazwa domyślna jest nazwą znajdującą się po ostatnim ukośniku w nazwie pliku źródłowego.
    - Nazwa domyślna jest taka sama jak nazwa pliku źródłowego, jeśli nie zawiera żadnego ukośnika.
- W przypadku korzystania z serwera innego niż System i należy uwzględnić następujące reguły:
  - Jeśli plik źródłowy należy do systemu plików zawierającego biblioteki, nazwa domyślna wygląda następująco: *nazwa_zbioru.nazwa_podzbioru*. Jeśli nie ma nazwy podzbioru, nazwą domyślną jest nazwa zbioru.
  - Jeśli plik źródłowy jest plikiem usług biblioteki dokumentów, domyślna nazwa składa się z nazwy pliku i rozszerzenia.
  - Jeśli plik źródłowy nie należy do systemu plików bibliotek ani nie jest plikiem usług biblioteki dokumentów, nazwą domyślną jest nazwa znajdująca się w nazwie źródłowej po ostatnim znaku ukośnika. Jeśli nazwa źródłowa nie zawiera ukośników, nazwa domyślna jest taka sama jak nazwa źródłowa.

W przypadku platform System i system generuje nazwę domyślną w tych podkomendach, stosując te same reguły, które odnoszą się do podkomendy PUT.

Podkomendy GET i MGET

W przypadku systemów innych niż platformy System i nazwa domyślna dla podkomend GET i MGET oparta jest na części nazwy źródłowej, która znajduje się po ostatnim ukośniku. Jeśli nazwa źródłowa nie zawiera ukośników, jako nazwa domyślna używana jest cała nazwa źródłowa. Poniżej przedstawiono reguły tworzenia nazw domyślnych.

- Jeśli system plików klienta jest *systemem plików bibliotek* (baza danych systemu i5/OS), obowiązują następujące reguły:

  - jeśli plik zdalny zawiera kropkę (.), znaki poprzedzające kropkę skracane są do 10 znaków i tworzą nazwę zbioru; znaki znajdujące się po kropce skracane są do 10 znaków i tworzą nazwę podzbioru,
  - jeśli nazwa pliku zdalnego nie zawiera kropki, zarówno nazwa zbioru, jak i nazwa podzbioru tego zbioru tworzone są tak, aby wykorzystać nazwę pliku zdalnego skróconą do 10 znaków,
  - jeśli formatem nazwy jest 1, system dodaje do zbioru odpowiednie rozszerzenia i części nazwy podzbioru.
- Jeśli system plików klienta to *usługi biblioteki dokumentów*, obowiązują następujące reguły:
  - jeśli plik zdalny zawiera kropkę, znaki znajdujące się przed kropką skracane są do 8 znaków; znaki znajdujące się po kropce skracane są do 3 znaków,
  - jeśli plik zdalny nie zawiera kropki, nazwa skracana jest do 8 znaków bez rozszerzenia.
- Dla pozostałych systemów plików nazwą domyślną jest nazwa znajdująca się w nazwie zdalnej po ostatnim ukośniku.

Uwagi:

1. Zbiory składowania nie zawierają podzbiorów, tak więc domyślne nazwy tych zbiorów nie zawierają części oznaczającej podzbiór.
2. System wyświetla nazwy domyślne, gdy aktywny jest tryb DEBUG.

Więcej informacji dotyczących składni:

Konwencje składni komend klienta FTP

Nazwy plików do przesyłania

Komendy klienta FTP używane do przesyłania danych mogą zawierać parametr **plik_lokalny**, **plik_zdalny** lub oba te parametry. Można ich użyć do określenia danych, które mają być przesłane. Istnieją następujące komendy przesyłania:

APPEND plik_lokalny [plik_zdalny]

DELETE plik_zdalny

GET plik_zdalny [plik_lokalny]

MDELETE pliki_zdalne

MGET pliki_zdalne

MPUT pliki_lokalne

PUT plik_lokalny [plik_zdalny]

Wartości parametrów plik_lokalny i plik_zdalny mogą być nazwami w pełni lub częściowo kwalifikowanymi. Niepełna nazwa zawiera nazwę danych i jedną lub więcej nazw znajdujących się w porządku hierarchicznym powyżej danych. Pełna nazwa zawiera wszystkie nazwy znajdujące się w porządku hierarchicznym powyżej danych.

W przypadku nazwy niepełnej, do określenia pliku, który ma być przetwarzany, używany jest bieżący katalog roboczy. Katalog roboczy w lokalnym systemie klienta można określić za pomocą podkomendy LCD. Katalog roboczy w systemie zdalnym można ustawić za pomocą podkomendy CD.

Format nazw parametru plik_lokalny musi być zgodny z regułami nazewnictwa plików systemu i5/OS. Nazwy parametru plik_zdalny muszą być zgodne z regułami nezewnictwa obowiązującymi w systemie zdalnym.

Więcej informacji dotyczących składni:

- Parametry podkomend można ująć w znaki apostrofu (') lub cudzysłowu (″).
- Konwencje składni komend klienta FTP: w sekcji tej opisane są zasady składni podkomend klienta FTP.

  Zadania pokrewne

  "Ujmowanie parametrów podkomend w cudzysłowy lub apostrofy" na stronie 147
  Parametry podkomend można ująć w znaki apostrofu (') lub cudzysłowu (″).

  Odsyłacze pokrewne

"APPEND (Dodanie podzbioru zbioru lokalnego do pliku zdalnego - Append a Local File Member to a Remote File)" na stronie 62
Podkomenda APPEND klienta FTP i5/OS służy do dodawania lokalnego podzbioru zbioru, dokumentu lub innego pliku systemu plików do zbioru zdalnego.

"GET (Kopiowanie pliku z systemu zdalnego do lokalnego - Copy a File from a Remote System to the Local System)" na stronie 69
Podkomenda GET klienta FTP i5/OS służy do kopiowania pliku z systemu zdalnego do systemu lokalnego.

"PUT (Kopiowanie podzbioru zbioru z systemu lokalnego do pliku w systemie zdalnym - Copy a File Member from the Local System to a File on a Remote System)" na stronie 81
Podkomenda PUT klienta FTP i5/OS służy do kopiowania lokalnego podzbioru zbioru do systemu zdalnego.

"MPUT (Wysłanie wielu podzbiorów z systemu lokalnego do systemu zdalnego - Send Multiple File Members from the Local System to a Remote System)" na stronie 78
Podkomenda MPUT klienta FTP i5/OS służy do kopiowania wielu plików do systemu zdalnego.

"MGET (Kopiowanie wielu plików z systemu zdalnego do systemu lokalnego - Copy Multiple Files from a Remote System to the Local System)" na stronie 76
Podkomenda MGET klienta FTP i5/OS służy do kopiowania wielu plików z systemu zdalnego.

"DEBUG (Zmiana wartości limitu czasu oczekiwania dla klienta - Change Client Time-Out Limit Values)" na stronie 67
Podkomenda DEBUG klienta FTP i5/OS służy do zmiany limitów czasu klienta, jeśli domyślne wartości limitu czasu są niewystarczające, aby przesyłanie danych zakończyło się pomyślnie. Wartości te należy zmieniać jedynie wtedy, gdy ruch w sieci lub inne warunki spowodują znaczne wydłużenie czasu przesyłania.

"LCD (Zmiana biblioteki roboczej lub katalogu w systemie lokalnym - Change Working Library or Directory on Local System)" na stronie 72
Podkomenda LCD klienta FTP i5/OS służy do zmiany katalogu roboczego w systemie lokalnym.

"CD (Zmiana katalogu roboczego lub biblioteki - Change Working Directory or Library)" na stronie 65
Podkomenda CD klienta FTP i5/OS służy do zmiany katalogu roboczego, biblioteki lub grupy plików w systemie zdalnym.

"DELETE (Usunięcie pliku z systemu zdalnego - Delete a File on a Remote System)" na stronie 68
Podkomenda DELETE klienta FTP i5/OS służy do usuwania zbioru lub podzbioru zbioru bazy danych w systemie zdalnym. System zdalny może zażądać uprawnień do usunięcia pliku. W celu wysłania odpowiedzi na to żądanie należy użyć podkomendy ACCT (Wysłanie informacji o koncie - Send Account Information).

"MDELETE (Usunięcie wielu plików w systemie zdalnym - Delete Multiple Files on a Remote System)" na stronie 75
Podkomenda MDELETE klienta FTP i5/OS służy do usuwania wielu plików z serwera FTP.

"Nazwy plików do przesyłania"
Podkomendy klienta FTP używane do przesyłania danych mogą zawierać parametr **plik_lokalny**, **plik_zdalny** lub oba te parametry. Można ich użyć do nazwania danych, które mają być przesłane.

Nazwy plików do przesyłania

Podkomendy klienta FTP używane do przesyłania danych mogą zawierać parametr **plik_lokalny**, **plik_zdalny** lub oba te parametry. Można ich użyć do nazwania danych, które mają być przesłane.

Istnieją następujące komendy przesyłania:

APPEND plik_lokalny [plik_zdalny]

DELETE plik_zdalny

GET plik_zdalny [plik_lokalny]

MDELETE pliki_zdalne

MGET pliki_zdalne

MPUT pliki_lokalne

PUT plik_lokalny [plik_zdalny]

Wartości parametrów plik_lokalny i plik_zdalny mogą być nazwami w pełni lub częściowo kwalifikowanymi. Niepełna nazwa zawiera nazwę danych i jedną lub więcej nazw znajdujących się w porządku hierarchicznym powyżej danych. Pełna nazwa zawiera wszystkie nazwy znajdujące się w porządku hierarchicznym powyżej danych.

W przypadku nazwy niepełnej, do określenia pliku, który ma być przetwarzany, używany jest bieżący katalog roboczy. Katalog roboczy w lokalnym systemie klienta można określić za pomocą podkomendy LCD. Katalog roboczy w systemie zdalnym można określić za pomocą podkomendy CD.

Format nazw parametru plik_lokalny musi być zgodny z regułami nazewnictwa plików systemu i5/OS. Nazwy parametru plik_zdalny muszą być zgodne z regułami nezewnictwa obowiązującymi w systemie zdalnym.

Więcej informacji dotyczących składni:

- Parametry podkomend można ująć w znaki apostrofu (') lub cudzysłowu (″).
- Domyślne nazwy plików dla podkomend klienta służących do przesyłania danych: odsyłacz do informacji o domyślnych nazwach plików dla podkomend klienta służących do przesyłania danych.
- Konwencje składni komend klienta FTP: w sekcji tej opisane są zasady składni podkomend klienta FTP.

Zadania pokrewne

"Ujmowanie parametrów podkomend w cudzysłowy lub apostrofy" na stronie 147
Parametry podkomend można ująć w znaki apostrofu (') lub cudzysłowu (″).

Odsyłacze pokrewne

"APPEND (Dodanie podzbioru zbioru lokalnego do pliku zdalnego - Append a Local File Member to a Remote File)" na stronie 62
Podkomenda APPEND klienta FTP i5/OS służy do dodawania lokalnego podzbioru zbioru, dokumentu lub innego pliku systemu plików do zbioru zdalnego.

"DELETE (Usunięcie pliku z systemu zdalnego - Delete a File on a Remote System)" na stronie 68
Podkomenda DELETE klienta FTP i5/OS służy do usuwania zbioru lub podzbioru zbioru bazy danych w systemie zdalnym. System zdalny może zażądać uprawnień do usunięcia pliku. W celu wysłania odpowiedzi na to żądanie należy użyć podkomendy ACCT (Wysłanie informacji o koncie - Send Account Information).

"GET (Kopiowanie pliku z systemu zdalnego do lokalnego - Copy a File from a Remote System to the Local System)" na stronie 69
Podkomenda GET klienta FTP i5/OS służy do kopiowania pliku z systemu zdalnego do systemu lokalnego.

"MDELETE (Usunięcie wielu plików w systemie zdalnym - Delete Multiple Files on a Remote System)" na stronie 75
Podkomenda MDELETE klienta FTP i5/OS służy do usuwania wielu plików z serwera FTP.

"MGET (Kopiowanie wielu plików z systemu zdalnego do systemu lokalnego - Copy Multiple Files from a Remote System to the Local System)" na stronie 76
Podkomenda MGET klienta FTP i5/OS służy do kopiowania wielu plików z systemu zdalnego.

"MPUT (Wysłanie wielu podzbiorów z systemu lokalnego do systemu zdalnego - Send Multiple File Members from the Local System to a Remote System)" na stronie 78
Podkomenda MPUT klienta FTP i5/OS służy do kopiowania wielu plików do systemu zdalnego.

"PUT (Kopiowanie podzbioru zbioru z systemu lokalnego do pliku w systemie zdalnym - Copy a File Member from the Local System to a File on a Remote System)" na stronie 81
Podkomenda PUT klienta FTP i5/OS służy do kopiowania lokalnego podzbioru zbioru do systemu zdalnego.

"LCD (Zmiana biblioteki roboczej lub katalogu w systemie lokalnym - Change Working Library or Directory on Local System)" na stronie 72
Podkomenda LCD klienta FTP i5/OS służy do zmiany katalogu roboczego w systemie lokalnym.

"CD (Zmiana katalogu roboczego lub biblioteki - Change Working Directory or Library)" na stronie 65
Podkomenda CD klienta FTP i5/OS służy do zmiany katalogu roboczego, biblioteki lub grupy plików w systemie zdalnym.

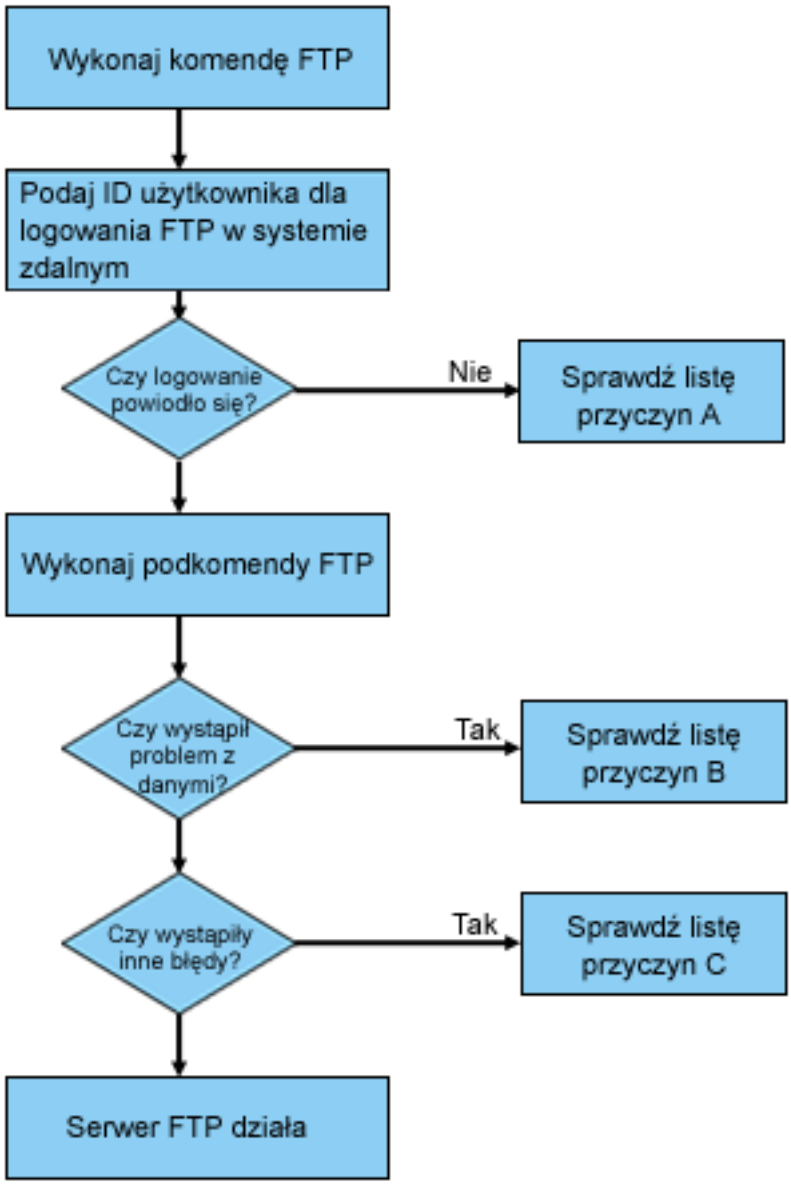
"Nazwy plików dla podkomend klienta służących do przesyłania danych" na stronie 148
W przypadku niektórych podkomend można używać domyślnych nazw plików źródłowych i docelowych; należy jednak określić nazwę pliku dla pozostałych podkomend.

Rozwiązywanie problemów z protokołem FTP

W tym temacie przedstawiono podstawowe informacje dotyczące rozwiązywania problemów z serwerem lub klientem FTP.

Określanie problemów związanych z protokołem FTP

Jeśli podczas korzystania z protokołu FTP wystąpi problem, należy za pomocą schematu oraz list przyczyn, które są zawarte w poniższym temacie, zidentyfikować przyczynę tego problemu.



Rysunek 13. Analiza problemów dotyczących FTP

Lista przyczyn A

1. Czy występuje duże opóźnienie między nawiązaniem połączenia z serwerem FTP i5/OS a otrzymaniem zapytania o identyfikator użytkownika? Jeśli tak, należy sprawdzić konfigurację systemu DNS w systemie. Serwer FTP wyśle zapytanie DNS natychmiast po zrealizowaniu nowego połączenia. Problemy związane z systemem DNS mogą być przyczyną zawieszania się systemu na kilka minut przed otrzymaniem odpowiedzi.

2. Sprawdź, czy program obsługi wyjścia został dodany do punktu wyjścia logowania do serwera FTP. Jeśli tak, to sprawdź, czy logowanie, które nie powiodło się, jest dozwolone przez program obsługi wyjścia.
3. Jeśli pojawiło się żądanie hasła sprawdź, czy logowanie zdalne wymaga podania hasła. Połączenie może zostać zerwane, ponieważ niektóre systemy żądają podania hasła, ale podanie hasła nie jest wymagane.
4. Jeśli jest to wymagane, skonfiguruj hasło w systemie zdalnym. Jeśli w systemie zostaną zmienione informacje o ochronie, może być konieczne ponowne uruchomienie systemu.
5. Sprawdź identyfikator użytkownika i hasło wykonując próbne wpisanie się do systemu zdalnego. Jeśli próba wpisania się do systemu powiodła się, skontaktuj się z właścicielem systemu w celu weryfikacji poprawności identyfikatora użytkownika i hasła.

Lista przyczyn B

1. Jeśli przesyłasz pliki binarne, upewnij się, czy aktywny jest tryb binarny.
2. Upewnij się, że tabele odwzorowań klienta i serwera są zgodne. Sprawdzenie takie jest konieczne tylko w przypadku, gdy korzystasz z własnych tabel odwzorowań.
3. Sprawdź, czy dla przesyłania danych został podany poprawny identyfikator CCSID. Jeśli nie, użyj komendy TYPE lub LTYPE, aby przed rozpoczęciem przesyłania danych ustawić poprawną wartość identyfikatora CCSID.
4. Utwórz zbiór w systemie, w którym planujesz przechowywać dane. Ustaw odpowiednią długość rekordu, liczbę podzbiorów, liczbę przyrostów. Ponownie spróbuj wykonać przesyłanie danych i sprawdź, czy powiodło się.
5. Upewnij się, czy posiadasz uprawnienia do korzystania ze zbiorów i podzbiorów zbioru.
6. Sprawdź, czy przesłany zbiór zawiera dane dziesiętne spakowane czy dane dziesiętne nieupakowane.
7. Jeśli przesyłasz zbiór składowania, sprawdź, czy wykorzystywany jest odpowiedni sposób przesyłania zbiorów.

Lista przyczyn C

1. Sprawdź ograniczenia wielkości zbiorów w systemie zdalnym.
2. Sprawdź, czy zakończył odliczanie czasu zegar serwera FTP. Wartość limitu czasu można ustawić za pomocą komendy QUOTE TIME.
3. Aby sprawdzić, czy interfejs *LOOPBACK jest aktywny, skorzystaj z komendy NETSTAT. Następnie odtwórz sytuację, która spowodowała pojawienie się problemu, wykonując komendę FTP LOOPBACK (z jednej platformy System i do drugiej platformy System i).
   - Jeśli *nie można odtworzyć* sytuacji, która spowodowała pojawienie się problemu, oznacza to, że jest to prawdopodobnie problem związany z systemem zdalnym.
   - Jeśli problem *można odtworzyć*, wykonaj następujące czynności:
     a. Jeśli jest to problem związany z serwerem FTP, uruchom śledzenie serwera FTP, używając komendy Śledzenie aplikacji TCP/IP (Trace TCP/IP Application - TRCTCPAPP).
     b. Odtwórz sytuację, która spowodowała pojawienie się problemu.
     c. Zakończ połączenie FTP. Więcej informacji zawiera temat Uruchamianie i zatrzymywanie serwera FTP.
     d. Zakończ śledzenie serwera FTP, używając komendy TRCTCPAPP.
     e. Znajdź zbiór buforowy o następujących parametrach:
        – nazwa zbioru - QTMFFTRC,
        – nazwa użytkownika powiązanego z plikiem jest nazwą użytkownika, który wydał komendę TRCTCPAPP.

        Wyniki śledzenia znajdują się w zbiorze buforowym w domyślnej kolejce wyjściowej systemu, który jest pozwiązany z zadaniem serwera FTP.
     f. Wyślij zbiór buforowy.
     g. Jeśli problem leży po stronie klienta FTP, śledzenie można przeprowadzić za pomocą podkomendy klienta DEBUG 100.
     h. Jeśli klient FTP jest uruchamiany interaktywnie, naciśnij klawisz F6 (Print - Drukuj), aby utworzyć zbiór buforowy zawierający historię wprowadzonych podkomend klienta FTP i odpowiedzi serwera FTP na te

komendy. Jeśli klient FTP jest uruchamiany w trybie wsadowym nienadzorowanym, historia podkomend i odpowiedzi serwera FTP jest zapisywana do podanego zbioru wyjściowego.

Zadania pokrewne

“Uruchamianie i zatrzymywanie serwera FTP” na stronie 26
Serwer FTP można uruchamiać i zatrzymywać za pomocą programu System i Navigator.

Odsyłacze pokrewne

“Punkt wyjścia logowania do serwera FTP” na stronie 106
Uwierzytelnianiem logowania do serwera aplikacji TCP/IP można sterować za pomocą punktu wyjścia logowania do serwera aplikacji TCP/IP. Ten punkt wyjścia umożliwia dostęp do serwera FTP na podstawie adresu systemu, który nawiązał sesję. Dzięki temu można określić początkowy katalog roboczy inny od tego, który znajduje się w profilu użytkownika.

Materiały wymagane do raportowania problemów dotyczących FTP

W tym rozdziale opisano informacje, których może wymagać przedstawiciel serwisu firmy IBM, aby rozwiązać problem związany z protokołem FTP.

Podczas zgłaszania problemu związanego z protokołem FTP do firmy IBM należy dołączyć następujące informacje:

- Wyniki śledzenia komunikacji od momentu awarii (wymagane tylko dane TCP/IP) w dwóch formatach: ASCII i EBCDIC.
- Jeśli klient lub serwer FTP zaprotokołował dane błędu oprogramowania, należy wysłać te dane.

  Uwaga: Aby protokołowanie błędów oprogramowania było wykonywane, wartość systemowa QSFWERRLOG musi być równa *LOG. Jeśli wartość QSFWERRLOG wynosi *NOLOG, należy ją zmienić na *LOG, spróbować odtworzyć błąd i wysłać zaprotokołowane dane błędu oprogramowania. Jeśli zostaną przesłane dane błędu oprogramowania, nie ma potrzeby wykonywania śledzenia protokołu FTP.
- Protokoły zadań QTCPIP i wszelkie protokoły zadań serwera lub klienta FTP.
- Dane śledzenia debugowania klienta FTP i serwera FTP.
- W razie wystąpienia problemów związanych z klientem FTP zbiór buforowy zawierający sesję klienta FTP (który można uzyskać, naciskając klawisz Drukuj (F6) w trakcie sesji FTP).
- Jeśli problem jest związany z integralnością danych, należy wysłać zbiór, podzbiór lub bibliotekę, które są przyczyną problemu, a także kopię opisu zbioru, podzbioru lub biblioteki.

Pojęcia pokrewne

“Śledzenie klienta FTP” na stronie 157
Aby utworzyć zapis śledzenia klienta FTP lub wyświetlić komendy wysłane do serwera FTP, należy użyć komendy DEBUG klienta FTP.

“Śledzenie serwera FTP”
Serwer FTP można śledzić z dowolnego systemu używającego protokołu TCP/IP.

Śledzenie serwera FTP

Serwer FTP można śledzić z dowolnego systemu używającego protokołu TCP/IP.

Istnieją następujące sposoby śledzenia serwera FTP:

- Komenda DBUG serwera FTP uruchamia śledzenie w ramach sesji FTP.
- Komenda Śledzenie aplikacji TCP/IP (Trace TCP/IP Application - TRCTCPAPP) umożliwia śledzenie wszystkich serwerów FTP w systemie.

Śledzenie serwera FTP za pomocą podkomendy DBUG

Aby włączyć śledzenia serwera FTP, wykonaj następujące czynności:

1. Wpisz QUOTE DBUG.

```
                          Protokół FTP

 Poprzednie podkomendy i komunikaty FTP:
 Łączenie z hostem o nazwie xxxxxnnn.xxxxxxxx.xxx.xxx i adresie
 n.nnn.nn.nnn przy użyciu portu 21.
 220-QTCP w xxxxxnnn.xxxxxxxx.xxx.xxx.
 220 Połączenie zostanie zamknięte po 5 minutach pracy jałowej.
 215  Zdalnym systemem operacyjnym jest i5/OS. Wersja TCP/IP:
 "V4R4M0".
>
  331 Wpisanie hasła.
  230 Zarejestrowanie się jako TEST.
  250  Używany obecnie format nazewnictwa: "0".
  257 Biblioteka bieżąca: "QGPL".
> quote dbug
  250  Tryb debugowania jest włączony.
Wpisz podkomendę FTP.
===> quote dbug



 F3=Wyjście     F6=Drukuj     F9=Poprzednie komendy
 F17=Początek   F18=Koniec    F21=Wiersz komend CL
```

2. Wykonaj operacje FTP, które chcesz śledzić.
3. Ponownie wpisz QUOTEDBUG, aby zakończyć śledzenie. Proces śledzenia tworzy zbiór buforowy o nazwie QTMFFTRC. Znajduje się on w domyślnej kolejce wyjściowej. Jego właścicielem jest zawsze użytkownik, który zalogował się do serwera FTP w momencie zakończenia śledzenia.
4. Wpisz QUIT, aby zakończyć sesję FTP.
5. Aby odnaleźć kolejkę wyjściową, wprowadź następującą komendę:

   ```
   DSPSYSVAL QPRTDEV
   ```

   Zostanie wyświetlony ekran podobny do poniższego:

   ```
   Wartość systemowa . . . . . :   QPRTDEV
   Opis  . . . . . :   Opis drukarki
   Drukarka   . . . . :   PRT01          Nazwa
   ```

   Nazwa drukarki jest również nazwą domyślnej kolejki wyjściowej systemu.
6. Zapisz nazwę drukarki. W tym przykładzie nazwą drukarki jest PRT01.
7. Naciśnij klawisz F12 (Anuluj), aby wrócić do ekranu, na którym została wpisana komenda DSPSYSVAL.
8. Wpisz następującą komendę:

   ```
   WRKOUTQ OUTQ(drukarka)
   ```

   W miejsce słowa drukarka wpisz nazwę drukarki wyświetloną na poniższym ekranie. W tym przykładzie nazwą kolejki wyjściowej jest PRT01. Zostanie wyświetlony ekran podobny do poniższego:

   ```
                             Praca z kolejką wyjściową
   Kolejka: PRT01       Biblioteka:   QGPL           Status: RLS
   Wpisz opcje i naciśnij klawisz Enter.
     1=Wyślij 2=Zmień 3=Wstrzymaj 4=Usuń 5=Wyświetl 6=Zwolnij 7=Komunikaty
     8=Atrybuty          9=Praca ze statusem drukowania
   Opc  Zbiór       Użytkownik  Dane użytk. Stat. Strony  Kopie   Typ formatu Priorytet
    _   QTCPPRT     QTCP        QTMSMTP     HLD     46   1      *STD         5
    _   QTMFFTRC    QSECOFR                 HLD     44   1      *STD         5
   ```

9. Jeśli na ekranie zostanie wyświetlony komunikat Więcej..., naciśnij klawisz F18 (Dół strony), aby wyświetlić koniec listy zbioru buforowego.
10. Znajdź ostatni zbiór o nazwie QTMFFTRC, którego właścicielem jest użytkownik, który zalogował się do serwera FTP, gdy rozpoczęto śledzenie.

11. Naciśnij klawisz F11 (Widok 2), aby wyświetlić datę i godzinę zbioru, z którym chcesz pracować.
12. Sprawdź, czy pracujesz z najnowszym zbiorem buforowym QTMFFTRC.

W opisie problemu podaj, że wykonano śledzenie, oraz jego wynik. Razem z opisem wyślij wszystkie dostępne informacje śledzenia.

W poniższym przykładzie wykorzystano podkomendę DBUG serwera FTP:

```
                          Protokół FTP

 Poprzednie podkomendy i komunikaty FTP:
 Łączenie z hostem o nazwie xxxxxnnn.xxxxxxxx.xxx.xxx i adresie
 n.nnn.nn.nnn przy użyciu portu 21.
 220-QTCP w xxxxxnnn.nnnnnnnn.nnn.nnn.
 220 Połączenie zostanie zamknięte po 5 minutach pracy jałowej.
  215  Zdalnym systemem operacyjnym jest i5/OS. Wersja TCP/IP:
  "V4R4M0".
>
  331 Wpisanie hasła.
  230 Zarejestrowanie się jako TEST.
  250  Używany obecnie format nazewnictwa: "0".
  257 Biblioteka bieżąca: "QGPL".



Wpisz podkomendę FTP.
===> quote dbug



 F3=Wyjście     F6=Drukuj     F9=Poprzednie komendy
 F17=Początek   F18=Koniec    F21=Wiersz komend CL
```

Śledzenie serwera FTP za pomocą komendy Śledzenie aplikacji TCP/IP (Trace TCP/IP Application - TRCTCPAPP)

Komenda Śledzenie aplikacji TCP/IP (Trace TCP/IP Application - TRCTCPAPP) umożliwia śledzenie *wszystkich* serwerów FTP w *całym systemie*.

Komenda TRCTCPAPP jest przeznaczona do wykorzystania przez przeszkolony personel serwisu i programistów. Aby jej używać, wymagane jest uprawnienie specjalne *SERVICE. Należy się nią posłużyć w sytuacjach, które wymagają przechwycenia danych śledzenia w celu serwisowania i tworzenia programów. Komenda TRCTCPAPP pozwala doświadczonemu personelowi dynamicznie uruchamiać i zatrzymywać śledzenie aplikacji.

Za pomocą komendy TRCTCPAPP można przechwytywać informacje śledzenia dla aplikacji TCP/IP FTP. Wewnętrzne informacje śledzenia można przechwytywać dla serwera FTP i5/OS. Informacje te można filtrować za pomocą zdalnego adresu IP i portu lub profilu użytkownika systemu i5/OS. W danym momencie w systemie może być włączone tylko jedno śledzenie.

Dwa poniższe przykłady ilustrują stosowanie komendy TRCTCPAPP:

Przykład 1:

```
TRCTCPAPP APP(*FTP) SET(*ON)
```

Komenda ta uruchomi śledzenie wszystkich serwerów FTP. Śledzenie innych aplikacji TCP nie ulegnie zmianie.

Przykład 2:

```
TRCTCPAPP APP(*FTP) SET(*CHK)
```

Za pomocą tej komendy można sprawdzić status śledzenia zadań serwera FTP. Przyjmując, że ostatnio wpisaną komendą była:

```
TRCTCPAPP APP(*FTP) SET(*ON) USER(JOECOOL)
```

Formatem odpowiedzi na tę komendę będzie seria komunikatów podobnych do poniższych komend:

```
TCP45B7 TRCTCPAPP APP(*FTP) SET(*ON) USER(JOECOOL)
        MAXSTG(*DFT) TRCFULL(*WRAP)
TCP45B1 Śledzenie jest aktywne dla *FTP.
TCP45B2 Rozpoczęto przechwytywanie danych dla *FTP.
TCP45B3 Bufor danych został zawinięty dla *FTP.
```

Pojęcia pokrewne

“Materiały wymagane do raportowania problemów dotyczących FTP” na stronie 154
W tym rozdziale opisano informacje, których może wymagać przedstawiciel serwisu firmy IBM, aby rozwiązać problem związany z protokołem FTP.

Odsyłacze pokrewne

“DBUG (Włączenie śledzenia serwera FTP - Turn on the FTP Server Trace)” na stronie 47
Podkomenda DBUG serwera FTP i5/OS służy do uruchamiania lub zatrzymywania śledzenia serwera.

Śledzenie klienta FTP

Aby utworzyć zapis śledzenia klienta FTP lub wyświetlić komendy wysłane do serwera FTP, należy użyć komendy DEBUG klienta FTP.

Komenda DEBUG przełącza tryb debugowania. Jeśli zostanie podana opcjonalna wartość trybu debugowania, poziom debugowania zostanie ustawiony na nią. Przy włączonym debugowaniu po znakach ’>>>’ zostanie wyświetlona każda komenda wysyłana do serwera FTP. Aby włączyć śledzenie klienta FTP, parametr trybu debugowania należy ustawić na wartość 100.

DEBug *[wartość debugowania]*

wartość debugowania

Jeśli wartość ta wynosi 0, debugowanie jest wyłączone. Jeśli wartość debugowania jest dodatnią liczbą całkowitą, debugowanie jest włączone.

Jeśli nie zostanie podana żadna wartość, debugowanie jest przełączane z wartości zero na jeden lub z wartości dodatniej na zero.

100 Włącza tworzenie zapisu aktywności klienta FTP. Klient zapisuje wyniki śledzenia do czasu, gdy wartość DEBUG zostanie wyłączona lub gdy działanie klienta zostanie zakończone. (Formatowanie danych śledzenia po zakończeniu śledzenia może zająć dużo czasu.)

Uwaga: Śledzenie klienta FTP powinno być używane tylko w celu raportowania firmie IBM problemów z oprogramowaniem. Użycie tej funkcji może wpłynąć na wydajność systemu.

W wersji V4R4 do klienta FTP dodano nową funkcję debugowania. Jest ona podobna do opisanej wyżej funkcji DEBUG 100. Po uruchomieniu klient sprawdza istnienie obszaru danych o nazwie QTMFTPD100.

Obszar danych QTMFTPD100 należy utworzyć w bibliotece QTEMP za pomocą następującej komendy:

```
CRTDTAARA DTAARA(QTEMP/QTMFTPD100) TYPE(*LGL) AUT(*USE)
```

Jeśli obszar danych QTMFTPD100 istnieje, wówczas klient zmieni wartość debugowania na 100 i uruchomi śledzenie klienta FTP. Zadaniem tej opcji jest włączenie śledzenia klienta FTP w sytuacjach, gdy śledzenie to *nie może* być włączone za pomocą komendy DEBUG 100.

Pojęcia pokrewne

"Materiały wymagane do raportowania problemów dotyczących FTP" na stronie 154
W tym rozdziale opisano informacje, których może wymagać przedstawiciel serwisu firmy IBM, aby rozwiązać problem związany z protokołem FTP.

Praca z zadaniami i protokołami zadań serwera FTP

Istnieje możliwość otrzymania buforowego pliku protokołu zadań serwera FTP w celu wyszukania błędów. Serwer FTP automatycznie zapisuje w pliku buforowym protokół zadania serwera, jeśli kończy się ono błędem.

Protokół zadania serwera można zapisać w zbiorze buforowym, nie kończąc połączenia, poprzez wywołanie następującej podkomendy z poziomu klienta FTP:

```
QUOTE RCMD DSPJOBLOG
```

Aby uzyskać kopię komunikatów o błędzie zapisanych w protokole zadania serwera FTP, podkomenda ta musi zostać wydana bezpośrednio po wystąpieniu błędu. Protokół zadania można następnie przejrzeć, korzystając z komendy Praca ze zbiorami buforowymi (Work with Spooled Files - WRKSPLF).

Powyższa metoda jest polecana w sytuacjach, gdy komunikat odpowiedzi, który jest zwracany do klienta z serwera FTP, zawiera minimalną ilość informacji o błędzie mającym miejsce na serwerze FTP. Dzięki tej metodzie można na przykład uzyskać szczegółowe informacje dotyczące błędów we/wy, które wystąpiły w systemie z serwerem FTP.

Jeśli błędy uniemożliwiają utworzenie protokołu zadania serwera FTP w opisany powyżej sposób, to aby wymusić tworzenie buforowanego protokołu zadania dla każdej sesji FTP, wprowadź następującą komendę:

```
CHGJOBD JOBD(QUSRSYS/QTMFTPS) LOG(4 00 *SECLVL)
```

Następnie powtórz sytuację, która była przyczyną pojawienia się błędu. Aby odtworzyć normalne działanie protokołu zadania po uzyskaniu potrzebnych danych, wprowadź komendę:

```
CHGJOBD JOBD(QUSRSYS/QTMFTPS) LOG(4 00 *NOLOG)
```

Aby otrzymywać buforowy protokół zadania na koniec każdej sesji FTP i za każdym razem, gdy serwer FTP kończy działanie (z błędem lub bez błędu), należy skorzystać z komendy Zmiana opisu zadania (Change Job Description - CHGJOBD) w następujący sposób:

```
CHGJOBD JOBD(QUSRSYS/QTMFTPS) LOG(4 00 *SECLVL)
```

Aby uzyskać protokół zadania buforowania dopiero po zakończeniu połączenia, należy użyć komendy CHGJOBD w następujący sposób:

```
CHGJOBD JOBD(QUSRSYS/QTMFTPS) LOG(4 00 *NOLIST)
```

Zadania serwera FTP i nazwy zadań

Zadania serwera FTP są uruchamiane, gdy zostanie wykonana komenda Uruchomienie TCP/IP (Start TCP/IP - STRTCP), a parametr FTP AUTOSTART ma wartość *YES, lub gdy zostanie wykonana komenda Uruchomienie serwera TCP/IP (Start TCP/IP Server - STRTCPSVR) z parametrem SERVER mającym wartość *FTP lub *ALL. Te zadania są uruchamiane w podsystemie QSYSWRK, a ich celem jest monitorowanie użytkowników odwiedzających serwer FTP. Format nazw tych zadań to QTFTP*nnnnn*, gdzie *nnnnn* jest numerem zadania serwera FTP wprowadzonego do tego serwera FTP.

Aby pracować z zadaniami serwera FTP, należy podać następującą komendę CL:

```
WRKACTJOB JOB(QTFTP*)
```

Odsyłacze pokrewne

Praca ze zbiorami buforowymi (Work with Spooled Files - WRKSPLF)

Licencja na kod oraz Informacje dotyczące kodu

IBM udziela niewyłącznej licencji na prawa autorskie, stosowanej przy używaniu wszelkich przykładowych kodów programów, na podstawie których można wygenerować podobne funkcje dostosowane do indywidualnych wymagań.

Z ZASTRZEŻENIEM GWARANCJI WYNIKAJĄCYCH Z BEZWZGLĘDNIE OBOWIĄZUJĄCYCH PRZEPISÓW PRAWA, IBM, PROGRAMIŚCI ANI DOSTAWCY IBM NIE UDZIELAJĄ NA NINIEJSZY PROGRAM ANI W ZAKRESIE EWENTUALNEGO WSPARCIA TECHNICZNEGO ŻADNYCH GWARANCJI, W TYM TAKŻE RĘKOJMI, NIE USTALAJĄ ŻADNYCH WARUNKÓW, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI CZY WARUNKÓW PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CZY NIENARUSZANIA PRAW STRON TRZECICH.

W ŻADNYCH OKOLICZNOŚCIACH IBM, ANI TEŻ PROGRAMIŚCI CZY DOSTAWCY PROGRAMÓW IBM, NIE PONOSZĄ ODPOWIEDZIALNOŚCI ZA PONIŻSZE SZKODY, NAWET JEŚLI ZOSTALI POINFORMOWANI O MOŻLIWOŚCI ICH WYSTĄPIENIA:

1. UTRATA LUB USZKODZENIE DANYCH;
2. SZKODY BEZPOŚREDNIE, SZCZEGÓLNE, UBOCZNE, POŚREDNIE ORAZ SZKODY, KTÓRYCH NIE MOŻNA BYŁO PRZEWIDZIEĆ PRZY ZAWIERANIU UMOWY, ANI TEŻ
3. UTRATA ZYSKÓW, KONTAKTÓW HANDLOWYCH, PRZYCHODÓW, REPUTACJI (GOODWILL) LUB PRZEWIDYWANYCH OSZCZĘDNOŚCI.

USTAWODAWSTWA NIEKTÓRYCH KRAJÓW NIE DOPUSZCZAJĄ WYŁĄCZENIA CZY OGRANICZENIA ODPOWIEDZIALNOŚCI ZA SZKODY BEZPOŚREDNIE, UBOCZNE LUB SZKODY, KTÓRYCH NIE MOŻNA BYŁO PRZEWIDZIEĆ PRZY ZAWIERANIU UMOWY, W ZWIĄZKU Z CZYM W ODNIESIENIU DO NIEKTÓRYCH KLIENTÓW POWYŻSZE WYŁĄCZENIE LUB OGRANICZENIE (TAK W CAŁOŚCI JAK I W CZĘŚCI) MOŻE NIE MIEĆ ZASTOSOWANIA.

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 dotyczące interfejsu programistycznego

Niniejsza publikacja na temat protokołu FTP 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:

IBM
IBM (logo)
i5/OS
OS/2
RISC System/6000
RS/6000
S/390
System i

Adobe, logo Adobe, PostScript oraz logo PostScript są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Adobe Systems Incorporated 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.

UNIX jest zastrzeżonym znakiem towarowym Open Group w Stanach Zjednoczonych i w innych krajach.

Nazwy innych przedsiębiorstw, produktów i 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