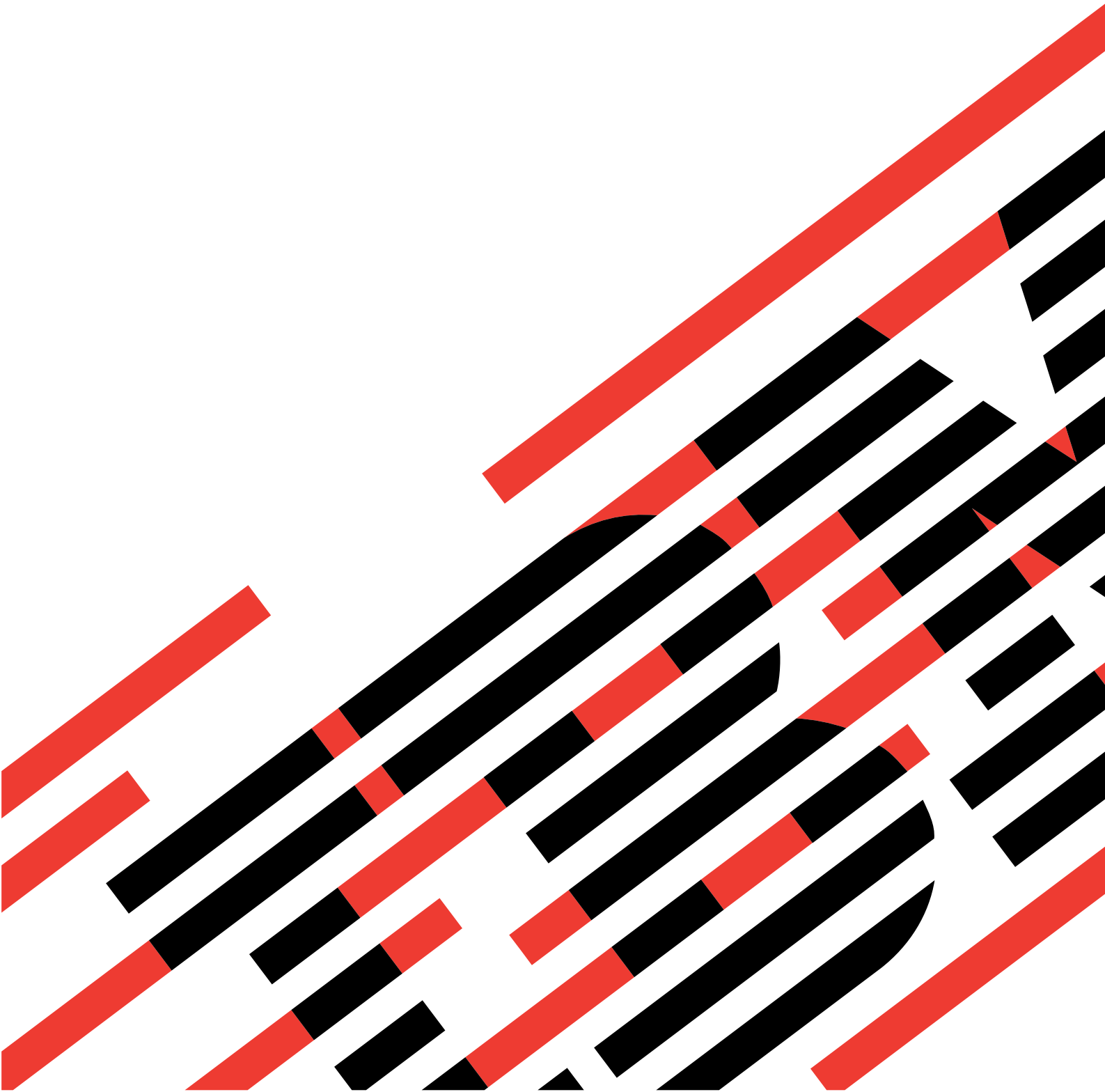


IBM

@server

iSeries

FTP



IBM

@server

iSeries

FTP

Spis treści

FTP	1
Co nowego w wersji V5R2	2
Drukowanie tego dokumentu	3
Scenariusze FTP	3
Scenariusz: Przesyłanie pliku ze zdalnego hosta	3
Scenariusz: Ochrona FTP za pomocą warstwy SSL	5
Szczegóły dotyczące konfiguracji	6
Konfigurowanie serwera FTP	9
Serwer FTP i program iSeries Navigator	10
Konfigurowanie serwerów FTP dla klientów FTP z interfejsem graficznym i dla narzędzi WWW	10
Konfigurowanie serwera anonimowego FTP	11
Przygotowanie serwera anonimowego FTP	12
Pisanie programów obsługi wyjścia dla anonimowego użytkownika FTP	13
Tworzenie w systemie OS/400 profilu użytkownika ANONYMOUS	14
Tworzenie publicznej biblioteki lub katalogu	14
Instalowanie i rejestrowanie programów obsługi wyjścia	14
Ochrona serwera FTP	15
Zapobieganie dostępowi do serwera FTP	15
Kontrolowanie dostępu do serwera FTP	17
Korzystanie z warstwy SSL do ochrony serwera FTP	18
Tworzenie lokalnego ośrodka certyfikacji	18
Wiązanie certyfikatów z serwerem FTP	20
Żądanie uwierzytelniania klienta dla serwera FTP (opcja)	20
Włączanie ochrony za pomocą SSL w serwerze FTP	21
Ochrona klienta FTP za pomocą TLS/SSL	22
Zarządzanie dostępem za pomocą programów obsługi wyjścia FTP	23
Zarządzanie dostępem za pomocą programu iSeries Navigator	24
Monitorowanie przyłączających się użytkowników FTP	24
Zarządzanie serwerem FTP	25
Uruchamianie i zatrzymywanie serwera FTP	25
Ustawianie liczby dostępnych serwerów FTP	25
Zwiększanie wydajności serwera FTP dzięki obsłudze podsystemów konfigurowalnych	25
Używanie klienta FTP w systemie iSeries	26
Uruchamianie i kończenie sesji klienta	26
Uwagi na temat przekroczenia limitu czasu przez serwer	30
Przesyłanie plików za pomocą FTP	31
Klient FTP jako zadanie wsadowe	32
Informacje dotyczące FTP	40
Komendy serwera FTP	40
ADDM (Dodanie podzbioru zbioru fizycznego - Add Physical File Member)	42
ADDV (Dodanie podzbioru zbioru fizycznego o zmiennej długości - Add Physical File Variable Length)	43
APPE (Dopisanie do istniejącego pliku - Append to Existing File)	43
AUTH (Autoryzacja - Authorization)	43
CRTL (Utworzenie biblioteki - Create Library)	44
CRTP (Utworzenie zbioru fizycznego - Create Physical File)	44
CRTS (Utworzenie źródłowego zbioru fizycznego - Create Source Physical File)	44
CWD (Zmiana katalogu roboczego lub biblioteki - Change working directory or library)	45
DEBUG (Włączenie śledzenia serwera FTP - Turn on the FTP Server Trace)	45
DELE (Usunięcie pliku lub dokumentu - Delete file or document)	45
DLTF (Usunięcie zbioru - Delete File)	46
DLTL (Usunięcie biblioteki - Delete Library)	46

HELP (Wyświetlanie pomocy ze zdalnego serwera iSeries - Getting Help from an iSeries Remote Server)	46
LIST (Lista zbiorów - File List)	47
MKD (Utworzenie katalogu - Make directory)	47
MODE (Ustawienie trybu przesyłania danych - Set Transfer Mode)	47
NLST (Lista nazw - Name List)	48
NOOP (Uzyskanie odpowiedzi serwera - Obtain Server Response)	48
PASS (Hasło -Password)	48
PASV (Użycie pasywnego połączenia danych - Use Passive Data Connection)	49
PBSZ (Zabezpieczenie wielkości bufora - Protection Buffer Size)	49
PORT (Port danych - Data Port)	49
PROT (Poziom ochrony kanału danych - Data Channel Protection Level)	50
PWD (Wyświetlenie katalogu roboczego lub biblioteki - Display Working Directory or Library)	50
QUIT (Zakończenie sesji serwera FTP - End an FTP Server Session)	50
RCMD (Wysłanie komendy języka CL do serwera FTP - Send a CL Command to an FTP Server System)	51
REIN (Reinicjowanie sesji pomiędzy systemami - Reinitialize Session between Systems)	51
RETR (Pobranie pliku - Retrieve file)	52
RMD (Usuwanie katalogu - Remove directory)	52
RNFR (Zmiana nazwy z - Rename From)	52
RNTO (Zmiana nazwy na - Rename To)	52
SITE (Wysłanie informacji używanych przez serwer - Send Information Used by a Server System)	53
STOR (Zapisanie pliku - Store File)	55
STOU (Zapisanie unikalnych - Store Unique)	55
STRU (Określenie struktury plików - Specify File Structure)	55
SYST (Identyfikacja nazwy systemu operacyjnego - Identify the Name of the Operating System)	56
TIME (Ustawienie wartości czasu oczekiwania dla serwera FTP - Set Time-Out Values for FTP Server)	56
TYPE (Określenie typu reprezentacji - Specify Representation Type)	57
USER (Wysłanie ID użytkownika do serwera - Send a User Logon ID to the Server)	58
Komendy klienta FTP	59
ACCT (Wysłanie informacji o koncie - Send Account Information)	61
APPEND (Dodanie podzbioru zbioru lokalnego do pliku zdalnego - Append a Local File Member to a Remote File)	61
ASCII (Zmiana typu pliku na ASCII - Change File Type to ASCII)	62
BINARY (Ustawienie typu przesyłania dla obrazu - Set Transfer Type to Image)	62
CD (Zmiana katalogu roboczego lub biblioteki - Change Working Directory or Library)	63
CLOSE (Zamknięcie sesji FTP z systemem zdalnym - End an FTP Session with the Remote System)	63
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)	64
DEBUG (Zmiana wartości limitu czasu oczekiwania dla klienta - Change Client Time-Out Limit Values)	64
DELETE (Usunięcie pliku z systemu zdalnego - Delete a File on a Remote System)	65
DIR (Wyświetlenie listy pozycji katalogu, bibliotek lub plików - List Directory Entries, Libraries, or Files)	65
EBCDIC (Zmiana typu pliku na EBCDIC - Change File Type to EBCDIC)	66
GET (Kopiowanie pliku z systemu zdalnego do lokalnego - Copy a File from a Remote System to the Local System)	66
HELP (Uzyskiwanie pomocy dla komend FTP - Getting Help for FTP Subcommands)	67
LCD (Zmiana biblioteki roboczej lub katalogu w systemie lokalnym - Change Working Library or Directory on Local System)	68
LOCSITE (Podanie informacji o środowisku lokalnym - Specify Local Site Information)	69
LOCSTAT (Wyświetlenie informacji o statusie lokalnym - Display Local Status Information)	70
LS (Wyświetlenie nazw plików zdalnych - List Remote File Names)	71

LTYPE (Typ lokalny - Local Type)	71
MDELETE (Usunięcie wielu plików w systemie zdalnym - Delete Multiple Files on a Remote System)	72
MGET (Kopiowanie wielu plików z systemu zdalnego do systemu lokalnego - Copy Multiple Files from a Remote System to the Local System)	73
MKDIR (Utworzenie katalogu - Make Directory).	73
MODE (Określenie trybu przesyłania danych - Specify Transmission Mode of Data)	74
MPUT (Wysłanie wielu podzbiorów z systemu lokalnego do systemu zdalnego - Send Multiple File Members from the Local System to a Remote System)	74
NAMEFMT (Wybranie formatu nazewnictwa plików - Select File Naming Format)	75
NULLFLDS (Umożliwienie przesyłania zbiorów z polami NULL -Allow Transfer of Files with NULL Fields).	76
OPEN (Połączenie z serwerem FTP w systemie zdalnym - Connect to FTP Server on a Remote System)	77
PASS (Wysłanie hasła - Send Your Password)	77
PUT (Kopiowanie podzbioru z systemu lokalnego do pliku w systemie zdalnym - Copy a File Member from the Local System to a File on a Remote System)	77
PWD (Wyświetlenie bieżącego katalogu, folderu lub biblioteki - Display Current Directory, Folder, or Library)	78
QUOTE (Wysłanie komendy do serwera FTP - Send a Subcommand to an FTP Server)	79
REINITIALIZE (Reinicjowanie sesji pomiędzy systemami - Reinitialize Session between Systems)	80
RENAME (Zmiana nazwy pliku w systemie zdalnym - Rename a File on a Remote System)	80
RESET (Resetowanie - Reset).	81
RMDIR (Usuwanie katalogu - Remove Directory)	81
SECData (Konfigurowanie ochrony danych - Setting data security protection).	81
SECOpen (Konfigurowanie ochrony danych - Setting data security protection)	82
SENDPASV (Określenie, czy wysyłać komendę PASV - Specify Whether to send a PASV Subcommand).	83
SENDPORT (Określenie, czy wysyłać komendę PORT - Specify Whether to Sends a PORT Subcommand).	84
SENDSITE (Określenie, czy wysłać komendę SITE - Specify Whether to Send a SITE Subcommand).	85
SITE (Wysłanie informacji używanych przez system zdalny - Send Information Used by a Remote System)	85
STATUS (Pobranie informacji o statusie z systemu zdalnego - Retrieve Status Information from a Remote System)	86
STRUCT (Określenie struktury plików - Specify File Structure)	86
SUNIQUE (Sterowanie nadpisywaniem plików - Control Overwriting of Files)	87
SYSCMD (Prześlij komendę CL iSeries do lokalnego systemu iSeries - Pass an iSeries 400 CL Command to Your Local iSeries 400 System)	87
TYPE (Określenie typu przesyłania plików - Specify File Transfer Type)	88
USER (Wysłanie ID użytkownika do systemu zdalnego - Send Your User ID to the Remote System)	90
VERBOSE (Sterowanie wyświetlaniem komunikatów odpowiedzi o błędach - Control of Text Display of Error Reply Messages)	90
Programy obsługi wyjścia FTP	91
Punkt wyjścia potwierdzenia żądania: klient i serwer	91
Przykład: kod programu obsługi wyjścia potwierdzenia żądania klienta lub serwera FTP w języku CL	93
Przykład: kod programu obsługi wyjścia potwierdzenia żądania serwera FTP w języku ILE RPG	95
Format punktu wyjścia VLRQ0100	99
Punkt wyjścia logowania do serwera	103
Przykład: kod programu obsługi wyjścia logowania do serwera FTP w języku CL	105
Przykład: kod programu obsługi wyjścia logowania do serwera FTP w języku C	106
Przykład: kod programu obsługi wyjścia logowania do serwera FTP w języku ILE RPG	115
Format TCPL0100 punktu wyjścia	118
Format TCPL0200 punktu wyjścia	122

Format TCPL0300 punktu wyjścia	127
Usuwanie programu obsługi wyjścia	131
Metody przesyłania danych	131
Przesyłanie pomiędzy serwerami iSeries plików zawierających upakowane dane dziesiętne	132
Przesyłanie zbiorów *SAVF	132
Przesyłanie dokumentów QDLS	133
Przesyłanie plików w systemach plików "root", QOpenSys, QLANSrv, QDLS i QOPT.	134
Przesyłanie plików za pomocą systemu plików QfileSvr.400.	134
Przesyłanie zbiorów QSYS.LIB	135
Otrzymywanie plików tekstowych w systemie plików QSYS.LIB	137
Uwagi dotyczące tworzenia zbiorów	138
Konwersje CCSID	138
Określanie tabel odwzorowań	138
Znakowanie strony kodowej CCSID dla plików serwera iSeries	139
Uwagi dla FTP dotyczące obsługi języków narodowych	140
Systemy plików i konwencje nazewnictwa	141
Systemy plików OS/400 obsługiwane przez protokół FTP	142
Komunikaty o statusie odpowiedzi serwera FTP	142
Konwencje składni komend serwera FTP	144
Konwencje składni komend klienta FTP	145
Umieszczanie parametrów komend	145
Nazwy plików dla komend klienta służących do przesyłania danych	146
Nazwy plików do przesyłania	147
Rozwiązywanie problemów dotyczących FTP	148
Określanie problemów dotyczących FTP.	149
Materiały wymagane do raportowania problemów dotyczących FTP.	151
Śledzenie serwera FTP	151
Śledzenie klienta FTP	154
Praca z zadaniami i protokołem zadania serwera FTP.	154

FTP

System iSeries można skonfigurować tak, aby wysyłał, odbierał i udostępniał pliki w sieci poprzez protokół przesyłania plików (FTP). Można w ten sposób także dodawać i usuwać pliki, a także zmieniać ich nazwy. Aby skonfigurować przesyłanie plików w systemie, należy skonfigurować i uruchomić protokół TCP/IP.

Więcej informacji o używaniu protokołu na serwerze iSeries zawierają poniższe sekcje:



Co nowego w wersji V5R2
Nowe funkcje do obsługi FTP w systemie iSeries w wersji V5R2.

Drukowanie tego dokumentu

Dokumentacja dotycząca FTP w formacie PDF do pobrania lub wydrukowania.

Scenariusze FTP

Informacje ułatwiające zrozumienie sposobu skonfigurowania i wykorzystania protokołu FTP.

Konfigurowanie serwera FTP

Konfigurowanie serwera FTP iSeries dla klientów FTP z interfejsami graficznymi, przeglądark i narzędzi WWW. Konfigurowanie serwera anonimowego FTP.

Ochrona serwera FTP

Zabezpieczenie danych poprzez ochronę FTP za pomocą warstwy SSL, monitorowanie użytkowników FTP i zarządzanie dostępem użytkowników do funkcji FTP.

Zarządzanie serwerem FTP

Administrowanie serwerem FTP, obejmujące uruchamianie i zatrzymywanie go, ochronę FTP i używanie warstwy SSL.

Używanie klienta FTP w systemie iSeries

Uruchamianie i zakańczanie sesji klienta, przesyłanie i otrzymywanie plików oraz konfigurowanie FTP jako zadania wsadowego.

Informacje dotyczące FTP

Informacje dotyczące komend serwera i klienta, programy obsługi wyjścia FTP, metody przesyłania danych i inne informacje.

Rozwiązywanie problemów dotyczących FTP

Informacje o rozwiązywaniu problemów dotyczących serwera lub klienta FTP.

Uwaga:

Aby zapoznać się z informacjami prawnymi, należy przeczytać sekcję Informacje dotyczące zastrzeżeń odnoszących się do kodu.



Co nowego w wersji V5R2

W wersji 5 wydanie 2 serwer FTP iSeries zawiera następujące udoskonalenia:

Udoskonalenia funkcji

- Serwer FTP obsługuje teraz biblioteki, które rezydują w niezależnych pulach pamięci dyskowej (IASP).
- Obsługa warstwy TLS (Transport Layer Security)/SSL (Secure Sockets Layer)
W wersji V5R2 serwer FTP umożliwia wykorzystanie warstwy TLS/SSL z poziomu klienta FTP systemu OS/400^R (tylko w razie uwierzytelnienia serwera). Ta obsługa pozwala na określenie, czy przepływ danych przez połączenia kontrolowane przez FTP, włączając w to hasło używane do uwierzytelniania, ma być szyfrowany. Zmiany wymienione niżej zostały wprowadzone w celu obsługi nowych możliwości:

Nowe komendy klienta:

- SECOpen (Konfigurowanie ochrony danych - Setting data security protection)
- SECDData (Konfigurowanie ochrony danych - Setting data security protection)

Nowe parametry dla komendy STRTCPFTP:

- Ochrona połączenia (Secure connection - SECCNN)
- Ochrona danych (Data protection - DTAPROT)

Nowe parametry dla komendy LOCSITE:

- DTAPROT C
- DTAPROT P
- DTAPROT

Nowe informacje

Temat FTP dla wersji V5R2 w Centrum informacyjnym został zaktualizowany. W niektórych przypadkach została zmieniona organizacja informacji, w celu zapewnienia łatwiejszego dostępu do nich. Do FTP dla wersji V5R2 dodano następujące informacje:

- scenariusze FTP udostępniają przykłady podstawowych zastosowań FTP; można je wykorzystać podczas planowania i konfigurowania serwera FTP w systemie iSeries,
- instrukcje korzystania z sesji SSL do ochrony serwera FTP zostały przeniesione do tego tematu z tematu omawiającego warstwę SSL,
- przykładowe programy punktów wyjścia do konfiguracji anonimowego FTP zostały przeniesione do tego tematu z serwisu Technical Reference,
 - punkt wyjścia logowania do serwera zawiera przykłady programów obsługi wyjścia logowania do serwera FTP napisane w językach CL, C i ILE RPG,
 - punkt wyjścia potwierdzenia żądania zawiera przykłady programów obsługi potwierdzenia żądania napisane w językach CL, C i ILE RPG,
- informacje dotyczące FTP, które dostępne były wcześniej w podręczniku Configuration and Reference, zostały dodane do tematu o protokole FTP.

Jak oznaczono informacje nowe lub zmienione

Aby łatwiej było zobaczyć wprowadzone zmiany techniczne, w dokumencie tym używa się:

- symbolu



do oznaczenia miejsca, w którym zaczynają się informacje nowe i zmienione,

- symbolu



do oznaczenia miejsca, w którym kończą się informacje nowe lub zmienione.

Aby znaleźć więcej informacji na temat tego, co jest nowe lub zmienione w tym wydaniu, przeczytaj Informacje dla użytkowników



Drukowanie tego dokumentu

Aby wyświetlić lub pobrać wersję PDF, należy wybrać FTP (około 600 kB lub 154 strony).

Zapisywanie plików PDF

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

1. W oknie przeglądarki kliknij prawym przyciskiem myszy wybrany dokument (jeden z powyższych odsyłaczy).
2. Kliknij **Zapisz jako...**
3. Przejdź do katalogu, w którym chcesz zapisać plik PDF.
4. Kliknij **Zapisz**.

Pobieranie programu Adobe Acrobat Reader

Program Adobe Acrobat Reader, potrzebny do drukowania i przeglądania plików PDF, można pobrać z serwisu WWW firmy Adobe (www.adobe.com/products/acrobat/readstep.html)



Scenariusze FTP



Następujące scenariusze 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.

Przesyłanie pliku ze zdalnego hosta

Przesyłanie pliku do serwera testowego. Wykorzystanie podstawowych funkcji FTP do przesłania pliku do zdalnego hosta.

Ochrona FTP za pomocą warstwy SSL

Wykorzystanie protokołu SSL w celu ochrony danych przesyłanych do przedsiębiorstw partnerskich.



Scenariusz: Przesyłanie pliku ze zdalnego hosta



Cele

Programista pracuje na zdalnym serwerze w środowisku języka Java™. Inżynier testujący system musi przesłać ze zdalnego serwera plik przykład.jar do lokalnego serwera testowego. Do przesłania pliku (w trybie binarnym) poprzez sieć TCP/IP wykorzystane zostaną podstawowe funkcje FTP. Zarówno klient, jak i serwer są systemami korzystającymi z FTP OS/400.

Szczegóły

Do przesłania pliku wykorzystywane są dwa połączenia: *połączenie sterujące* i *połączenie dla danych*. Połączenie sterujące używane jest do wysyłania komend od klienta do serwera i otrzymywania odpowiedzi na te komendy. Klient będzie wprowadzał komendy FTP, które są wysyłane do serwera FTP. Połączenie dla danych wykorzystywane jest do przesyłania plików. Zarówno klient, jak i serwer łączą się z systemem plików OS/400. Aby przesłać pliki, potrzebny jest zazwyczaj w obu systemach identyfikator użytkownika. Niżej wymienione zostały pozostałe wymagania:

- serwer iSeries z systemem OS/400,
- narzędzie TCP/IP Connectivity Utilities (5722-TC1),
- skonfigurowany serwer FTP,
- 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 wykonać proste przesyłanie pliku, zakończ każde z poniższych zadań:

1. Uruchom sesję klienta FTP.
W tym scenariuszu: w interfejsie znakowym iSeries wpisz STRTCPFTP i naciśnij klawisz **Enter**.
2. Podaj nazwę zdalnego systemu, do którego chcesz wysłać plik.
W tym scenariuszu: ichfirma.com
3. Podaj zdalnemu systemowi swoją nazwę użytkownika dla tego serwera.
W tym scenariuszu:
Wpisz identyfikator logowania (twój_identyfikator):
====>twój_identyfikator
4. Podaj zdalnemu systemowi swoje hasło dla tego serwera.
W tym scenariuszu:
Wpisz hasło:
====>twoje_hasło
5. Odszukaj katalog na serwerze IchFirmy, z którego chcesz przesłać plik.
W tym scenariuszu: ====>cd /qibm/userdata/os400/dirserv/usrtools/windows
6. Przejdź do katalogu na lokalnym serwerze, do którego chcesz przesłać plik.
W tym scenariuszu: ====>lcd /qibm/userdata/os400/dirserv/usrtools/windows
7. Określ typ 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.
W tym scenariuszu: ====> get przyklad.jar
9. Po zakończeniu Wyjdź z FTP.
W tym scenariuszu: ====> QUIT

Następny krok

Można pójść jeden krok dalej. Pliki można przesyłać także w sposób automatyczny za pomocą FTP jako

zadania wsadowego.



Scenariusz: Ochrona FTP za pomocą warstwy SSL



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 poprzez FTP. MojaFirma zawsze zapewniała prywatność i ochronę danych rozprawdzanych do jej klientów, bez względu na ich format. W tym przypadku MojaFirma musi nawiązać z IchFirmą sesje FTP chronione za pomocą SSL.

Cele

Cele tego scenariusza są następujące:

- utworzenie i zarządzanie lokalnym ośrodkiem certyfikacji (CA) na serwerze iSeries MojejFirmy,
- włączenie ochrony za pomocą warstwy SSL na serwerze FTP MojejFirmy,
- wyeksportowanie kopii certyfikatu lokalnego CA do pliku,
- utworzenie bazy certyfikałów *SYSTEM na serwerze IchFirmy,
- zaimportowanie certyfikatu lokalnego CA MojejFirmy do bazy certyfikatów *SYSTEM IchFirmy,
- określenie lokalnego CA MojejFirmy jako zaufanego CA dla klienta FTP IchFirmy.

Wymagania wstępne

MojaFirma

- posiada serwer iSeries z systemem OS/400 w wersji V5R1 lub późniejszej,
- na serwerze iSeries zainstalowane jest narzędzie TCP/IP Connectivity Utilities (5722-TC1) w wersji V5R1 lub późniejszej,
- na serwerze iSeries zainstalowane jest narzędzie Cryptographic Access Provider 128-bit dla iSeries (5722-AC3),
- na serwerze iSeries zainstalowany jest program IBM^R DCM (5722-SS1 opcja 34),
- na serwerze iSeries zainstalowany jest IBM HTTP Server (5722-DG1),
- korzysta z certyfikatów do ochrony dostępu do aplikacji i zasobów publicznych (szczegółowe informacje znajdują się w sekcji Scenariusz: Korzystanie z certyfikatów do ochrony dostępu do aplikacji zasobów publicznych).

IchFirma

- posiada serwer iSeries z systemem OS/400 w wersji V5R2 lub późniejszej,
- na serwerze iSeries zainstalowane jest narzędzie TCP/IP Connectivity Utilities (5722-TC1) w wersji V5R2,
- na serwerze iSeries zainstalowane jest narzędzie Cryptographic Access Provider 128-bit dla iSeries (5722-AC3),
- na serwerze iSeries zainstalowany jest program IBM DCM (5722-SS1 opcja 34),
- na serwerze iSeries zainstalowany jest IBM HTTP Server (5722-DG1),
- do nawiązywania sesji FTP korzysta z klienta FTP TCP/IP OS/400.

Szczegóły

IchFirma korzysta z klienta FTP OS/400, aby żądać chronionego przesyłania plików z serwera FTP MojejFirmy. Dodatkowe informacje na ten temat zawiera sekcja: Ochrona klienta FTP za pomocą TLS/SSL. Serwer jest uwierzytelniany.

IchFirma otrzymuje raporty finansowe z MojejFirmy poprzez sesję FTP chronioną za pomocą warstwy SSL.

Zadania konfiguracyjne

W MojejFirmie i IchFirmie należy wykonać poniższe zadania, aby chronić sesje FTP za pomocą warstwy SSL:

Zadania MojejFirmy:

1. Utworzenie i zarządzanie lokalnym ośrodkiem certyfikacji (CA) na serwerze iSeries MojejFirmy
2. Włączenie warstwy SSL dla serwera FTP MojejFirmy
3. Eksportowanie kopii certyfikatu lokalnego ośrodka certyfikacji (CA) MojejFirmy do pliku

Zadania IchFirmy:

1. Utworzenie bazy certyfikałów *SYSTEM na serwerze IchFirmy
2. Zaimportowanie certyfikatu lokalnego ośrodka certyfikacji (CA) MojejFirmy do bazy certyfikatów *SYSTEM IchFirmy
3. Określenie lokalnego ośrodka certyfikacji (CA) MojejFirmy jako zaufanego CA dla klienta FTP IchFirmy



Szczegóły dotyczące konfiguracji

Wykonaj poniższe zadania, aby chronić FTP za pomocą sesji SSL.

Krok 1: Utworzenie i zarządzanie lokalnym ośrodkiem certyfikacji (CA) na serwerze iSeries MojejFirmy

W tym scenariuszu przyjęto, że MojaFirma nie używała wcześniej programu DCM do konfigurowania certyfikatów dla serwera iSeries. W oparciu o założenia tego scenariusza, MojaFirma wybrała tworzenie i zarządzanie lokalnym ośrodkiem certyfikacji (CA), w celu wystawienia certyfikatu serwerowi FTP. Zamiast tego MojaFirma może korzystać z programu DCM do konfigurowania serwera FTP, aby posłużyć się certyfikatem publicznym dla SSL.

Jeśli podczas tworzenia lokalnego CA używany jest program DCM, użytkownik jest prowadzony przez cały proces, co daje pewność skonfigurowania wszystkich elementów niezbędnych do uaktywnienia SSL.

Za pomocą programu DCM wykonaj poniższe kroki, w celu stworzenia i zarządzania lokalnym CA na serwerze MojejFirmy:

1. Uruchom sesję DCM.
2. W ramce nawigacji programu DCM wybierz **Tworzenie ośrodka certyfikacji**, aby wyświetlić szereg formularzy. Te formularze pomagają w procesie tworzenia lokalnego CA oraz uzupełniania innych zadań niezbędnych do rozpoczęcia korzystania z certyfikatów cyfrowych dla SSL, podpisywania obiektów oraz weryfikacji podpisów.
3. Uzupełnij wszystkie wyświetlane formularze. Dla każdego zadania, które jest wymagane podczas tworzenia i zarządzania lokalnym CA na serwerze iSeries, jest oddzielny formularz. Zadania te obejmują:
 - a. Wybór, w jaki sposób ma być przechowywany klucz prywatny certyfikatu lokalnego CA. Ten krok wymagany jest jedynie w przypadku, gdy w serwerze iSeries zainstalowany jest koprocesor szyfrujący IBM 4758-023 PCI. Jeśli w systemie nie ma takiego koprocesora, program DCM automatycznie składowuje certyfikat i jego klucz prywatny w bazie certyfikatów lokalnego ośrodka certyfikacji.

- b. Udostępnienie lokalnemu CA informacji identyfikujących.
- c. Zainstalowanie certyfikatu lokalnego CA na komputerze PC lub w przeglądarce. Dzięki temu oprogramowanie PC będzie mogło rozpoznać lokalny ośrodek certyfikacji (CA) oraz certyfikaty, które on wydaje.
- d. Wybór strategii danych dla lokalnego CA.
- e. Wykorzystanie lokalnego CA do wydawania certyfikatu serwera lub klienta, którego aplikacje mogą używać do połączeń SSL. Jeśli w serwerze iSeries zainstalowany jest koprocesor szyfrujący IBM 4758-023 PCI, ten krok pozwoli wybrać, w jaki sposób ma być przechowywany klucz prywatny serwera lub certyfikat 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. Wybór aplikacji, które będą mogły używać certyfikatu serwera lub klienta w połączeniach SSL. Uwaga: Należy się upewnić, czy wybrany został identyfikator aplikacji dla serwera FTP TCP/IP OS/400 (QIBM_QTMF_FTP_SERVER).
- g. Wykorzystanie lokalnego CA do wydawania certyfikatów do podpisywania obiektów, których aplikacje mogą używać 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 zadanie zostanie przerwane w tym punkcie, to zakończy się i trzeba będzie wykonać oddzielne zadanie w celu ukończenia konfigurowania certyfikatów SSL.
- h. Wybór aplikacji, które mają ufać lokalnemu CA. Uwaga: Należy się upewnić, czy wybrany został identyfikator aplikacji dla serwera FTP TCP/IP OS/400 (QIBM_QTMF_FTP_SERVER).

Kiedy formularze dla tych zadań zostaną już wypełnione, można skonfigurować serwer FTP do korzystania z SSL.

Krok 2: Włączenie warstwy SSL dla serwera FTP MojejFirmy

Teraz gdy serwer FTP ma przypisany certyfikat, skonfiguruj serwer FTP MojejFirmy do korzystania z warstwy SSL:

1. W programie iSeries Navigator rozwiń **serwer iSeries** → **Sieci** → **Serwery** → **TCP/IP**.
2. Kliknij prawym przyciskiem **FTP**.
3. Wybierz **Właściwości**.
4. Wybierz zakładkę **Ogólne**.
5. Wybierz następującą opcję obsługiwaną przez SSL: **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. Aby to zrobić, 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 OS/400 do korzystania z SSL.

Krok 3: Eksportowanie kopii certyfikatu lokalnego ośrodka certyfikacji (CA) MojejFirmy do pliku

Moja Firma musi udostępnić IchFirmie kopię certyfikatu lokalnego CA. Aplikacja klienta IchFirmy musi być skonfigurowana tak, aby ufać certyfikatowi ośrodka certyfikacji, zanim będzie mogła uczestniczyć w sesji SSL.

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

1. Uruchom sesję DCM.
2. Kliknij **Wybierz bazę certyfikatów**.
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 CA MojejFirmy i kliknij **Eksportuj**.
8. Jak miejsce docelowe eksportu podaj **Plik** i kliknij przycisk **Kontynuuj**.
9. Podaj pełną ścieżkę oraz nazwę pliku dla eksportowanego certyfikatu lokalnego CA i kliknij przycisk **Kontynuuj**, aby wyeksportować certyfikat.
10. Kliknij przycisk **OK**, aby opuścić stronę potwierdzenia eksportu.

Od tego momentu można przysyłać te pliki do systemów końcowych iSeries, w których mają być weryfikowane podpisy utworzone za pomocą tego certyfikatu. Do przesłania tych plików można użyć poczty e-mail lub protokołu FTP, ponieważ nie muszą one być przesyłane w sesji chronionej.

Następnie IchFirma korzysta z programu DCM do zaimportowania certyfikatu lokalnego CA do bazy certyfikatów *SYSTEM i określenia lokalnego CA MojejFirmy (i certyfikatów, które on zatwierdza) jako zaufanych.

Krok 4: Tworzenie bazy certyfikatów *SYSTEM na serwerze IchFirmy

Aby uczestniczyć w sesji SSL, klient FTP OS/400 IchFirmy musi umieć rozpoznawać i akceptować certyfikat, który przedstawia serwer FTP MojejFirmy podczas ustanawiania sesji SSL. Aby uwierzytelnić certyfikat serwera, klient FTP IchFirmy musi mieć kopię certyfikatu ośrodka certyfikacji w bazie certyfikatów *SYSTEM. Baza certyfikatów *SYSTEM zawiera kopie certyfikatów większości ogólnie znanych, publicznych ośrodków certyfikacji. Jeśli jednak serwer FTP MojejFirmy korzysta z certyfikatu lokalnego CA, klient FTP IchFirmy musi otrzymać kopię tego certyfikatu i zaimportować go do bazy certyfikatów *SYSTEM.

W tym scenariuszu założono, że do tworzenia i zarządzania certyfikatami nie był wcześniej wykorzystywany program DCM. W takiej sytuacji należy najpierw w IchFirmie utworzyć bazę certyfikatów *SYSTEM, wykonując poniższe kroki:

1. Uruchom program DCM.
2. W ramce nawigacji programu DCM wybierz **Tworzenie nowej bazy certyfikatów**, a następnie ***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**.

Po wykonaniu tych czynności IchFirma może zaimportować certyfikat lokalnego CA do bazy certyfikatów i określić go jako zaufane źródło certyfikatów.

Krok 5: Importowanie certyfikatu lokalnego ośrodka certyfikacji (CA) MojejFirmy do bazy certyfikatów *SYSTEM IchFirmy

W systemie IchFirma wykonaj poniższe kroki, aby zaimportować certyfikat lokalnego CA do bazy certyfikatów *SYSTEM i określić, że jest certyfikatem zaufanym:

1. W ramce nawigacji programu DCM kliknij **Wybór ośrodka certyfikacji** i wybierz ***SYSTEM**, aby utworzyć 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 **Zarządzanie certyfikatami**, aby wyświetlić listę zadań.
4. Z listy zadań wybierz **Import certyfikatu**.
5. Jako typ certyfikatu wybierz **Ośrodek certyfikacji (CA)** i kliknij przycisk **Kontynuuj**.
6. Podaj pełną ścieżkę oraz nazwę pliku dla pliku certyfikatu CA i kliknij przycisk **Kontynuuj**. Wyświetli się komunikat albo potwierdzający, że importowanie zakończyło się pomyślnie, albo wyświetlający informację o błędzie, jeśli importowanie nie powiodło się.

Teraz IchFirma może określić, że ich klient FTP ufa certyfikatowi lokalnego CA MojejFirma, tak więc klient FTP IchFirma będzie mógł nawiązywać sesje SSL z aplikacjami serwera, które używają certyfikatu z lokalnego CA MojejFirma.

Krok 6: Określanie lokalnego ośrodka certyfikacji (CA) MojejFirma jako zaufanego ośrodka certyfikacji (CA) dla klienta FTP IchFirma

Zanim IchFirma będzie mogła korzystać z klienta FTP do nawiązywania bezpiecznych połączeń z serwerem FTP MojejFirma, musi użyć programu DCM do podania informacji, którym ośrodkiem certyfikacji klient powinien ufać. To znaczy, że IchFirma musi określić, że zaimportowany wcześniej certyfikat lokalnego CA, jest godny zaufania.

W systemie IchFirma wykonaj poniższe kroki, aby określić, że klient FTP IchFirma powinien ufać certyfikatowi lokalnego CA MojejFirma:

1. Uruchoom sesję DCM.
2. Kliknij **Wybór ośrodka certyfikacji** i wybierz *SYSTEM, aby utworzyć 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. Z listy wybierz aplikację klienta FTP TCP/IP OS/400 (QIBM_QTMF_FTP_CLIENT) i kliknij przycisk **Kontynuuj**, aby wyświetlić listę certyfikatów ośrodków certyfikacji.
8. Wybierz certyfikat lokalnego CA MojejFirma, który był wcześniej zaimportowany, i kliknij przycisk **OK**. Program DCM wyświetli komunikat potwierdzający wybór listy zaufanych certyfikatów.

Po zakończeniu tych kroków serwer FTP MojejFirma może ustanowić sesję SSL z klientem lub serwerem FTP IchFirma. Dodatkowe informacje na ten temat zawiera sekcja: Ochrona klienta FTP za pomocą TLS/SSL.

Konfigurowanie serwera FTP



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 serwera FTP do połączenia z siecią Internet trzeba zabezpieczyć dane. W tym celu należy:

- wykorzystać firewall pomiędzy serwerem iSeries a Internetem,
- jako serwer FTP wykorzystać inny niż produkcyjny serwer iSeries,
- 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,
- 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 iSeries i przeglądać je codziennie lub co tydzień w poszukiwaniu możliwych ataków,
- raz na miesiąc sprawdzać, czy dla serwera FTP są zarejestrowane prawidłowe programy obsługi wyjścia,
- zapoznać się z sekcją Ochrona serwera FTP w celu uzyskania informacji na temat zabezpieczania serwera FTP iSeries,

Wymienione poniżej sekcje zawierają opis sposobów podglądu i dostosowywania serwera FTP do własnych potrzeb:

Serwer FTP i program iSeries Navigator

Wykorzystanie programu iSeries Navigator do konfigurowania i zarządzania serwerem FTP iSeries.

Konfigurowanie serwerów FTP dla klientów FTP z interfejsem graficznym i dla narzędzi WWW

Opis konfiguracji serwera FTP w systemie iSeries do obsługi klientów FTP z interfejsem graficznym, przeglądarek WWW i narzędzi WWW.

Konfigurowanie serwera anonimowego FTP

Obsługa anonimowego FTP umożliwiającą zdalnym użytkownikom korzystanie z serwera FTP bez przypisanego identyfikatora użytkownika oraz hasła.



Serwer FTP i program iSeries Navigator

Programu iSeries Navigator można używać do pracy przy konfigurowaniu serwera FTP. Aby użyć do tego celu graficznego interfejsu użytkownika w programie iSeries Navigator, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń **serwer iSeries** —> **Sieci** —> **Serwery** —> **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 przeglądać klikając przyciski pomocy. Aby wyświetlić pomoc dla określonego pola, należy kliknąć przycisk ze znakiem zapytania, a następnie żądane pole.

Konfigurowanie serwerów FTP dla klientów FTP z interfejsem graficznym i dla narzędzi WWW



Serwer FTP iSeries obsługuje graficzne interfejsy klientów FTP, narzędzia do projektowania stron WWW i przeglądarki WWW.

Większość klientów FTP z interfejsami graficznymi używa formatu systemu UNIX^R jako formatu listingu i pliku ścieżki jako formatu nazewnictwa plików. Aby używać obsługiwanych formatów, należy wykonać następujące instrukcje konfigurowania właściwości serwera FTP:

1. W programie iSeries Navigator rozwiń **serwer iSeries** → **Sieci** → **Serwery** → **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:

Ustawieniami LISTFMT i NAMEFMT, dla określonych sesji FTP, można sterować 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 komendy 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.

Warto także zapoznać się z następującymi sekcjami:

- Wyświetlanie (LIST) informacji w formacie systemu iSeries
- Wyświetlanie (LIST) informacji w formacie systemu UNIX



Konfigurowanie serwera anonimowego FTP

Anonimowy FTP umożliwia niezabezpieczony dostęp (bez hasła) do wybranych informacji w systemie zdalnym. Ośrodek zdalny określa, jakie informacje mają być ogólnodostępne. Informacje te są traktowane jako publicznie dostępne i mogą być czytane przez każdego. 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 oraz ograniczony zakres działań, które może wykonywać. Najczęściej dozwolone są tylko:

- 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 systemu serwera FTP. Niektóre systemy udostępniają katalog wejściowy do wysłania danych dla użytkowników anonimowych. Tradycyjnie, specjalne konto użytkownika anonimowego akceptuje ciąg znaków jako hasło, mimo że 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 z hasłem "guest" (gość). Podawanie adresu poczty elektronicznej jest uprzywileżowaniem wyświadczanym operatorom serwisów archiwalnych, która umożliwia im zorientowanie się, kto korzysta z ich serwisów.

Anonimowy FTP w serwerze iSeries

Podstawowy serwer FTP nie obsługuje anonimowego logowania do FTP. Aby skonfigurować anonimowy FTP w serwerze iSeries, należy udostępnić programy obsługi wyjścia dla dwóch punktów wyjścia serwera FTP (punktu wyjścia logowania serwera i punktu wyjścia potwierdzenia żądania).

Anonimowy FTP jest wygodną i często potrzebną usługą. Jednak wykorzystanie anonimowego FTP zwiększa problemy związane z ochroną systemu dla serwera iSeries. Więcej informacji o zabezpieczeniu systemu zawiera sekcja Zarządzanie dostępem za pomocą programów obsługi wyjścia FTP.

Aby skonfigurować anonimowy FTP, wykonaj poniższe kroki:

1. Przygotowanie serwera anonimowego FTP

Zapoznaj się z wymaganiami technicznymi i określ strategię ochrony.

2. Pisanie programów obsługi wyjścia dla anonimowego użytkownika FTP

Napisz dwa programy obsługi wyjścia obsługujące anonimowy FTP. Sekcja ta zawiera wiele przykładów programów obsługi wyjścia wraz ze wskazówkami.

3. Tworzenie w systemie OS/400 profilu użytkownika ANONYMOUS

Zapobiegij wpisywaniu się do serwera iSeries *bezpośrednio* za pomocą identyfikatora użytkownika ANONYMOUS.

4. Tworzenie publicznej biblioteki lub katalogu

Utwórz, załaduj i skonfiguruj publiczne biblioteki oraz katalogi.

5. Instalowanie i rejestrowanie programów obsługi wyjścia

Utwórz biblioteki zawierające programy obsługi wyjścia i ich protokoły, skompiluj i zarejestruj te programy jako programy do używania przez serwer FTP.

Przygotowanie serwera anonimowego FTP

Podczas przygotowywania serwera anonimowego FTP należy rozważyć następujące informacje.

Wymagane umiejętności

Aby skonfigurować serwer anonimowego FTP, potrzebne są następujące umiejętności:

- znajomość interfejsu znakowego systemu iSeries oraz wprowadzania komend z wieloma parametrami i słowami kluczowymi,
- umiejętność tworzenia bibliotek, podzbiorów i źródłowych zbiorów fizycznych w systemie iSeries (niezbędne jest posiadanie uprawnień na poziomie przynajmniej *SECOFR),
- umiejętność przypisywania uprawnień do bibliotek, zbiorów, podzbiorów i programów,
- umiejętność pisania, edytowania, kompilowania i testowania programów na serwerze iSeries.

Bezpieczeństwo w sieci

Pierwszym krokiem podczas implementacji serwera anonimowego FTP jest zdefiniowanie jego strategii. Ten plan definiuje ochronę serwera FTP i określa sposób kodowania programów obsługi wyjścia. Ponieważ serwer FTP będzie zezwalał na dostęp wszystkich użytkowników z zewnątrz do danych na nim przechowywanych, należy dokładnie rozważyć, jak będzie on wykorzystywany i jakie dane muszą być chronione.

W celu ustalenia planu strategii serwera FTP, należy:

- wykorzystać firewall pomiędzy serwerem iSeries a Internetem,
- jako serwer FTP wykorzystać inny niż produkcyjny serwer iSeries,
- 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 na dostęp żadnym innym użytkownikom 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 iSeries,

- 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.

Następny krok:

Pisanie programów obsługi wyjścia dla anonimowego użytkownika FTP.

Pisanie programów obsługi wyjścia dla anonimowego użytkownika FTP



Aby móc obsługiwać anonimowego użytkownika FTP, należy zapisać dwa programy obsługi wyjścia: program obsługi wyjścia logowania do serwera FTP i program obsługi wyjścia potwierdzenia żądania serwera 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. Więcej informacji na temat programów obsługi punktu wyjścia FTP znajduje się w sekcji Programy obsługi wyjścia FTP. Dla anonimowego użytkownika FTP wykorzystywane są następujące punkty wyjścia:

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

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

Poniżej udostępniono przykładowe programy ułatwiające konfigurację anonimowego FTP na serwerze. Przykłady te mogą posłużyć jako punkt wyjścia do pisania własnych programów. Kopiując części kodu z przykładów można je dodać do tworzonych programów. Zaleca się uruchamianie programów przykładowych na serwerze 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 jednak używać jako podstawy do tworzenia własnego kodu lub wykorzystywać ich części przy pisaniu własnych programów.

Aby zapoznać się z przykładowymi programami, należy przejść do sekcji Punkt wyjścia logowania do serwera i Punkt wyjścia potwierdzenia żądania: klient i serwer.

Następny krok:

Tworzenie w systemie OS/400 profilu użytkownika ANONYMOUS



Tworzenie w systemie OS/400 profilu użytkownika ANONYMOUS

Aby uniemożliwić osobom niepowołanym wpisywanie się do serwera iSeries za pomocą profilu ANONYMOUS, zalecane jest utworzenie profilu użytkownika ANONYMOUS i przypisanie mu hasła *NONE. Profil użytkownika można utworzyć za pomocą programu iSeries Navigator.

1. W programie **iSeries Navigator** rozwiń **Użytkownicy i grupy**.
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 biżącą oraz Katalog osobisty, z których użytkownik Anonymous powinien korzystać.
6. Kliknij przycisk **OK** i dokończ inne ustawienia.
7. Kliknij przycisk **Dodaj**, aby utworzyć profil.

Następny krok:

Tworzenie publicznej biblioteki lub katalogu

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 ograniczenie dostępu tych użytkowników do pojedynczej biblioteki lub 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.

Następny krok:

Instalowanie i rejestrowanie programów obsługi wyjścia

Instalowanie i rejestrowanie programów obsługi wyjścia

Instalowanie programu obsługi wyjścia

1. Utwórz bibliotekę zawierającą programy obsługi wyjścia i ich protokoły.
2. Skompiluj program obsługi wyjścia w tej bibliotece.
3. Nadaj bibliotece, programom i zbiorom uprawnienia PUBLIC *EXCLUDE.
Serwer aplikacji FTP zaadaptuje uprawnienia, jeśli będzie to konieczne, do określenia i wywołania programu obsługi wyjścia.

Rejestrowanie programu obsługi wyjścia

1. W znakowym interfejsie systemu iSeries wpisz **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. Wpisz **8** w polu Opc na lewo od pozycji punktu wyjścia i naciśnij klawisz **Enter**.
4. Na ekranie Praca z programami obsługi wyjścia (Work with Exit Programs) wpisz **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.

Temat pokrewny: Usuwanie programu obsługi wyjścia

Ochrona serwera FTP

Jeśli system iSeries jest używany jako Internetowy serwer FTP, jest on dostępny na całym świecie. Dlatego niezbędne jest poświęcenie uwagi ochronie FTP, aby mieć pewność, że przechowywane na serwerze iSeries istotne dane związane z działalnością firmy nie będą narażone na szwank. Można także podjąć odpowiednie kroki zmierzające do ochrony klienta FTP.

Informacje o sposobach zabezpieczania serwera i klienta FTP znajdują się w następujących sekcjach:

Zapobieganie dostępowi do serwera FTP

Jeśli protokół FTP nie jest wykorzystywany, należy zapobiec jego uruchomieniu, aby mieć pewność, że nikt nie dostanie się do serwera iSeries poprzez port FTP. Ta sekcja wyjaśnia, w jaki sposób zablokować port FTP.

Kontrolowanie dostępu do 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.

Korzystanie z warstwy SSL do ochrony serwera FTP

Obsługa sesji SSL przez serwer FTP OS/400 podczas komunikacji z klientem obsługującym sesję SSL pozwala wyeliminować ryzyko związane z przesyłaniem przez sieć haseł i danych w postaci niezasyfrowanej.

Zarządzanie dostępem za pomocą programów obsługi wyjścia FTP

Sekcja ta opisuje, w jaki sposób wykorzystać punkty wyjścia FTP do ochrony serwera iSeries.

Zarządzanie dostępem za pomocą programu iSeries Navigator

Do ochrony serwera lub klienta FTP iSeries można wykorzystać opcję ograniczonego dostępu do administrowania aplikacjami w programie iSeries Navigator.

Monitorowanie przyłączających się użytkowników FTP

Sposoby monitorowania osób logujących się do serwera FTP.

Zapobieganie dostępowi do serwera FTP



Jeśli dostęp do serwera iSeries poprzez FTP ma być niemożliwy, należy zapobiec uruchamianiu serwera FTP. Aby zapobiec dostępowi do serwera iSeries przez FTP, wykonaj poniższe kroki:

Zapobieganie automatycznemu uruchamianiu serwera FTP

Aby zapobiec automatycznemu uruchamianiu zadań serwera FTP podczas uruchamiania TCP/IP, wykonaj następujące kroki:

1. W programie iSeries Navigator rozwiń **serwer iSeries** → **Sieci** → **Serwery** → **TCP/IP**.
2. Kliknij prawym przyciskiem **FTP** i wybierz **Właściwości**.


3. Anuluj wybór **Uruchom wraz z TCP/IP**.

Zapobieganie dostępowi do portów FTP

Aby zapobiec uruchamianiu FTP oraz dołączaniu aplikacji użytkowników, takich jak aplikacje używające gniazd, do gniazd, których zwykle używa serwer iSeries dla FTP, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń **serwer iSeries** → **Sieci** → **Serwery** → **TCP/IP**.
2. Kliknij prawym przyciskiem **Konfiguracja TCP/IP** i wybierz **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 **Dodaj ograniczenia dla portów** podaj następujące informacje:
 - **Nazwa użytkownika:** Podaj nazwę profilu użytkownika, który jest chroniony na serwerze iSeries. (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**.
9. Ograniczenia dla portów zadziałają przy następnym uruchomieniu protokołu TCP/IP. Jeśli podczas ustawiania ograniczeń dla portów potokół TCP/IP był aktywny, należy zakończyć jego działanie, a następnie uruchomić go ponownie.

Uwagi:

- Ograniczenia dla portów zadziałają przy następnym uruchomieniu protokołu TCP/IP. Jeśli podczas ustawiania ograniczeń dla portów potokół TCP/IP był aktywny, należy zakończyć jego działanie, a następnie uruchomić go ponownie.
- Pod adresem WWW <http://www.iana.org>
 organizacji Internet Assigned Numbers Authority (IANA) znajdują się informacje na temat przypisanych numerów portów.
- Jeśli porty 20 lub 21 są zarezerwowane 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 istnieje potrzeba zezwolenia klientom FTP na dostęp do systemu klientów FTP, 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. Programu obsługi wyjścia potwierdzenia żądania serwera FTP można użyć do kontroli nad tym, które operacje są dozwolone. Na przykład można odrzucać żądania komendy GET dla określonych plików bazy danych.
- Punktu wyjścia logowania do serwera można używać do uwierzytelniania użytkowników, którzy logują się na serwerze FTP. W sekcji Konfigurowanie serwera anonimowego FTP opisano, w jaki sposób używać programów obsługi wyjścia, do 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 używana jest ochrona 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, w jaki sposób współpracują ze sobą parametr INACTTIMO i licznik czasu połączeń (dla uruchomień serwera), należy przeczytać dokumentację lub pomoc elektroniczną.

Uwaga: Wartość systemowa QINACTITV nie dotyczy sesji FTP.

- Podczas korzystania z obsługi FTP jako zadania wsadowego program musi wysyłać 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 są potencjalną słabą stroną ochrony. Jeśli korzysta się z FTP jako zadania wsadowego, należy upewnić się, że do zabezpieczenia informacji o identyfikatorze użytkownika i hasle 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.
- Serwer FTP udostępnia możliwość korzystania ze zdalnych komend, tak jak to robią zaawansowana komunikacja program-program (APPC) oraz iSeries Access. 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 poprzez FTP, ładuje te niepożądane informacje do systemu iSeries. Następnie informuje innych o adresie FTP tego serwera. Potem uzyskują oni dostęp do systemu iSeries za pomocą FTP i pobierają te informacje.

Programów obsługi wyjścia serwera FTP można używać do obrony przed tego typu atakiem. Na przykład można skierować wszystkie żądania przesłania informacji do katalogu, który jest tylko do odczytu. Niweczy to cel hakerów, ponieważ jego koledzy nie będą mogli pobrać informacji z katalogu. Podręcznik AS/400^R Internet Security: Protecting Your AS/400 from HARM on the Internet



zawiera więcej informacji na temat ryzyka, jakim jest zezwolenie na przesyłanie przez serwer FTP, i możliwości jego uniknięcia.



Korzystanie z warstwy SSL do ochrony serwera FTP



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 obejmujące uwierzytelnianie klienta oraz automatyczne wpisywanie się (dodatkowe informacje na temat protokołów TLS i SSL zawiera sekcja Uwagi na temat SSL).

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 przyjmuje połączenia SSL. Serwer FTP iSeries udostępnia obie opcje.

Zanim będzie można skonfigurować serwer FTP do korzystania z SSL, należy najpierw w systemie iSeries zainstalować wstępnie wymagane programy i skonfigurować certyfikaty cyfrowe.

Aby skonfigurować warstwę SSL w celu ochrony serwera FTP, należy wykonać poniższe zadania:

1. utworzyć lokalny ośrodek certyfikacji lub skorzystać z programu DCM, aby skonfigurować serwer FTP do korzystania z certyfikatu publicznego dla SSL,
2. powiązać certyfikat z serwerem FTP,
3. ustanowić uwierzytelnianie klienta przez serwer FTP (opcja),
4. włączyć ochronę za pomocą SSL na serwerze FTP.

Powiązane z tym tematem informacje znajdują się w sekcji Ochrona klienta FTP za pomocą TLS/SSL.



Tworzenie lokalnego ośrodka certyfikacji



Do tworzenia i zarządzania lokalnym ośrodkiem certyfikacji (CA) na serwerze iSeries można użyć programu IBM DCM. Lokalny CA umożliwia tworzenie prywatnych certyfikatów dla aplikacji uruchamianych na serwerze iSeries.

Aby za pomocą programu DCM utworzyć i zarządzać lokalnym CA, wykonaj poniższe kroki:

1. Uruchom sesję DCM.
2. W ramce nawigacji programu DCM wybierz **Tworzenie ośrodka certyfikacji**, aby wyświetlić szereg formularzy. Te formularze pomagają w procesie tworzenia lokalnego CA oraz uzupełniania innych zadań niezbędnych do rozpoczęcia korzystania z certyfikatów cyfrowych dla SSL, podpisywania obiektów oraz weryfikacji podpisów.
3. Uzupełnij wszystkie wyświetlane formularze. Dla każdego zadania, które jest wymagane podczas tworzenia i zarządzania lokalnym CA na serwerze iSeries, jest oddzielny formularz. Uzupełnienie tych formularzy umożliwi:
 - a. Wybór, w jaki sposób ma być przechowywany klucz prywatny certyfikatu lokalnego CA. Ten krok wymagany jest jedynie w przypadku, gdy w serwerze iSeries zainstalowany jest koprocesor szyfrujący IBM 4758-023 PCI. Jeśli w systemie nie ma takiego koprocesora, program DCM automatycznie składowe certyfikat i jego klucz prywatny w bazie certyfikatów lokalnego ośrodka certyfikacji.
 - b. Udostępnienie lokalnemu CA informacji identyfikujących.
 - c. Zainstalowanie certyfikatu lokalnego CA na komputerze PC lub w przeglądarce. Umożliwi to rozpoznawanie przez oprogramowanie lokalnego CA oraz zatwierdzonych certyfikatów, które on wydaje.
 - d. Wybór strategii danych dla lokalnego CA.
 - e. Wykorzystanie lokalnego CA do wydawania certyfikatu serwera lub klienta, którego aplikacje mogą używać do połączeń SSL. Jeśli w serwerze iSeries zainstalowany jest koprocesor szyfrujący IBM 4758-023 PCI, ten krok pozwoli wybrać, w jaki sposób ma być przechowywany klucz prywatny serwera lub certyfikat 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. Wybrać aplikacje, które będą mogły używać certyfikatu serwera lub klienta w połączeniach SSL. Uwaga: Należy się upewnić, czy wybrany został identyfikator aplikacji dla serwera FTP OS/400 (QIBM_QTMF_FTP_SERVER).
 - g. Wykorzystanie lokalnego CA do wydawania certyfikatów do podpisywania obiektów, których aplikacje mogą używać 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 zadanie zostanie przerwane w tym punkcie, to zakończy się i trzeba będzie wykonać oddzielne zadanie w celu zakończenia konfigurowania certyfikatów SSL.
 - h. Wybór aplikacji, które mają ufać lokalnemu CA. Uwaga: Należy się upewnić, czy wybrany został identyfikator aplikacji dla serwera FTP OS/400 (QIBM_QTMF_FTP_SERVER).

Więcej informacji na temat certyfikatów zawierają poniższe sekcje:

Zarządzanie certyfikatami użytkowników

Sekcja zawiera informacje, w jaki sposób użytkownicy mogą skorzystać z programu DCM do uzyskania certyfikatów lub powiązania istniejących certyfikatów z ich profilami użytkowników iSeries.

Korzystanie z funkcji API do programowego wystawiania certyfikatów dla użytkowników systemów innych niż iSeries

Sekcja zawiera informacje, w jaki sposób można wykorzystać lokalny CA do wystawiania prywatnych certyfikatów użytkownikom, bez przypisywania certyfikatu profilowi użytkownika iSeries.

Otrzymywanie kopii certyfikatu prywatnego CA

Sekcja zawiera informacje, w jaki sposób otrzymać kopię certyfikatu prywatnego CA i zainstalować ją na komputerze PC, tak żeby można było uwierzytelniać jakiegokolwiek certyfikaty serwera wystawiane przez CA.

Następny krok:

Wiązanie certyfikatów z serwerem FTP



Wiązanie certyfikatów z serwerem FTP



To zadanie należy wykonać, jeśli podczas tworzenia lokalnego ośrodka certyfikacji (CA) nie przypisano aplikacji serwera FTP certyfikatu jeśli lub system został skonfigurowany tak, aby żądał certyfikatu z publicznego ośrodka certyfikacji.

1. Uruchom program DCM. Jeśli chcesz uzyskać lub utworzyć certyfikaty, skonfigurować lub zmienić system certyfikatów, zrób to teraz. Informacje na temat konfigurowania systemu certyfikatów zawiera sekcja Korzystanie z programu DCM.
2. Kliknij przycisk **Wybierz bazę certyfikatów**.
3. Wybierz ***SYSTEM**. Kliknij przycisk **Kontynuuj**.
4. Wpisz odpowiednie hasło dla bazy certyfikatów ***SYSTEM**. Kliknij przycisk **Kontynuuj**.
5. Po odświeżeniu menu nawigacji po lewej stronie, rozwiń pozycję **Zarządzanie aplikacjami**.
6. Kliknij **Aktualizuj przypisanie certyfikatów**.
7. Na następnym ekranie wybierz aplikację **Serwer**. Kliknij przycisk **Kontynuuj**.
8. Wybierz pozycję **Serwer FTP TCP/IP OS/400**.
9. Kliknij **Aktualizuj przypisanie certyfikatów**, aby przypisać certyfikat do serwera FTP TCP/IP OS/400.
10. Z listy wybierz certyfikat, aby przypisać go do serwera.
11. Kliknij **Przypisz nowy certyfikat**.
12. Program DCM przejdzie do strony **Aktualizuj przypisanie certyfikatów**, pokazując komunikat potwierdzający. Kiedy zakończysz konfigurację certyfikatów dla serwera FTP, kliknij przycisk **Gotowe**.

Następny krok:

Żądanie uwierzytelniania klienta serwera FTP (opcja)
lub
Włączanie ochrony za pomocą SSL w serwerze FTP



Żądanie uwierzytelniania klienta dla serwera FTP (opcja)



Jeśli serwer FTP ma uwierzytelniać klientów, można zmienić opisy aplikacji w programie IBM Menedżer certyfikatów cyfrowych.

Uwaga: Serwer FTP obsługuje opcję uwierzytelniania klienta, ale klient FTP OS/400 jej nie obsługuje. Niektórzy użytkownicy nadal mogą żądać uwierzytelniania klienta, jednak uniemożliwi to korzystanie z klienta FTP OS/400 dla połączeń SSL.

Jeśli klient FTP nawiązuje połączenie, a opcja uwierzytelniania klienta jest na serwerze wyłączona, musi on wysłać komendę USER. Kiedy już informacje komendy USER zostaną wysłane, serwer FTP sprawdzi, czy użytkownik jest zgodny z profilem powiązany z certyfikatem klienta, który użytkownik wysłał do serwera jako część uzgodnienia połączenia SSL. Jeśli użytkownik i certyfikat są zgodne, nie jest potrzebne hasło, a serwer FTP loguje użytkownika do systemu. Komenda USER jest potrzebna z tego względu, że w protokole FTP nie ma mechanizmu "informującego" klienta, że jest logowany bez komendy.

1. Uruchom program DCM. Jeśli chcesz uzyskać lub utworzyć certyfikaty, skonfigurować lub zmienić system certyfikatów, zrób to teraz. Informacje na temat konfigurowania systemu certyfikatów zawiera sekcja Korzystanie z programu DCM.
2. Kliknij przycisk **Wybierz bazę certyfikatów**.
3. Wybierz ***SYSTEM**. Kliknij przycisk **Kontynuuj**.
4. Wpisz odpowiednie hasło dla 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. Wybierz pozycję **Serwer FTP TCP/IP OS/400**.
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**.

Następny krok:

Włączanie ochrony za pomocą SSL w serwerze FTP



Włączanie ochrony za pomocą SSL w serwerze FTP



Wykonaj następujące kroki, aby włączyć ochronę za pomocą SSL w serwerze FTP:

1. W programie iSeries Navigator rozwiń **serwer iSeries** → **Sieci** → **Serwery** → **TCP/IP**.
2. Kliknij prawym przyciskiem **FTP**.
3. Wybierz **Właściwości**.
4. Wybierz zakładkę **Ogólne**.
5. Wybierz jedną z następujących opcji do obsługi SSL:
 - **Tylko 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.
 - **Tylko niechronione**
Wybierz tę opcję, aby zabronić nawiązywania sesji chronionych. Próby połączenia do portu SSL nie zostaną zrealizowane.
 - **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 na serwerze iSeries są zainstalowane najnowsze poprawki PTF.



Ochrona klienta FTP za pomocą TLS/SSL



Do szyfrowania danych przesyłanych przez połączenia FTP sterujące i przeznaczone dla danych, można wykorzystać połączenia TLS/SSL. Podstawową przyczyną szyfrowania połączenia sterującego jest chęć ukrycia hasła podczas logowania do serwera FTP.

Zanim klient FTP będzie wykorzystywany do nawiązywania bezpiecznych połączeń z serwerem, należy skorzystać z programu DCM do skonfigurowania uprawnień zaufanego certyfikatu dla klienta FTP. Należy także dodać wszystkie uprawnienia certyfikatu, które zostały użyte do utworzenia certyfikatów przypisanych do serwerów, z którymi będzie nawiązywane połączenie. W zależności od używanego CA może być wymagane eksportowanie lub importowanie certyfikatów ośrodka certyfikacji. Więcej informacji na temat uprawnień zaufanego ośrodka certyfikacji znajduje się w temacie programu DCM Definiowanie listy zaufania CA dla aplikacji.

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 komend, które są wykorzystywane jako część obsługi TLS/SSL (SECOpen i SECData).

Definiowanie ochrony TLS/SSL dla klienta FTP iSeries

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 podać *IMPLICIT, aby uzyskać połączenie chronione przez wcześniej zdefiniowany numer portu serwera. (Więcej szczegółów znajduje się w sekcji poniżej: Niejawne połączenie SSL.)

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

udostępnia 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 do oczekiwania na negocjację połączenia SSL/TLS.

Metodę tę udosępniono, 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, współcześnie jednak się ich nie zaleca, a grupa IETF wręcz je odrzuca.

Uwaga:

Standardowy protokół do konfigrowania połączenia TLS/SSL wymaga, żeby podczas nawiązywania połączenia z serwerem, była użyta komenda AUTH (Autoryzacja - Authorization). Do określenia poziomu ochrony używane są komendy serwera PBSZ i PROT.

Dla niejawnych połączeń SSL komendy serwera AUTH, PBSZ i PROT **nie** są wysyłane do serwera. Zamiast tego serwer zadziała tak, jakby klient przesłał te komendy z parametrami podanymi poniżej:

- AUTH SSL
- PBSZ 0
- PROT P



Zarządzanie dostępem za pomocą programów obsługi wyjścia FTP

Protokół FTP zapewnia ochronę na poziomie obiektów systemu OS/400. Oznacza to, że zdalni użytkownicy nie mogą zalogować się do serwera FTP w systemie iSeries, jeśli nie mają prawidłowego profilu użytkownika i hasła do systemu.

Dodatkową ochronę można zapewnić dodając programy obsługi wyjścia FTP do punktów wyjścia serwera czy klienta FTP, dzięki czemu można uzyskać większe ograniczenie dostępu do systemu. Na przykład można ograniczyć możliwość logowania się poprzez FTP, jak również ograniczyć dostęp do bibliotek, obiektów i komend.

Aby ograniczyć dostęp użytkowników do komend CL i komend FTP, można napisać program obsługi wyjścia potwierdzania żądań serwera FTP. Instrukcje i przykłady na ten temat zawiera sekcja Punkt wyjścia potwierdzenia żądania: klient i serwer.

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: potwierdzenia żądania klienta. Format ten umożliwi ograniczenie użytkownikowi możliwości wykonania pewnych funkcji klienta FTP.

W zależności od sytuacji można rozważyć ograniczenie dostępu do komend FTP za pomocą ograniczonego dostępu do administracji aplikacji, jako sposobu alternatywnego do pisania programów obsługi wyjścia dla punktów wyjścia potwierdzenia żądania serwera czy klienta FTP.

Aby zapewnić poprawność działania programów obsługi wyjścia, należy zapoznać się z sekcją Instalowanie i rejestrowanie programów obsługi wyjścia. Jeśli programy obsługi wyjścia nie są już potrzebne, należy je usunąć zgodnie z instrukcjami podanymi w sekcji Usuwanie programu obsługi wyjścia, aby przerwać ich funkcjonowanie w przyszłości.

Zarządzanie dostępem za pomocą programu iSeries Navigator

Aplikacji iSeries Navigator można używać do ograniczania dostępu użytkowników do serwera FTP i do funkcji klienta FTP. Za pomocą Administracji aplikacji można przyznawać dostęp lub odmawiać dostępu do poszczególnych funkcji dla pojedynczych użytkowników lub grup użytkowników. Dostępem do funkcji FTP można także zarządzać, pisząc programy obsługi wyjścia FTP dla punktów wyjścia potwierdzania żądania FTP.

Aby za pomocą aplikacji iSeries Navigator zarządzać dostępem użytkowników do poszczególnych funkcji, wykonaj poniższe czynności:

1. W aplikacji iSeries Navigator prawym przyciskiem kliknij **serwer iSeries server**, a następnie wybierz opcję **Administracja aplikacji**.
2. Wybierz zakładkę **Aplikacje hosta**.
3. Rozwiń **Narzędzia TCP/IP dla iSeries**.
4. Rozwiń **Protokół FTP**.
5. Rozwiń **Klient FTP** lub **Serwer FTP**.
6. Wybierz funkcję, do której chcesz umożliwić lub zablokować dostęp.
7. Kliknij **Dostosuj**.
8. Za pomocą okna dialogowego **Dostosowanie dostępu** zmień listę użytkowników i grup, które mają dostęp do danej funkcji lub nie.
9. Kliknij przycisk **OK**, aby zapisać zmiany na stronie **Dostosowanie dostępu**.
10. Kliknij przycisk **OK**, aby opuścić stronę **Administracja aplikacji**.

Dostępem określonego użytkownika lub grupy do zarejestrowanych funkcji FTP można także zarządzać za pomocą narzędzia do zarządzania użytkownikami i grupami w aplikacji iSeries Navigator. W tym celu:

1. W programie iSeries Navigator rozwiń **serwer iSeries** → **Użytkownicy i grupy**.
2. Wybierz **Wszyscy użytkownicy** lub **Grupy**.
3. Prawym przyciskiem kliknij użytkownika lub grupę, a następnie wybierz **Właściwości**.
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 dla funkcji "nadrzędnej".

Więcej informacji o ochronie serwera FTP iSeries znajduje się w sekcji Ochrona serwera FTP.

Monitorowanie przyłączających się użytkowników FTP

Protokołowanie FTP i przeglądanie protokołów umożliwia monitorowanie aktywności oraz sprawdzanie, czy nie nastąpiły ataki z zewnątrz. Aby monitorować przyłączających się użytkowników FTP, wykonaj poniższe kroki:

1. W programie iSeries Navigator rozwiń **serwer** → **Sieci** → **Serwery** → **TCP/IP**.
2. W prawym panelu kliknij prawym przyciskiem myszy **FTP** i wybierz **Zadania serwera**.
3. Pojawia się panel zadania serwera FTP. Kolumna bieżących użytkowników wyświetla użytkowników zalogowanych w zadaniu serwera. Jeśli nie jest zalogowany żaden użytkownik, wyświetlany jest profil użytkownika Qtcp. Aby odświeżyć ekran, naciśnij **F5** lub wybierz **Widok** → **Odśwież**.

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

Aby uruchomić zadania serwera FTP, należy wykonać kroki opisane w sekcji Uruchamianie i zatrzymywanie serwera FTP.

Zarządzanie serwerem FTP

Serwer iSeries można skonfigurować tak, aby wysyłał, odbierał i udostępniał pliki w sieci poprzez protokół przesyłania plików (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. Użytkownik zwykle nie pracuje bezpośrednio z serwerem FTP. Poniższe sekcje zawierają informacje pomocne przy administrowaniu serwerem FTP:

- Uruchamianie i zatrzymywanie serwera FTP
- Ustawianie liczby dostępnych serwerów FTP
- Zwiększanie wydajności serwera FTP dzięki obsłudze podsystemów konfigurowalnych

Uruchamianie i zatrzymywanie serwera FTP

Serwer FTP można uruchamiać i zatrzymywać za pomocą aplikacji iSeries Navigator. Instrukcje uzyskiwania dostępu do serwera FTP znajdują się w sekcji Serwer FTP i program iSeries Navigator.

Aby uruchomić serwer FTP, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń **serwer iSeries** → **Sieci** → **Serwery** → **TCP/IP**.
2. W prawym panelu kliknij prawym przyciskiem myszy **FTP** i wybierz **Uruchom**.

Aby zatrzymać serwer FTP, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń **serwer iSeries** → **Sieci** → **Serwery** → **TCP/IP**.
2. W prawym panelu kliknij prawym przyciskiem myszy **FTP** i wybierz **Zatrzymaj**.

Ustawianie liczby dostępnych serwerów FTP



Istnieje możliwość podania minimalnej liczby dostępnych serwerów, które mają czekać w gotowości, na wypadek prób nawiązania połączeń przez klientów. 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**. Podanie wartości 1 opóźnia połączenia przychodzące do serwera FTP. Zalecaną wartością jest 3.

Kiedy klient łączy się z serwerem FTP iSeries, serwer sprawdza liczbę aktywnych serwerów, które nie są połączone z klientem oraz wartość podaną dla początkowej liczby serwerów do uruchomienia. Jeśli ta wartość jest większa od liczby dostępnych serwerów, uruchamiane są dodatkowe serwery, aż do chwili, gdy obie te liczby będą równe. Jeśli natomiast wartość początkowa jest mniejsza niż liczba dostępnych serwerów, nie jest podejmowane żadne działanie. Zmiana początkowej liczby serwerów daje efekt podczas łączenia się następnego klienta, gdy powyższy proces jest aktywowany.

Na przykład, gdy w tym samym czasie ustanowionych jest pięć połączeń klienta FTP, a początkowa liczba serwerów jest ustawiona na 10, będzie działało 15 serwerów. Liczba ta obejmuje pięć serwerów dla pięciu aktywnych sesji klientów oraz dziesięć dostępnych serwerów. Liczba dostępnych serwerów może być większa niż ich liczba początkowa. I tak jak w powyższym przykładzie, gdyby pięciu klientów zamknęło swoje sesje, a inne sesje nie zostałyby uruchomione, dostępnych byłoby 15 serwerów.



Zwiększanie wydajności serwera FTP dzięki obsłudze podsystemów konfigurowalnych

Domyślny podsystem (QSYS/QSYSWRK) jest używany do wielu zadań serwerów firmy IBM. Korzystanie z podsystemów innych niż domyślny może doprowadzić do wzrostu wydajności FTP, ponieważ eliminowana jest potrzeba współużytkowania zasobów.

Aby skonfigurować podsystem dla serwera FTP, wykonaj następujące kroki:

1. W programie iSeries Navigator rozwiń **serwer iSeries** → **Sieci** → **Serwery** → **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. Zadanie uruchamiania serwera podczas wykonywania określi parametry nowo utworzonego podsystemu i wprowadzi zadania serwera do uruchamiania wsadowego w tym podsystemie.

Używanie klienta FTP w systemie iSeries

Klient FTP umożliwia przesyłanie plików znalezionych w serwerze iSeries, a także w systemach plików Root, QSYS.Lib, QOpenSys, QOPT i QFileSvr.400. Pozwala również na przesyłanie folderów i dokumentów w systemie plików usługi 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 kończenie sesji klienta

Opis sposobu uruchamiania i zakańczania sesji klienta.

Uwagi na temat przekroczenia limitu czasu przez serwer

Opis sposobu zapobiegania utracie połączenia po przekroczeniu limitu czasu.

Przesyłanie plików za pomocą FTP

Opis sposobu przesyłania i odbierania plików za pomocą protokołu FTP.

FTP jako zadanie wsadowe

Przedstawienie przykładów uruchamiania FTP w trybie nienadzorowanym.

Uruchamianie i kończenie sesji klienta

Sekcja ta zawiera szczegóły dotyczące używania klienta FTP na serwerze iSeries.

Uruchamianie sesji klienta FTP

Kończenie sesji klienta FTP

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 Uruchomienie protokołu przesyłania plików TCP/IP (Start TCP/IP File Transfer Protocol - STRTCPFTP "zdalny_system") uruchamia sesję klienta w lokalnym serwerze iSeries, a następnie otwiera połączenie z serwerem FTP w podanym systemie zdalnym. Na przykład wprowadzenie komendy FTP mojserwer.com uruchomi sesję klienta na serwerze iSeries, a następnie otworzy połączenie z serwerem FTP w zdalnym systemie mojserwer.com. Dzięki wpisaniu komendy STRTCPFTP, bez określania zdalnego systemu, można podać dodatkowe parametry lub być o nie zapytany.

```

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

Wypełnij pola i naciśnij 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:

System zdalny (RMTSYS)

Nazwa zdalnego systemu, do lub z którego mają być przesyłane pliki. Możliwymi wartościami są:

***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 (Coded character set identifier - 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. Ale w niektórych sytuacjach serwer FTP może łączyć się za pomocą portu innego niż 21. W takich sytuacjach parametr port może być używany 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, gdy podana jest opcja *SECURE.



Połączenie chronione (SECNN)

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, używanymi szyfrowania do ochrony danych przed przeglądaniem podczas przesyłania i weryfikującymi, czy nie nastąpiła utrata lub zniekształcenie danych.

Uwaga:

Komenda klienta FTP SECOPEN może być wykorzystana do otwarcia 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 nie obsługuje niejawniej ochrony TLS/SSL, określonego portu lub negocjacja ochrony TLS/SSL nie powiodła się z jakiegokolwiek powodu, połączenie jest zamykane.

***SSL**

Po połączeniu z określonym serwerem FTP, klient FTP wysyła komendę AUTH (Autoryzacja - Authorization), która żąda ochrony TLS/SSL danej sesji. Jeśli serwer obsługuje ochronę TLS/SSL, wykonywana jest negocjacja TLS/SSL. Jeśli serwer nie obsługuje ochrony TLS/SSL lub negocjacja nie powiodła się, połączenie jest zamykane.

***NONE**

Klient FTP nie korzysta z szyfrowania dla połączenia sterującego z określonym serwerem FTP.



Ochrona danych (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 SECDData 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. Możliwymi wartościami są:

***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.

Kroki pozwalające na przeprowadzenie przesyłania plików pomiędzy systemami, zostały opisane w sekcji Przesyłanie plików za pomocą FTP.

Kończenie sesji klienta FTP

Sesja FTP kończy się po wprowadzeniu komendy QUIT. Zamyka ona połączenie ze zdalnym hostem i kończy sesję FTP na serwerze iSeries. W tym celu można także nacisnąć klawisz F3 (Wyjście), a następnie potwierdzić zamiar zakończenia sesji FTP.

Uwagi na temat przekroczenia limitu czasu przez serwer

Wartość limitu czasu bezczynności wymaga krótkiego omówienia. Jest to czas liczony w sekundach, po którym serwer zamyka sesję, jeśli serwer FTP nie jest aktywny. Niektóre systemy zdalne pozwalają klientom na zmianę tej wartości. Na przykład serwer iSeries obsługuje komendę TIME serwera FTP, która może być wysłana do niego za pomocą komendy klienta FTP QUOTE, jak to zostało opisane w sekcji QUOTE (Wysłanie komendy do serwera FTP - Send a Subcommand to an FTP Server). Serwery UNIX często obsługują komendę SITE IDLE.

Podczas stosowania lokalnej komendy systemu iSeries z komendą SYSCMD lub przyciskiem F21 nie dochodzi do żadnej interakcji pomiędzy klientem a serwerem. Dlatego, jeśli uruchamianie tych lokalnych komend systemu iSeries przekracza limit czasu bezczynności serwera, połączenie zostanie zamknięte. Jeśli połączenie zostanie utracone, trzeba ponownie zalogować się do serwera za pomocą komendy OPEN (OPEN <nazwa zdalnego systemu>) i komendy USER, jak zostało to opisane w uwagach do sekcji Logowanie do zdalnego systemu (Serwera).



Przesyłanie plików za pomocą FTP

Aby przesłać pliki za pomocą protokołu FTP, wykonaj następujące kroki:

1. Zbierz 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 wpisz nazwę TCP/IP lub adres IP zdalnego systemu i naciśnij klawisz **Enter**. Możesz użyć nazwy lub adresu IP, takich jak:
remote.systemname.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 w celu zabezpieczenia haseł i danych ma być stosowane połączenie chronione, jako wartość parametru Port podaj *SECURE.



6. Naciśnij klawisz **Enter**, aby nawiązać połączenie. Klient FTP wyświetli komunikaty, które powiadomią o pomyślnym nawiązaniu połączenia z systemem zdalnym.



Uwaga:

Jeśli dla portu podano parametr *SECURE, a serwer nie obsługuje niejawniej ochrony TLS/SSL określonego portu lub negocjacja ochrony TLS/SSL nie powiodła się z jakiegokolwiek powodu, połączenie jest zamykane.



7. Aby zmienić typ przesyłanego pliku:
 - a. Aby zmienić typ na EBCDIC, wpisz **EBCDIC** i naciśnij klawisz **Enter**, zanim prześlesz plik.
 - b. Aby zmienić typ na BINARY, wpisz **BINARY** i naciśnij klawisz **Enter**, zanim prześlesz plik.
 - c. Aby powrócić do domyślnego typu ASCII, wpisz **ASCII** i naciśnij klawisz **Enter**, zanim prześlesz plik.
8. Od tego momentu można już przysyłać 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, wpisz komendę **GET** z nazwą pliku:
GET mojplik.txt
 - Aby przesłać plik znajdujący się na systemie klienta do systemu serwera, wpisz **PUT** z nazwą pliku:
PUT mojplik.txt

9. Aby zakończyć sesję klienta FTP i powrócić do wiersza komend iSeries, wpisz komendę **QUIT**.

Klient FTP jako zadanie wsadowe

Klient FTP może być uruchamiany interaktywnie lub w trybie nienadzorowanym. Ta sekcja przedstawia dwa przykłady metod uruchamiania klienta FTP: przykład prosty i przykład złożony. Jeszcze inny przykład znajduje się także w Sekcji 6.7 Batch FTP w podręczniku V4 TCP/IP for AS/400: More Cool Things Than Ever



(około 744 strony).

Klient FTP jako zadanie wsadowe: przykład prosty

Poniżej podano prosty przykład przesyłania danych za pomocą pliku wsadowego. Przykład ten umożliwia przesłanie zawartości 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 ILE CL, 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
*****
```



```

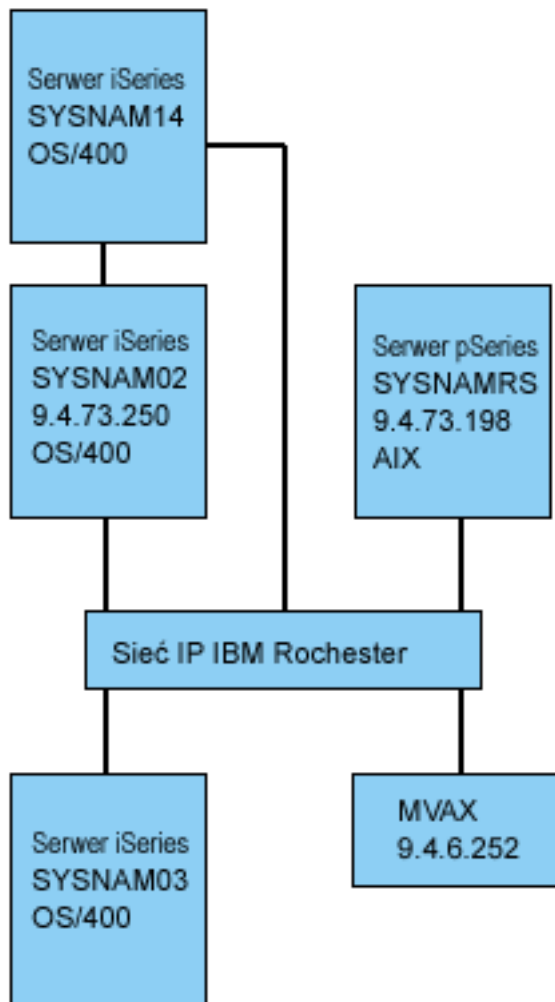
Connecting to host name SYSxxx
at address x.xxx.xx.xxx using port 21.
220-QTCP at SYSxxx.sysnam123.ibm.com.
220 Connection will close if idle more than 5 minutes.
Enter login ID (itso):
> ITSO ITSO
331 Enter password.
230 ITSO logged on.
  OS/400 is the remote operating system. The TCP/IP version is "V3R1M0".
250 Now using naming format "0".
257 "QGPL" is current library.
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.

Klient FTP jako zadanie wsadowe: przykład złożony

Poniższy przykład przedstawia sposób pobrania w trybie wsadowym plików z kilku zdalnych hostów do głównego serwera iSeries.



*

Użytkownik GWIL w serwerze iSeries SYSNAM03 chce:

1. Pobrać pliki z hostów SYSNAMRS (RS/6000^R) i MVAX (VAX).
2. Po pobraniu pliku z hosta SYSNAMRS, przesłać plik do hosta SYSNAM02 (kolejnego serwera iSeries) za pomocą protokołu FTP.
3. Wysłać plik do serwera iSeries SYSNAM14 poprzez TCP/IP.

Tworzenie programu CL do uruchomienia FTP

1. Jak można było to zobaczyć w powyższym przykładzie, FTP pobiera komendy oraz wysyła komunikaty do terminalu, dlatego zarówno wejście, jak i wyjście muszą zostać nadpisane, aby można było je wykorzystać w trybie wsadowym. Komenda OVRDBF jest wykorzystywana do nadpisania starych wartości nowymi, które mają zostać użyte w zadaniu wsadowym:


```
OVRDBF FILE(INPUT) TOFILE(GERRYLIB/QCLSRC) MBR(FTPCMDS)
OVRDBF FILE(OUTPUT) TOFILE(GERRYLIB/QCLSRC) MBR(FTPLOG)
```
2. Komenda STRTCPFTP wymaga podania jako parametru nazwy hosta lub adresu internetowego w pliku z programem CL. Jeśli system zdalny ma zostać podany w wejściowym pliku komend, a nie w pliku z programem CL, w komendzie STRTCPFTP należy podać nazwę fikcyjnego hosta, aby zachować poprawną składnię komendy. Nazwa fikcyjna może być nazwą wymyślanego hosta lub nazwą rzeczywistego 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 wymaganego hosta, nie są wymagane pozycje jak wyżej, aby nawiązać połączenie z wybranym systemem serwera, tylko jako pierwszą pozycję należy podać komendę OPEN.

```
FTP RMTSYS(LOOPBACK)
```

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

- Po zakończeniu aplikacji FTP należy usunąć nadpisanie:

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

W systemie SYSNAM01 program CL dla klienta FTP jako zadania wsadowego może być taki, jak przykładowy program pokazany poniżej:

```

                                Przeglądanie
Kolumny . . . : 1 71          (Browse)          GERRYLIB/QCLSRC
SEU==>                                     FTPBATCH
FMT **  ...+... 1 ...+... 2 ...+... 3 ...+... 4 ...+... 5 ...+... 6 ...+... 7
***** Beginning of data *****
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
***** End of data *****

F3=Wyjście  F5=Odśwież  F9=Odtwórz  F10=Kursor  F12=Anuluj
F16=Powtórz znajdź    F24=Więcej klawiszy
                                (C) COPYRIGHT IBM CORP. 1981, 1994.

```

Rysunek 1. Program CL FTPBATCH dla klienta FTP jako zadania wsadowego.

Tworzenie pliku wejściowego FTP (FTCPDMS)

Plik wejściowy musi zawierać wszystkie komendy klienta FTP niezbędne do połączenia i zalogowania się do serwera, skonfigurowania i wykonania przesyłania danych plików, zamknięcia połączenia z serwerem oraz zakończenia sesji klienta. Podany niżej przykład zawiera komendy użyte do przesyłania danych plików do dwóch różnych systemów zdalnych.

```

                                Przeglądanie
Kolumny . . . : 1 71          (Browse)          GERRYLIB/QCLSRC
SEU==>                                     FTCPDMS
FMT **  ...+... 1 ...+... 2 ...+... 3 ...+... 4 ...+... 5 ...+... 6 ...+... 7
***** Beginning of data *****
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 ebclic
0016.00 put gerrylib/rs6.rs6 gerrylib/rs6.rs6
0017.00 quote rcmd sndnetf file(gerrylib/rs6) tousrid((gwil sysnam14))
0018.00 close
0019.00 quit
***** End of data *****
F3=Wyjście F5=Odśwież F9=Odtwórz F10=Kursor F12=Anuluj
F16=Powtórz znajdź F24=Więcej klawiszy

```

Rysunek 2. Przesyłanie plików do dwóch zdalnych systemów.

Poniżej przedstawiono wyjaśnienie komend klienta FTP pokazanych na Rysunku 2. Numery wierszy na ekranie odpowiadają numerom w poniższym zestawieniu.

0001

Identyfikator użytkownika i hasło dla fikcyjnego połączenia z klientem iSeries SYSNAM03.

0002

Zamknięcie fikcyjnego połączenia w serwerze iSeries SYSNAM03.

0003

Otwarcie połączenia sterującego do hosta RISC System/6000^R 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 FTP jest uruchomiony interaktywnie, klient automatycznie wywołuje komendę USER i podpowiada identyfikator do zalogowania się. Gdy FTP jest uruchomiony w trybie wsadowym, komenda USER nie jest wywoływana automatycznie.

0005

Przesyłanie danych ASCII (w serwerze iSeries zostanie wykonana konwersja do/z EBCDIC).

0006

Komenda CL uruchamiana dla klienta iSeries: usunięcie pliku. Zamiast parametru (REPLACE może być użyta w następnej komendzie).

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 iSeries.

0012

Zamknięcie połączenia sterującego z hostem VAX MVAX.

0013

Otwarcie połączenia sterującego ze zdalnym hostem iSeries SYSNAM02.

0014

Komenda USER z identyfikatorem użytkownika i hasłem dla hosta SYSNAM02.

0015

Przesyłanie danych EBCDIC (na zasadzie takiej, jak pomiędzy serwerami iSeries).

0016

Wysłanie pliku iSeries do hosta iSeries SYSNAM02 poprzez TCP/IP.

0017

Wysłanie tego pliku z serwera iSeries SYSNAM03 do zdalnego hosta iSeries SYSNAM14 poprzez TCP/IP.

0018

Zamknięcie połączenia sterującego z hostem iSeries SYSNAM02.

0019

Zakończenie aplikacji FTP.

Tworzenie programu CL do wprowadzania zadania FTPBATCH

Utworzenie programu CL, który wprowadza zadanie FTPBATCH, pozwala na ustalenie harmonogramu przesyłania danych plików oraz uruchamianie przesyłania w trybie nienadzorowanym. W poniższym przykładzie przesyłanie danych plików ma zostać uruchomione w następną piątek o godzinie 17:00, w trybie nienadzorowanym.

```

                                Przeglądanie
Kolumny . . . : 1 71          (Browse)          GERRYLIB/QCLSRC
SEU==>                                     FTPSUBMIT
FMT **  ...+... 1 ...+... 2 ...+... 3 ...+... 4 ...+... 5 ...+... 6 ...+... 7
***** Beginning of data *****
0001.00 PGM
0002.00          SBMJOB      CMD(CALL PGM(GERRYLIB/FTPBATC)) +
0003.00                                JOB(FTPFRIDAY) OUTQ(QUSRSYS/GERRYQ)  +
0004.00                                SCDDATE(*FRI) SCDTIME(170000) /* FTP for +
0005.00                                Friday, 5:00 in the afternoon */
0006.00 ENDPGM
***** End of data *****

F3=Wyjście   F5=Odśwież   F9=Odtwórz   F10=Kursor   F12=Anuluj
F16=Powtórz  F24=Więcej  F24=Więcej  klawiszy
                                (C) COPYRIGHT IBM CORP. 1981, 1994.

```

Rysunek 3. Program CL do wprowadzenia zadania wsadowego FTP.

Sprawdzanie w pliku wyjściowym FTP, czy podczas przetwarzania nie pojawiły się błędy

Podczas uruchamiania o godzinie ustalonej w harmonogramie klient FTP wpisuje dane do podzbioru zbioru FTPLOG pokazanego poniżej. Dane w podzbiorze zbioru FTPLOG odpowiadają rzeczywistym instrukcjom dla obu przykładów.

```

        Łączenie z hostem LOOPBACK pod adresem 127.0.0.1 za pomocą portu 21.
220-QTCP w hoście lokalnym.
220 Połączenie zostanie zamknięte, jeśli będzie bezczynne przez ponad 5 minut.
Wpisz identyfikator logowania (gwil):

>>>GWIL ****
331 Wpisz hasło.
230 GWIL zalogowany.
    OS/400 jest zdalnym systemem operacyjnym. Wersja TCP/IP "V4R2M0".
250 Obecnie używany format nazewnictwa "0".
257 Biblioteka bieżąca to "QGPL".
Wpisz komendę FTP.

> CLOSE
221 Otrzymanie komendy QUIT.
Wpisz komendę FTP.

> 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) gotowy.
Wpisz komendę FTP.

```

Rysunek 4. Wyjście FTP (FTPLLOG) po uruchomieniu programu FTPBATCH (część 1)

```

> USER root ****
331 Wymagane hasło dla użytkownika root.
230 Użytkownik root zalogowany.
    UNIX Typ: L8 Wersja: BSD-44
Wpisz komendę FTP.

> ASCII
200 Typ ustawiony na A; z N.
Wpisz komendę FTP.

> SYSCMD DLTf FILE(GERRYLIB/RS6)
Wpisz komendę FTP.

> GET /Itsotest GERRYLIB/RS6/RS7
200 Żądanie komendy PORT powiodło się.
150 Otwieranie połączenia danych dla /Itsotest (467 bajtów).
226 Przesyłanie zakończone.
467 bytes transferred in 2.845 seconds. Transfer rate 0.167 kB/sec.
Wpisz komendę FTP.

```

Rysunek 5. Wyjście FTP (FTPLLOG) po uruchomieniu programu FTPBATCH (część 2)

```

> CLOSE
221 Do widzenia.
Wpisz komendę FTP.

> OPEN MVAX
    Łączenie z hostem mvax pod adresem 9.4.6.252 za pomocą portu 21.
220 Usługa FTP gotowa
Wpisz komendę FTP.

```

```

> USER TESTER *****
331 Otrzymano nazwę użytkownika TESTER, proszę podać hasło
230 TESTER zalogowany, katalog $DISK1:[TESTER]
Wpisz komendę FTP.

GET SCREEN1.FILE GERRYLIB/VAX.VAX (REPLACE
200 Żądanie komendy PORT powiodło się.
125 Przesyłanie ASCII rozpoczęte dla $DISK1:[TESTER SCREEN1.FILE;1(266586 bytes)
226 Przesyłanie pliku powiodło się.
265037 bytes transferred in 8.635 seconds. Transfer rate 30.694 kB/sec.
Wpisz komendę FTP.

> CLOSE
221 Do widzenia.
Wpisz komendę FTP.

OPEN SYSNAM02
    Łączenie z hostem SYSNAM02 pod adresem 9.4.73.250 za pomocą portu 21.
220-QTCP pod nazwą SYSNAM02.sysnam123.ibm.com.
220 Połączenie zostanie zamknięte, jeśli będzie bezczynne przez ponad 5 minut.
Wpisz komendę FTP.

```

Rysunek 6. Wyjście FTP (FTPLOG) po uruchomieniu programu FTPBATCH (część 3)

```

> USER GWIL ****
331 Wpisz hasło.
230 GWIL zalogowany.
    OS/400 jest zdalnym systemem operacyjnym. Wersja TCP/IP "V4R2M0".
250 Obecnie używany format nazewnictwa "0".
257 Biblioteka bieżąca to "QGPL".
Wpisz komendę FTP.

> EBCDIC
200 Typ reprezentacji niedrukowalny EBCDIC.
Wpisz komendę FTP.

> PUT GERRYLIB/RS6.RS6 GERRYLIB/RS6.RS6
200 Żądanie komendy PORT powiodło się.
150 Wysyłanie zbioru do podzbioru RS6 w zbiorze RS6 w bibliotece GERRYLIB.
250 Przesyłanie zbioru zakończone pomyślnie.
467 bytes transferred in 0.148 seconds. Transfer rate 3.146 KB/sec.
Wpisz komendę FTP.

> RCMD SNDNETF FILE(GERRYLIB/RS6) TOUSRID((GERRYLIB SYSNAM14))
250 Wykonanie komendy SNDNETF FILE(GERRYLIB/RS6) TOUSRID((GWIL SYSNAM14))
    powiodło się.
Wpisz komendę FTP.

```

Rysunek 7. Wyjście FTP (FTPLOG) po uruchomieniu programu FTPBATCH (część 4)

```

> CLOSE
221 Otrzymanie komendy QUIT.
Wpisz komendę FTP.
> QUIT
    (To kończy działanie aplikacji FTP)

```

Rysunek 8. Wyjście FTP (FTPLOG) po uruchomieniu programu FTPBATCH (część 5)

Należy przejrzeć powyższe dane wyjściowe, aby sprawdzić, czy podczas przetwarzania FTP nie pojawiły się błędy. Można to zrobić, przeglądając dane lub uruchomić program testujący pojawienie się kodów błędu odpowiedzi. Trzycyfrowe kody błędu odpowiedzi FTP zaczynają się od 4 lub 5. Należy uważać, aby unikać komunikatów, takich jak "467 bytes transferred..." ("467 przesłanych bajtów...").

Przykładowa procedura: Przykładowa procedura REXX i przykładowy podzbiór zbioru fizycznego są dostarczone 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 FTP



Poniższe sekcje zawierają informacje, które mogą być przydatne podczas pracy z serwerem lub klientem FTP:

Komendy serwera FTP

Te komendy odpowiadają za komunikację pomiędzy klientem a serwerem. W sekcji znajduje się opis komend CL systemu iSeries, które są unikalne dla serwera FTP iSeries.

Komendy klienta FTP

Za pomocą komend klienta FTP można nawiązać połączenie ze zdalnym serwerem FTP, poruszać się po bibliotekach i katalogach, tworzyć, usuwać oraz przysyłać pliki.

Programy obsługi wyjścia FTP

Programów obsługi wyjścia FTP należy używać w celu zabezpieczenia dostępu do serwera FTP. Serwer FTP komunikuje się z każdym programem obsługi wyjścia za pomocą określonego punktu wyjścia. Sekcja zawiera opisy parametrów oraz kody przykładowych programów.

Dodatkowe informacje

- Metody przesyłania danych
- Systemy plików i konwencje nazewnictwa
- Komunikaty o statusie odpowiedzi serwera FTP
- Konwencje składni komend serwera FTP
- Konwencje składni komend klienta FTP



Komendy serwera FTP

Sekcja ta dotyczy komend serwera FTP. Klienci FTP komunikują się z serwerem za pomocą komend serwera. Ponieważ użytkownik zazwyczaj nie komunikuje się z serwerem FTP, w tej sekcji przedstawione są poszczególne komendy serwera, opisy ich działania, konwencje składni i komunikaty statusu odpowiedzi FTP.

Serwer FTP iSeries obsługuje następujące komendy:

Komenda	Działanie
ABOR	Anuluje poprzednią komendę
ADDM	Dodaje podzbiór do zbioru fizycznego

Komenda	Działanie
ADDV	Dodaje podzbiór o zmiennej długości do zbioru fizycznego
APPE	Dopisuje dane do podanego pliku
AUTH	Definiuje mechanizm uwierzytelniania używany dla bieżącej sesji FTP
CDUP	Zmienia katalog na katalog nadrzędny
CRTL	Tworzy bibliotekę
C RTP	Tworzy zbiór fizyczny
C RTS	Tworzy źródłowy zbiór fizyczny
CWD	Zmienia katalog roboczy lub bibliotekę
DEBUG	Uruchamia lub zatrzymuje śledzenie serwera
DELE	Usuwa zbiór, podzbiór lub dokument
DLTF	Usuwa zbiór
DLTL	Usuwa bibliotekę
HELP	Pobiera informacje o komendach serwera FTP
LIST	Wyświetla listę plików lub pozycji katalogu
MKD	Tworzy katalog
MODE	Określa format przesyłanych danych
NLST	Wyświetla listę nazw plików lub katalogów
NOOP	Sprawdza, czy serwer odpowiada
PASS	Wysyła hasło do serwera
PASV	Nakazuje serwerowi pasywne otwarcie kolejnego łącza danych
PBSZ	Definiuje maksymalną zabezpieczoną wielkość bufora dla zakodowanych danych na poziomie aplikacji wysyłanych lub odbieranych przez połączenie danych
PORT	Identyfikuje port danych, w którym klient będzie nasłuchiwał połączenia
PROT	Definiuje ochronę używaną dla połączeń danych w protokole FTP
PWD	Wyświetla bieżący katalog roboczy
QUIT	Wypisuje użytkownika z systemu; zamyka połączenie
RCMD	Wysyła komendę CL do serwera FTP
REIN	Ponownie uruchamia sesję w serwerze
RETR	Pobiera dane z serwera
RMD	Usuwa katalog
RNFR	Określa plik, który ma mieć zmienioną nazwę
RNTO	Określa nową nazwę pliku
SITE	Wysyła informacje do użycia przez serwer
STAT	Pobiera z serwera informacje o statusie
STOR	Zachowuje informacje w serwerze i zastępuje istniejący plik
STOU	Zachowuje informacje w serwerze, ale nie zastępuje istniejącego pliku

Komenda	Działanie
STRU	Określa strukturę pliku
SYST	Wyświetla nazwę systemu operacyjnego serwera
TIME	Ustawia wartość limitu czasu dla serwera FTP
TYPE	Określa typ przesyłania plików
USER	Wysyła ID użytkownika do serwera
XCUP	Zmienia katalog na nadrzędny
XCWD	Zmienia katalog roboczy
XMKD	Tworzy katalog
XPWD	Wyświetla bieżący katalog lub bibliotekę
XRMD	Usuwa katalog

Komendy unikalne dla serwera FTP iSeries

Komendy serwera FTP iSeries obejmują specjalny zestaw komend, które są skróconymi nazwami odpowiadających im, lecz dłuższych, komend języka CL systemu iSeries. Nazwy specjalnych komend serwera muszą być skrócone do czterech liter, aby spełniały ograniczenia architektury FTP. Gdy serwer iSeries otrzymuje te komendy, interpretuje je następująco:

- ADDM = ADDPFM (Add Physical File Member - Dodanie podzbioru zbioru fizycznego)
- ADDV = ADDPVL (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, można używać komendy RCMD serwera FTP do wysłania dowolnej komendy CL do serwera.

Tematy pokrewne:

- Konwencje składni komend serwera FTP
- Komunikaty o statusie odpowiedzi serwera FTP
- Komendy klienta FTP: Służą one do nawiązywania połączeń ze zdalnym serwerem FTP, poruszania się po bibliotekach i katalogach, tworzenia, usuwania i przesyłania plików.

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

Komenda serwera FTP

ADDM parametry

parametry

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

Na przykład, aby dodać podzbiór BANANA do zbioru fizycznego GEORGE w bibliotece RLKAYS w serwerze iSeries, należy wpisać:

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

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

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

ADDV parametry

parametry

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

Na przykład, aby dodać podzbiór POLEBEAN do zbioru fizycznego GEORGE w bibliotece RLKAYS w serwerze iSeries, należy wpisać:

```
ADDV FILE(RLKAYS/GEORGE) MBR(POLEBEAN)
```

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

**APPE (Dopisanie do istniejącego pliku - Append to Existing File)
Komenda serwera FTP**

Komenda APPE serwera FTP akceptuje przekazane dane i zapisuje je w plikach w systemie serwera. Jeśli podany plik istnieje, dane są dodawane do tego pliku; w przeciwnym razie podany plik jest tworzony.

APPE *nazwa_pliku*

nazwa_pliku

Plik, w którym pobrane dane zostaną zapisane w systemie serwera.

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

**AUTH (Autoryzacja - Authorization)
Komenda serwera FTP**

Komenda AUTH serwera FTP określa mechanizm uwierzytelniania/ochrony, który jest używany dla bieżącej sesji FTP. Składnia komendy jest następująca:

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

Wartości parametrów:

TLS-C	Jako mechanizm ochrony wykorzystywany jest protokół ochrony warstwy transportowej TLS. 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	Ma takie samo znaczenie jak TLS-C.
SSL	Ma takie samo znaczenie jak TLS-P.

Uwaga:

Protokół TLS jest kompatybilny z protokołem SSL (secure sockets layer).

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

**CRTL (Utworzenie biblioteki - Create Library)
Komenda serwera FTP**

CRTL parametry

parametry

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

Na przykład, aby utworzyć bibliotekę o nazwie TESTTCP w systemie serwera iSeries, należy wpisać:

CRTL TESTTCP

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

**CRTP (Utworzenie zbioru fizycznego - Create Physical File)
Komenda 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)

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

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

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

CWD (Zmiana katalogu roboczego lub biblioteki - Change working directory or library)

Komenda serwera FTP

Komenda CWD serwera FTP służy do zmiany katalogu roboczego, biblioteki lub grupy plików.

```
CWD katalog
```

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

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

Uwaga:

Śledzenie serwera FTP powinno być używane jedynie do raportowania błędów w programach IBM. Użycie tej funkcji może wpłynąć na wydajność systemu.

Komenda serwera FTP

```
DEBUG
```

Jeśli śledzenie serwera FTP nie jest aktywne, zostanie ono uruchomione. Serwer wykonuje śledzenie, dopóki nie odbierze innej komendy DEBUG lub komendy QUIT. Gdy serwer zakończy śledzenie, sformatowanie jego wyników może odbyć się z pewnym opóźnieniem.

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

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

Komenda serwera FTP

Aby usunąć plik, podzbiór lub dokument, należy użyć komendy DELE serwera FTP:

```
DELE plik_zdalny
```

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

DLTF (Usunięcie zbioru - Delete File) **Komenda 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)
```

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

DLTL (Usunięcie biblioteki - Delete Library) **Komenda 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
```

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

HELP (Wyświetlanie pomocy ze zdalnego serwera iSeries - Getting Help from an iSeries Remote Server)

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

HELP [komenda]

komenda

Nazwa komendy serwera, dla której mają zostać wyświetlone informacje pomocy. Na przykład HELP ADDM spowoduje wyświetlenie informacji pomocy dotyczących dodawania podzbioru do zbioru fizycznego w serwerze iSeries.

Aby określić składnię komendy ADDV używanej przez serwer iSeries, należy wpisać komendę:

```
HELP ADDV
```

Idź do:

- Komendy serwera FTP

- Konwencje składni komend serwera FTP

LIST (Lista zbiorów - File List)

Komenda serwera FTP

Aby wyświetlić pozycje katalogów, zawartość biblioteki lub pliki w grupie plików, należy użyć komendy LIST serwera FTP:

```
LIST [katalog | nazwa]
```

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

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP
- SITE (Wysłanie informacji używanych przez serwer - Send Information Used by a Server System): Komenda służąca do zmiany danych wyświetlanych przez komendę LIST.
- Wyświetlanie (LIST) informacji w formacie systemu UNIX: Komenda służąca do sprawdzenia, jakie dane wyświetlane są przez komendę LIST.
- Wyświetlanie (LIST) informacji w formacie systemu iSeries: Komenda służąca do sprawdzenia, jakie dane wyświetlane są przez komendę LIST.

MKD (Utworzenie katalogu - Make directory)

Komenda serwera FTP

Aby utworzyć katalog, należy użyć komendy MKD serwera FTP.

```
MKD nazwa_katalogu
```

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

MODE (Ustawienie trybu przesyłania danych - Set Transfer Mode)

Komenda serwera FTP

Komenda MODE serwera FTP służy do określania trybu lub formatu przesyłanych bitów danych:

```
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 tym trybie dane przesyłane są jako strumień bajtów. W trybie strumieniowym można użyć dowolnego typu reprezentacji. Ten typ przesyłania jest bardziej wydajny, ponieważ serwer nie przekazuje żadnych informacji o blokach danych.

Uwagi:

1. Tryb strumieniowy jest domyślnym i preferowanym trybem przesyłania danych używanym w serwerze iSeries.
2. Jeśli nie podano żadnych parametrów, serwer zwraca odpowiedź wskazującą aktualne ustawienia MODE.

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

**NLST (Lista nazw - Name List)
Komenda serwera FTP**

Komendy NLST serwera FTP używa się do wyświetlania samych nazw plików w zestawach plików, grupie plików oraz katalogach lub bibliotekach w następującym formacie:

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

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

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

**NOOP (Uzyskanie odpowiedzi serwera - Obtain Server Response)
Komenda serwera FTP**

Komenda NOOP serwera FTP wysyła do klienta odpowiedź "OK". Komenda ta nie wpływa w żaden sposób na przetwarzanie serwera. Klient używa tej komendy do określenia, czy serwer jest podłączony i czy odpowiada. Użycie komendy NOOP:

```
NOOP
```

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

**PASS (Hasło -Password)
Komenda serwera FTP**

```
PASS hasło
```

hasło

Łańcuch tekstu, który określa hasło w systemie serwera.

Uwaga:

Komenda serwera USER musi być wydana tuż przed komendą serwera PASS.

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

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

Komenda serwera FTP

Aby nakazać serwerowi pasywne otwarcie następnego połączenia danych, należy użyć komendy PASV serwera FTP w następującym formacie:

```
PASV
```

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

PBSZ (Zabezpieczenie wielkości bufora - Protection Buffer Size)

Komenda serwera FTP

Komenda PBSZ definiuje maksymalną wielkość bufora dla danych zakodowanych na poziomie aplikacji, wysyłanych lub odbieranych przez połączenie danych. Składnia tej komendy jest następująca:

PBSZ *wartość*

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

Uwaga:

Dokument RFC2228 wymaga, aby komenda PBSZ była wysyłana przed komendą PROT. Ponieważ TLS/SSL obsługuje blokowanie danych, jedyną dopuszczalną wartością jest "0".

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

PORT (Port danych - Data Port)

Komenda serwera FTP

Aby podać port, na którym klient będzie nasłuchiwał połączenia danych, należy użyć komendy PORT serwera FTP w następującym formacie:

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

hn

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

pn

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:

$$\text{port} = (p1 * 256) + p2$$

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:

Zgodnie ze specyfikacją TCP/IP RFC 1122, gdy serwer zamknie połączenie, nie może połączyć się z tym samym adresem IP klienta i numerem portu, dopóki nie upłynie dwuminutowy czas opóźnienia. Serwer może nawiązać połączenie z tym samym adresem IP klienta przy innym numerze portu, bez tej restrykcji.

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

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

Komenda serwera FTP

Komenda PROT definiuje ochronę używaną dla połączeń danych w protokole FTP (używanych do przesyłania listingów katalogów i danych w plikach). Składnia tej komendy jest następująca:

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

Wartości parametrów:

C	Jawne. Połączenie danych przesyła "surowe dane" w plikach bez ochrony.
P	Poufne. Połączenie danych będzie korzystał z protokołu TLS/SSL, który zapewnia ochronę integralności i poufność.

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

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

Komenda serwera FTP

Gdy wydana zostanie komenda PWD serwera FTP, serwer zwraca do klienta odpowiedź zawierającą nazwę bieżącego katalogu lub biblioteki. Komenda ta ma następujący format:

```
PWD
```

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

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

Komenda serwera FTP

Komenda QUIT serwera FTP wypisuje użytkownika klienta z systemu i zamyka połączenie sterujące. Jeśli trwa przesyłanie plików, połączenie utrzymywane jest do momentu zakończenia przesyłania, a następnie serwer je zamyka.

```
QUIT
```

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

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

Komenda serwera FTP

Komenda RCMD serwera FTP służy do uruchamiania komend systemu iSeries w języku CL w systemie serwera FTP. Łańcuch komendy RCMD ma długość do 1000 znaków. Ponieważ żaden wiersz komend nie jest dostępny, komenda RCMD musi zawierać wszystkie parametry niezbędne do uruchomienia komendy CL.

Jeśli komenda CL, wywołana przez komendę RCMD, zostanie pomyślnie wykonana, wyświetlany jest komunikat informujący o jej pomyślnym wykonaniu. Gdyby wystąpił błąd, 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.

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

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

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

Komenda 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 wartości domyślne wszystkich parametrów serwera.
4. Pozostawia otwarte łącze sterujące.

Idź do:

- Komendy serwera FTP

- Konwencje składni komend serwera FTP

RETR (Pobranie pliku - Retrieve file)

Komenda serwera FTP

Komenda RETR serwera FTP służy do pobrania danych z systemu serwera.

```
RETR plik_zdalny
```

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

RMD (Usuwanie katalogu - Remove directory)

Komenda serwera FTP

Komenda RMD serwera FTP służy do usuwania katalogu.

```
RMD nazwa_katalogu
```

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

RNFR (Zmiana nazwy z - Rename From)

Komenda serwera FTP

Komenda RNFR serwera FTP używana jest do zmiany nazw plików. Bezpośrednio po niej należy użyć komendy RNTO (Zmiana nazwy na - Rename To) serwera FTP.

```
RNFR nazwa_pliku
```

nazwa_pliku

Nazwa pliku, która ma zostać zmieniona.

Uwaga:

W serwerze iSeries plik, którego nazwa jest zmieniana, nie może zostać przeniesiony do innego systemu plików.

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

RNTO (Zmiana nazwy na - Rename To)

Komenda serwera FTP

Komenda RNTO serwera FTP określa nową nazwę pliku podczas zmieniania nazwy plików w systemie serwera. Należy jej użyć bezpośrednio po komendzie RNFR, która określa nazwę pliku.

```
RNTO nazwa_pliku
```

nazwa_pliku

Nowa nazwa pliku, jaka ma być nadana.

Uwaga:

W serwerze iSeries plik, którego nazwa jest zmieniana, nie może zostać przeniesiony do innego systemu plików.

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

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

Komenda serwera FTP

Komenda SITE serwera FTP używana jest do wysłania informacji lub do udostępniania usług typowych dla serwera. Używana jest w następującym formacie:

```
SITE [parametry]
```

Serwer FTP iSeries obsługuje następujące parametry komendy SITE:

LISTFMT 0

Serwer zwraca informacje dla komendy LIST w formacie iSeries, wprowadzonym w wersji V3R1M0. Klient iSeries obsługuje formaty systemu iSeries oraz systemu UNIX.

LISTFMT 1

Serwer zwraca informacje dla komendy LIST w formacie UNIX. Nazwa pliku jest ostatnią pozycją każdego zwróconego wiersza. Klient iSeries obsługuje formaty systemu iSeries oraz systemu UNIX.

LISTFMT

Zwraca komunikat wskazujący bieżące ustawienia LISTFMT serwera FTP.

Uwagi:

Aby zmienić domyślne ustawienia LISTFMT na serwerze, należy użyć opcji LISTFMT komendy CHGFTP. Do ustawienia tej właściwości serwera FTP można także wykorzystać program iSeries Navigator:

1. W programie iSeries Navigator rozwiń **serwer iSeries** —> **Sieci** —> **Serwery** —> **TCP/IP**.
2. W prawym panelu kliknij prawym przyciskiem myszy **FTP** i wybierz **Właściwości**.
3. Kliknij zakładkę **Formaty**.
4. W części **Lista zbiorów** uaktywnij iSeries lub UNIX jako domyślną wartość LISTFMT w serwerze.
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 nazewnictwa jest dopuszczalny dla wszystkich

systemów plików, które obsługiwane są przez FTP, w tym dla systemu plików bibliotek. Aby pracować ze wszystkimi systemami plików iSeries z wyjątkiem systemu plików bibliotek, należy ustawić format nazewnictwa na "1".

NAMEFMT

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

Uwaga:

Ustawienia domyślnej wartości NAMEFMT serwera FTP iSeries można zmienić za pomocą opcji NAMEFMT komendy CHGFTP.

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 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 nie dopuszcza przesyłania zbiorów baz danych zawierających pola NULL. Jest to wartość domyślna.

NULLFLDS 1

Serwer dopuszcza przesłanie zbiorów baz danych zawierających pola NULL.

Uwaga:

Przesyłanie zbiorów, które zawierają pola NULL, wymaga włączenia tej opcji w serwerze i kliencie. Nie można przewidzieć wyników przesyłania, gdy zbiór zawierający pola NULL jest przesyłany do systemu innego niż serwer iSeries oraz gdy typ przesyłania wymaga konwersji strony kodowej danych.

NULLFLDS

Zwraca komunikat wskazujący bieżące ustawienia NULLFLDS serwera FTP.

TRIM 0

Ustawienie opcji Trim na OFF (Wyłączone). Serwer wysyła odstępy na końcu rekordów bazy danych.

TRIM 1

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

TRIM 2

Dla wszystkich przesyłań (w tym dokonanych za pomocą struktury rekordów i trybu blokowego) serwer nie wysyła odstępów na końcu rekordów bazy danych.

TRIM

Zwraca komunikat zawierający aktualne ustawienia opcji Trim serwera FTP.

Uwagi:

1. Zanim komenda ta została udostępniona, przed przesłaniem pliku do serwera odstępy na końcu rekordów systemu zbiorów 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.

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

STOR (Zapisanie pliku - Store File) Komenda serwera FTP

Aby zapisać dane w serwerze i nadpisać istniejący plik, można użyć komendy STOR serwera FTP w następującym formacie:

```
STOR plik_zdalny
```

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

STOU (Zapisanie unikalnych - Store Unique) Komenda serwera FTP

Aby zapisać dane w serwerze i nie nadpisać istniejącego pliku, można użyć komendy STOU serwera FTP w następującym formacie:

```
STOU plik_zdalny
```

Serwer tworzy unikalną nazwę pliku. Zostanie ona umieszczona w komunikacie zwracanym do klienta.

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

STRU (Określenie struktury plików - Specify File Structure) Komenda serwera FTP

Komenda STRU serwera FTP używana jest do określania struktury pliku jako ciągłej sekwencji bajtów danych. Używana jest w następującym formacie:

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.

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

SYST (Identyfikacja nazwy systemu operacyjnego - Identify the Name of the Operating System) **Komenda serwera FTP**

Komenda SYST serwera FTP służy do uzyskania nazwy systemu operacyjnego w serwerze:

SYST

Zwrócone informacje zależą od systemu.

Serwer iSeries podaje wersję TCP/IP.

Oto przykładowa odpowiedź serwera:

OS/400 jest zdalnym systemem operacyjnym. Wersja TCP/IP "V4R4M0".

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

TIME (Ustawienie wartości czasu oczekiwania dla serwera FTP - Set Time-Out Values for FTP Server) **Komenda serwera FTP**

Po nawiązaniu połączenia sterującego między klientem a serwerem FTP, serwer FTP kontroluje limity czasu dla połączeń. Jest to wartość limitu czasu braku aktywności.

Istnieje także wartość limitu czasu dla połączenia, 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. Wartości limitu czasu braku aktywności mogą być z zakresu od 1 do 9,999,999 sekund. Domyślną wartością limitu czasu braku aktywności jest 300 sekund.

przesyłanie

Limit czasu przesyłania w sekundach. Parametr ten jest opcjonalny. Jeśli nie zostanie podany, serwer nie zmieni bieżącej wartości. Wartość limitu czasu przesyłania może być z zakresu od 1 do 9,999,999 sekund. Domyślnym limitem czasu przesyłania jest 420 sekund.

Na przykład, aby ustawić limit 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 to wyłącznie komenda serwera FTP iSeries.

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

TYPE (Określenie typu reprezentacji - Specify Representation Type) Komenda serwera FTP

Aby określić typ przesyłania plików lub reprezentację znaków, z jaką ma odbywać się przesyłanie, należy użyć komendy TYPE serwera FTP w następującym formacie:

```
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 CHGFTP.

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

IBM EBCDIC Kanji (CCSID 5035)

F 1

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.

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

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

USER nazwa_użytkownika

nazwa_użytkownika

Profil użytkownika w serwerze iSeries.

Uwaga:

Jeśli komenda USER powiedzie się, a w serwerze iSeries skonfigurowano ochronę przy użyciu hasła, do klienta zostanie wysłana odpowiedź z żądaniem hasła. Klient wyśle do serwera hasło za pomocą komendy serwera PASS. Jeśli serwer pracuje na poziomie ochrony 10, pytanie o hasło nie pojawi się.

Idź do:

- Komendy serwera FTP
- Konwencje składni komend serwera FTP

Komendy klienta FTP

Komendy protokołu FTP umożliwiają przesyłanie plików pomiędzy komputerami. Używając komend klienta FTP można nawiązać połączenie ze zdalnym serwerem FTP, poruszać się po bibliotekach i katalogach, tworzyć, usuwać oraz przysyłać pliki.

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

Klient FTP iSeries obsługuje wymienione poniżej komendy. W tabeli podano te komendy, ich poprawne skróty i wszystkie spełniane przez nie funkcje.

Komenda	Działanie
?	Opisuje sposób używania FTP
ACCT	Wysyła do systemu zdalnego informacje o koncie użytkownika
APPEND	Dodaje do zbioru w systemie zdalnym podzbiór zbioru lokalnego
ASCII	Zmienia tryb przesyłania plików na format ASCII
BINARY	Zmienia tryb przesyłania plików na BINARY
CD	Zmienia katalog roboczy w systemie zdalnym
CDUP	Zmienia katalog w systemie zdalnym na nadrzędny
CLOSE	Zamyka sesję z systemem zdalnym
DEBUG	Włącza i wyłącza opcję debugowania
DEBUG	Zmienia wartości czasu oczekiwania klienta
DELETE	Usuwa plik z systemu zdalnego
DIR	Wyświetla katalogi i pliki systemu zdalnego
EBCDIC	Zmienia tryb przesyłania plików na format EBCDIC
GET	Kopiuje plik z systemu zdalnego do lokalnego
HELP	Pobiera informacje o komendach klienta FTP
LCD	Zmienia katalog roboczy w systemie lokalnym
LOCSITE	Podaje informacje o jednostce lokalnej
LOCSTAT	Wyświetla informacje o statusie jednostki lokalnej
LPWD	Wyświetla katalog roboczy systemu lokalnego
LS	Wyświetla listę nazw plików znajdujących się w zestawie plików systemu zdalnego

Komenda	Działanie
LTYPE	Określa typ przesyłania plików w systemie lokalnym
MDELETE	Usuwa grupę plików w serwerze
MGET	Kopiuje plik lub pliki z systemu zdalnego
MKDIR	Tworzy katalog lub podkatalog
MODE	Określa format danych dla przesyłania plików
MPUT	Wysyła lokalny plik lub pliki do systemu zdalnego
NAMEFMT	Określa obowiązujący format nazewnictwa plików
NOOP	Sprawdza, czy uzyskiwane są odpowiedzi
NULLFLDS	Umożliwia przesyłanie pól NULL
OPEN	Nawiązuje połączenie z serwerem FTP
PASS	Wysyła hasło użytkownika
PUT	Kopiuje podzbiór zbioru lokalnego do systemu zdalnego
PWD	Wyświetla bieżący katalog systemu zdalnego
QUIT	Kończy sesję FTP
QUOTE	Wysyła komendę do serwera FTP
REINITIALIZE	Ponownie uruchamia sesję z systemem 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 ustanowione jest połączenie chronione
SECOPEN	Otwiera chronione połączenie sterujące z serwerem FTP, używając określonego protokołu ochrony
SENDPASV	Określa, czy komenda PASV jest wysyłana
SENDPORT	Określa, czy komenda PORT jest wysyłana
SENDSITE	Określa, czy komenda SITE jest wysyłana
SITE	Wysyła informacje używane przez system zdalny
STATUS	Pobiera z systemu zdalnego informacje o statusie
STRUCT	Określa strukturę wysyłanych danych
SUNIQUE	Steruje zastępowaniem plików
SYSCMD	Uruchamia komendę języka CL w systemie lokalnym bez przerywania działania FTP
SYSTEM	Wyświetla dane o systemie operacyjnym zdalnego systemu
TYPE	Określa typ przesyłania plików
USER	Wysyła ID użytkownika do systemu zdalnego
VERBOSE	Steruje wyświetlaniem odpowiedzi serwera FTP

Tematy pokrewne:

- Konwencje składni komend klienta FTP
- Komendy serwera FTP

- Komunikaty o statusie odpowiedzi serwera FTP: Najczęściej spotykane kody odpowiedzi i ich znaczenie.

ACCT (Wysłanie informacji o koncie - Send Account Information)

Komenda klienta FTP

Wiele systemów przed udostępnieniem niektórych funkcji systemu wymaga podania informacji o koncie. System zdalny żąda podania tych informacji. Do wysyłania informacji o koncie służy komenda ACCT.

```
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 TCP/IP w systemie operacyjnym IBM Virtual Machine (VM) wymaga podania hasła dostępu do minidysków podczas operacji odczytu i zapisu. Komenda ACCT służy do podania hasła do minidysków bieżącego katalogu. Jeśli system zdalny jest systemem iSeries, komenda ACCT nie wykonuje żadnych działań.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

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

Komenda klienta FTP

Aby dodać lokalny podzbiór lub dokument albo inny plik systemu plików do pliku zdalnego, należy użyć komendy APPEND klienta FTP w następującym formacie:

```
APpend plik_lokalny [plik_zdalny]
```

plik_lokalny

Nazwa podzbioru zbioru lokalnego, dokumentu albo innego pliku iSeries. Nazwa pliku hierarchicznego systemu plików (HFS), który został dodany do katalogu w systemie zdalnym. Więcej informacji o nazewnictwie plików zawiera sekcja NAMEFMT (Wybieranie formatu nazewnictwa plików - Select File Naming Format).

plik_zdalny

Plik w systemie zdalnym. Jeśli nie zostanie podany plik zdalny, klient FTP utworzy nazwę domyślną. Więcej informacji o mechanizmie tworzenia nazw domyślnych zawiera sekcja Nazwy plików dla komend klienta służących do przesyłania danych.

Jeśli plik zdalny nie istnieje w serwerze, tworzy go serwer FTP.

Do dodania pliku do systemu zdalnego wymagane są uprawnienia zapisu w tym systemie. Może powstać konieczność podania dodatkowych informacji o koncie za pomocą komendy 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 komendy MODE. W przypadku zbioru zdalnego w formacie o stałej długości rekordów, serwer zachowuje format zbioru i długość rekordów. Gdy jest to wymagane, rekordy podzbioru zbioru lokalnego są wypełniane znakami pustymi lub skracane.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

**ASCII (Zmiana typu pliku na ASCII - Change File Type to ASCII)
Komenda klienta FTP**

AScii

Istnieją dwa podstawowe typy plików, których można używać podczas przesyłania plików za pomocą serwera FTP: ASCII i BINARY. Pliki ASCII są zwykłymi plikami tekstowymi. Mogą one mieć rozszerzenie .txt lub nie. Pliki BINARY są programami lub plikami innymi niż tekstowe, zapisanymi w formacie aplikacji, w której zostały stworzone, lub 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 nie przypisuje do pliku kontroli formatu pionowego. ASCII obsługuje jedynie domyślny format NON PRINT.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

**BINARY (Ustawienie typu przesyłania dla obrazu - Set Transfer Type to Image)
Komenda klienta FTP**

Binary

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

Jeśli do istniejącego zbioru iSeries przesyłane są dane binarne, system przyjmuje, że długość rekordu jest taka sama, jak długość rekordu w istniejącym zbiorze iSeries. Na przykład wielkość istniejącego zbioru powinna być wystarczająca, aby pomieścić nowe dane. Jeśli zbiór nie istnieje w serwerze iSeries, FTP wybiera odpowiednią długość rekordu.

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.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

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

Komenda CD klienta FTP służy do zmiany katalogu roboczego, biblioteki lub grupy plików w systemie zdalnym:

```
CD katalog
```

katalog

Nazwa znajdujących się w systemie zdalnym: katalogu plików, biblioteki lub specyfikatora grupy plików zależnych od systemu.

Jeśli system zdalny jest systemem iSeries, komenda ta zmienia bieżącą bibliotekę lub katalog. Aby sprawdzić, jakie katalogi znajdują się w systemie zdalnym, należy użyć komendy DIR. Spowoduje ona wyświetlenie listy katalogów.

Komendy DIR należy używać ostrożnie. Więcej informacji zawiera sekcja DIR (Wyświetlenie listy pozycji katalogu, bibliotek lub plików - List Directory Entries, Libraries, or Files).

Uwaga:

Używając komendy CD (lub LCD) do przejścia pomiędzy jednym systemem plików iSeries a innym, należy podać katalog główny systemu plików, który zawiera nowy katalog bieżący.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

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

Komenda CLOSE klienta FTP służy do zakończenia sesji z systemem zdalnym i pozostawienia działającego środowiska FTP w lokalnym systemie iSeries.

```
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. Komenda QUIT służy do zakończenia działania usługi i powrotu do środowiska iSeries, w którym uruchomiono FTP.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

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)

Uwaga:

Aby poinformować firmę IBM o problemach, wystarczy uruchomić śledzenie klienta protokołu FTP. Funkcja ta może mieć duży wpływ na wydajność systemu.

Możliwość taka istnieje dla systemu OS/400 w wersji V4R4 lub nowszej.

Komenda klienta FTP

Aby utworzyć zapis lub ekran śledzenia klienta FTP, należy użyć komendy DEBUG klienta FTP. 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.

```
DEBbug [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 do czasu, gdy wartość DEBUG zostanie zmieniona lub gdy działanie klienta zostanie zakończone. Gdy serwer zakończy śledzenie, sformatowanie jego wyników może odbyć się z pewnym opóźnieniem.

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.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

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

Komenda klienta FTP

Komenda DEBUG służy także do zmiany domyślnych wartości limitu czasu oczekiwania, gdy limit ten uniemożliwia pomyślne zakończenie przesyłania. Konieczność zmiany tych wartości może wystąpić jedynie wtedy, gdy ruch w sieci lub inne warunki spowodują poważne zwiększenie czasu przesyłania.

Aby zmienić limit czasu oczekiwania na przesyłanie klienta FTP, należy użyć komendy DEBUG klienta FTP:

```
DEBbug T1 | T2 [wartość]
```


T1

Zmiana lub wyświetlenie limitu czasu odczytu odpowiedzi serwera. Jeśli klient FTP nie otrzyma oczekiwanej odpowiedzi serwera w określonym czasie, klient zamyka 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.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

DELETE (Usunięcie pliku z systemu zdalnego - Delete a File on a Remote System) **Komenda klienta FTP**

Komenda DELETE służy do usuwania zbiorów lub podzbiorów zbiorów baz danych w systemie zdalnym. Komenda DELETE klienta FTP ma następujący format:

```
DELEte plik_zdalny
```

plik_zdalny

Plik, który ma być usunięty z systemu zdalnego. Informacje na temat określania zbioru w przypadku, gdy systemem zdalnym jest serwer iSeries, zawiera sekcja NAMEFMT (Wybranie formatu nazewnictwa plików - Select File Naming Format).

System zdalny może zażądać uprawnień do usunięcia pliku. W tym celu należy posłużyć się komendą ACCT (Wysłanie informacji o koncie - Send Account Information).

Warto także zapoznać się z następującymi sekcjami:

- MDELETE (Usunięcie wielu plików w systemie zdalnym - Delete Multiple Files on a Remote System)
- Komendy klienta FTP
- Konwencje składni komend klienta FTP

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

Komenda DIR klienta FTP służy do wyświetlania bibliotek i ich zawartości lub listy katalogów i pozycji katalogów w systemie zdalnym. Komendy DIR używa się w następującym formacie:

```
Dir [nazwa] [(Disk]
```

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 dozwolone jest używanie znaków gwiazdki *. Jeśli system zdalny jest systemem iSeries, to na przykład posłużenie się komendą:

DIR MYLIB/MYFILE.* powoduje wyświetlenie listy podzbiorów 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 nazewnictwa plików - Select File Naming Format).

(Disk

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

Jeśli system zdalny jest systemem iSeries, zwrócone informacje zawierają:

- 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 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 komendy List (LS - Wyświetlenie listy nazw zbiorów zdalnych) (patrz sekcja LS (Wyświetlenie nazw plików zdalnych - List Remote File Names)).

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

**EBCDIC (Zmiana typu pliku na EBCDIC - Change File Type to EBCDIC)
Komenda klienta FTP**

EBcdic

Typ przesyłania EBCDIC jest potrzebny do przesyłania plików do lub z innego systemu EBCDIC. Pomaga to uniknąć konieczności przeprowadzania konwersji pomiędzy reprezentacjami znaków ASCII a EBCDIC w obu systemach.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

**GET (Kopiowanie pliku z systemu zdalnego do lokalnego - Copy a File from a Remote System to the Local System)
Komenda 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 Nazwy plików dla komend 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 podana 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
```

Jeśli przyjmujemy, że serwer zdalny jest systemem iSeries, komenda ta pobiera podzbiór PODZB zbioru ZB w bibliotece BIBL i umieszcza go w podzbiórze PODZB zbioru ZB, w bieżącym katalogu systemu lokalnego. Więcej informacji o definiowaniu katalogu bieżącego zawiera sekcja LCD (Zmiana biblioteki roboczej lub katalogu w systemie lokalnym - Change Working Library or Directory on Local System).

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. Więcej informacji na ten temat zawiera sekcja Umieszczanie parametrów komend.

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

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP
- MGET (Kopiowanie wielu plików z systemu zdalnego do systemu lokalnego - Copy Multiple Files from a Remote System to the Local System)
- PUT (Kopiowanie podzbióru zbioru z systemu lokalnego do pliku w systemie zdalnym - Copy a File Member from the Local System to a File on a Remote System)
- MPUT (Wysłanie wielu podzbiórów z systemu lokalnego do systemu zdalnego - Send Multiple File Members from the Local System to a Remote System)

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

Komenda HELP służy do uzyskiwania informacji o komendach FTP używanych przez system lokalny i system zdalny.

Pomoc dla komend klienta FTP

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

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

*** lub ALL**

Powodują wyświetlenie listy komend klienta FTP.

komenda

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 wyświetlić listę lokalnych komend serwera iSeries, należy wpisać:

```
HELP
```

Informacje pomocy można uzyskać korzystając z komendy ? .

Pomoc dotycząca komend serwera FTP

Aby uzyskać informacje o komendach FTP systemu zdalnego, należy użyć komendy HELP w następującej formie:

```
Help SERVER [komenda]
```

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.

komenda

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.

Więcej informacji zawiera sekcja QUOTE (Wysłanie komendy do serwera FTP - Send a Subcommand to an FTP Server).

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

LCD (Zmiana biblioteki roboczej lub katalogu w systemie lokalnym - Change Working Library or Directory on Local System) **Komenda 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 komendy CD (lub LCD) w celu zmiany jednego systemu plików na inny, należy podać katalog główny. Na przykład /QDLS lub /QOPT.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

LOCSITE (Podanie informacji o środowisku lokalnym - Specify Local Site Information)

Komenda klienta FTP

Komenda LOCSITE klienta FTP służy do podawania informacji używanych przez klienta FTP w usługach typowych dla danego systemu klienta.

LOCSITE [parametry]

Klient FTP iSeries obsługuje następujące parametry i opcje parametrów komendy 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 sprawdza, czy podana wartość jest poprawna.

CRTCCSID

Wyświetlenie komunikatu, który zawiera aktualne ustawienia CRTCCSID klienta FTP.

TRIM 0

Ustawienie opcji Trim na OFF (Wyłączone). Serwer wysyła odstępy na końcu rekordów bazy danych.

TRIM 1

Ustawienie opcji Trim na ON (Włączone). Serwer nie wysyła odstępów na końcu rekordów 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 odstępy na końcu rekordów systemu zbiorów 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 bieżące wartości zmiennej ochrony danych.



Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

LOCSTAT (Wyświetlenie informacji o statusie lokalnym - Display Local Status Information)

Komenda 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.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

**LS (Wyświetlenie nazw plików zdalnych - List Remote File Names)
Komenda klienta FTP**

```
LS [nazwa] [(Disk]
```

nazwa

Nazwa zdalnego katalogu, pliku lub biblioteki, która ma zostać wyświetlona. Jeśli system zdalny jest serwerem iSeries, to wyświetli on 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 (patrz sekcja CD (Zmiana katalogu roboczego lub biblioteki - Change Working Directory or Library)). 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 podany zostanie parametr (Disk i ta sama wartość *CURLIB, serwer zmienia zawartość podzbioru pliku 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 niezawierający 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).

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

**LTYPE (Typ lokalny - Local Type)
Komenda klienta FTP**

Aby określić typ przesyłania plików lub reprezentację znaków, z jaką przesyłanie ma być przeprowadzone w systemie lokalnym, należy użyć komendy LTYPE klienta FTP w następującym formacie:

```
LType C nr_ccsid
```

C

Typ identyfikatora CCSID. Należy wpisać C.

nr_ccsid

Wartość identyfikatora CCSID. Należy wpisać CCSID z zakresu 1-65533.

Uwaga:

Komenda LTYPE jest podobna do komendy TYPE (opisanej w sekcji TYPE (Określenie typu przesyłania plików - Specify File Transfer Type)). Komenda LTYPE zmienia jedynie typ reprezentacji znaków po stronie klienta. Komenda TYPE zmienia typ reprezentacji znaków klienta i serwera.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

MDELETE (Usunięcie wielu plików w systemie zdalnym - Delete Multiple Files on a Remote System) **Komenda klienta FTP**

```
MDelete {plik_zdalny [plik_zdalny...]}
```

plik_zdalny

Plik lub pliki w systemie serwera, które mają być usunięte.

Uwaga:

Gdy zdalny zbiór jest zbiorem systemu plików QSYS.LIB iSeries, serwer usuwa wszystkie podzbiory zbioru fizycznego iSeries. Sam zbiór nie jest usuwany.

Poniżej znajduje się przykład dotyczący systemu plików bibliotek w formacie NAMEFMT 0:

```
MDELETE BIBLM/ZB1.PODZBA BIBLT/ZB2.PODZBB
```

Komenda ta usuwa podzbiór PODZBA w zbiorze ZB1, w bibliotece BIBLM i podzbiór PODZBB, w zbiorze ZB2 w bibliotece BIBLT w zdalnym serwerze iSeries. Ten sam przykład dla formatu NAMEFMT 1:

```
MDELETE /QSYS.LIB/BIBLM.LIB/ZB1.FILE/PODZBA.MBR  
/QSYS.LIB/BIBLT.LIB/ZB2.FILE./PODZBB.MBR
```

Oto przykład dotyczący systemu plików biblioteki dokumentów w formacie NAMEFMT 1:

```
MDELETE /QDLS/QIWSOS2/PCSMENU.EXE /QDLS/PCSDIR/PCSFIL.EXE
```

Wydanie tego polecenia powoduje usunięcie dokumentu PCSMENU.EXE w folderze QIWSOS2, w bibliotece dokumentów usług biblioteki dokumentów i jednocześnie zbioru PCSFILE.EXE w folderze PCSDIR, w bibliotece QDLS systemu iSeries.

Aby usunąć wiele plików, można użyć znaku gwiazdki (*). Na przykład dla NAMEFMT 0, jeśli system zdalny jest systemem iSeries, wpisz:

```
MDELETE BIBL/ZB.*
```

W przykładzie tym usunięte zostałyby wszystkie podzbiory zbioru ZB w bibliotece BIBL. Użycie gwiazdki dopuszczalne jest jedynie na końcu łańcucha znaków.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

MGET (Kopiowanie wielu plików z systemu zdalnego do systemu lokalnego - Copy Multiple Files from a Remote System to the Local System)

Komenda klienta FTP

Przekazywanie plików za pomocą komendy MGET:

Komenda MGET klienta FTP służy do kopiowania wielu plików. Używana jest w następującym formacie. Dla każdego pliku zdalnego, który ma być przesłany, wykonywana jest osobna komenda GET. Serwer automatycznie tworzy nazwę odpowiedniego pliku lokalnego, tak jak określają to reguły 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 używa bieżącej biblioteki lub bieżącego katalogu,
- jeśli użytkownik nie wydał komendy LCD, serwer przyjmuje 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 bieżącej biblioteki, serwer używa QPGL jako bieżącego katalogu.

```
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. Więcej informacji dotyczących komendy GET zawiera sekcja GET (Kopiowanie pliku z systemu zdalnego do lokalnego - Copy a File from a Remote System to the Local System).

Aby skopiować wszystkie podzbiory do bieżącej biblioteki lub katalogu można użyć znaku gwiazdki (*). Na przykład jeśli system zdalny jest systemem iSeries, to komenda:

- 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.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

MKDIR (Utworzenie katalogu - Make Directory)

Komenda klienta FTP

```
MKdir nazwa_ścieżki
```

nazwa_ścieżki

Nazwa znajdujących się w systemie zdalnym: katalogu plików, biblioteki lub specyfikatora grupy plików zależnych od systemu.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

MODE (Określenie trybu przesyłania danych - Specify Transmission Mode of Data) **Komenda klienta FTP**

```
MODE [ B | S]
```

B

Tryb blokowy. W tym trybie serwer przesyła dane jako serie bloków danych zaopatrzonych w jeden lub więcej bajtów nagłówka. Jeśli dane przesyłane są w trybie blokowym, typ danych musi zostać ustawiony na EBCDIC.

S

Tryb strumieniowy. W trybie tym serwer 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.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

MPUT (Wysyłanie wielu podzbiorów z systemu lokalnego do systemu zdalnego - Send Multiple File Members from the Local System to a Remote System) **Komenda klienta FTP**

Komenda MPUT klienta FTP służy do wysyłania jednego lub więcej plików lokalnych do systemu zdalnego. Klient wykonuje oddzielne komendy PUT dla każdego pliku lokalnego, który ma być przekazany. 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 obsługiwane 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) (patrz sekcja SUNIQUE (Sterowanie nadpisywaniem plików - Control Overwriting of Files)).

Szczegółowe informacje o tym, jak określić plik w przypadku, gdy system zdalny jest systemem iSeries, zawiera sekcja NAMEFMT (Wybranie formatu nazewnictwa plików - Select File Naming Format). W poniższym przykładzie użyto polecenia NAMEFMT 0:

```
MPUT BIBL/ZB1.PODZB1 BIBL/ZB1.PODZB2
```

Polecenie to powoduje wysłanie do systemu zdalnego podzbiorów MBR1 i MBR2 zbioru FILE1 z biblioteki MYLIB.

W poniższym przykładzie użyto polecenia NAMEFMT 1:

```
MPUT /QDLS/QIWSOS2/PCSMENU.EXE /QDLS/QIWSOS2/PCSMENU2.EXE
```

Polecenie to powoduje wysłanie do systemu zdalnego dokumentów 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. Informacje dodatkowe na ten temat zawiera sekcja MGET (Kopiowanie wielu plików z systemu zdalnego do systemu lokalnego - Copy Multiple Files from a Remote System to the Local System).

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP
- 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)

NAMEFMT (Wybranie formatu nazewnictwa plików - Select File Naming Format)
Komenda klienta FTP

Komenda NAMEFMT klienta FTP służy do wybierania formatu nazw plików, który ma być używany w systemie lokalnym i systemie zdalnym (jeśli jest to system iSeries).

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 pracować ze wszystkimi systemami plików iSeries, należy ustawić format nazewnictwa 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_foldera[.ext]/}]nazwa_zbioru[.ext]
```

Dla napędów optycznych przyjmowany jest następujący format:

```
/QOPT/nazwa_wooluminu/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.

Warto także zapoznać się z następującymi sekcjami:

- Systemy plików i konwencje nazewnictwa
- Komendy klienta FTP
- Konwencje składni komend klienta FTP

NULLFLDS (Umożliwienie przesyłania zbiorów z polami NULL -Allow Transfer of Files with NULL Fields) **Komenda klienta FTP**

Za pomocą tej komendy można zdecydować, czy przesyłanie zbiorów bazy danych zawierających wartości pola NULL w systemie lokalnym i systemie zdalnym, jeśli jest to system iSeries, jest dopuszczalne, czy też nie.

```
NULLflids [ 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 tej opcji w serwerze i kliencie. Zbiór docelowy musi istnieć zanim przesyłanie zostanie rozpoczęte. Musi on także mieć tę samą definicję zbioru, co zbiór źródłowy.
2. Nie można przewidzieć wyników przesyłania zbioru zawierającego pola NULL do serwera, który nie jest serwerem iSeries oraz jeśli typ przesyłania wymaga konwersji strony kodowej danych.
3. Jeśli wydana zostanie komenda NULLFLDS bez parametru, klient wyświetli bieżące ustawienia.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

OPEN (Połączenie z serwerem FTP w systemie zdalnym - Connect to FTP Server on a Remote System)**Komenda klienta FTP**

```
Open nazwa_systemu [numer_portu]
```

nazwa_systemu

Nazwa lub adres internetowy systemu zdalnego.

numer_portu

Numer portu, którego ma używać dana sesja do momentu, gdy serwer zamknie połączenie. Wartość opcjonalna. Jeśli numer portu nie zostanie podany, serwer go wybierze sam.

Gdy połączenie z systemem zdalnym zostanie otwarte, nie można połączyć się z innym systemem, zanim bieżąca sesja nie zostanie zamknięta.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

PASS (Wysłanie hasła - Send Your Password)**Komenda klienta FTP**

```
PASS hasło
```

hasło

Łańcuch tekstu będący hasłem.

Komendę tę muszą poprzedzać komendy OPEN i USER. Dla niektórych systemów komenda ta kończy weryfikację podczas kontroli dostępu. Komenda ta nie jest konieczna, gdy serwer wymaga wpisania hasła podczas łączenia lub logowania się do serwera.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

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)**Komenda 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. Więcej informacji o nazwach domyślnych zawiera sekcja Nazwy plików dla komend klienta służących do przesyłania danych. Jeśli zdalny plik o tej nazwie już istnieje, serwer zastępuje jego zawartość zawartością pliku_lokalnego, chyba że włączono opcję Store Unique (SUNIQUE) (informacje na ten temat zawiera sekcja SUNIQUE (Sterowanie nadpisywaniem plików - Control Overwriting of Files)).

Aby wysłać plik do systemu zdalnego, należy wybrać bieżący katalog roboczy z uprawnieniami do zapisu.

W przykładzie tym użyto komendy PUT do przesłania podzbioru:

```
PUT MYLIB/MYFILE.MYMBR (NAMEFMT = 0)
```

Komenda ta powoduje przesłanie podzbioru MYMBR zbioru MYFILE z biblioteki MYLIB do systemu zdalnego.

W przykładzie tym dokument PCSMENU.EXE wysyłany jest z folderu QIWSOS2 znajdującego się w systemie plików usług biblioteki dokumentów 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. Sekcja Umieszczanie parametrów komend zawiera więcej informacji na ten temat.

```
PUT LIBRARY/FILE.MEMBER 'MEMBER.ONE'
```

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP
- MPUT (Wysłanie wielu podzbiorów z systemu lokalnego do systemu zdalnego - Send Multiple File Members from the Local System to a Remote System)
- GET (Kopiowanie pliku z systemu zdalnego do lokalnego - Copy a File from a Remote System to the Local System)
- MGET (Kopiowanie wielu plików z systemu zdalnego do systemu lokalnego - Copy Multiple Files from a Remote System to the Local System)

PWD (Wyświetlenie bieżącego katalogu, folderu lub biblioteki - Display Current Directory, Folder, or Library)

Komenda klienta FTP

Komenda PWD klienta FTP służy do wyświetlenia bieżącego katalogu lub biblioteki w systemie zdalnym.

```
PWd
```

Jeśli serwer zdalny jest systemem iSeries, serwer wyświetla bieżącą bibliotekę lub katalog systemu plików systemu zdalnego. 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).

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

QUOTE (Wysłanie komendy do serwera FTP - Send a Subcommand to an FTP Server)

Komenda 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 komendy QUOTE do uruchomienia specjalnej komendy RCMD (Wysłanie komendy języka CL do serwera FTP - Send a CL Command to an FTP Server System) serwera FTP iSeries. Na przykład, aby zapisać protokół zadania serwera w kolejce wydruków, należy wpisać:

```
QUOTE RCMD DSPJOBLOG
```

Aby uzyskać dostęp do protokołu zadań, można skorzystać z komendy WRKSPLF. Trzeba pamiętać, że należy podać profil użytkownika, który zalogowany jest na serwerze FTP, jeśli komenda WRKSPLF jest uruchamiana z poziomu innego profilu użytkownika.

2. Serwer FTP iSeries ogranicza długość łańcucha do 1000 znaków.
3. W komendzie QUOTE do serwera przekazywany jest niezmieniony łańcuch. Na przykład, jeśli wpisane zostanie:

```
QUOTE CWD 'SYS1'
```

serwer otrzymuje

```
CWD 'SYS1'
```

Informacje pomocy z serwera można uzyskać wpisując komendę:

```
QUOTE HELP
```

Serwer wysyła komendę HELP do zdalnego hosta, który zwraca ekran z wszystkimi obsługiwanymi komendami. Wyświetlane informacje różnią się w zależności od typu zdalnego hosta.

Należy zauważyć, że komendy serwera wpisane z komendą QUOTE mają wpływ jedynie na serwer, ale podobne komendy klienta mogą mieć wpływ zarówno na klienta, jak i na serwer. Na przykład komenda klienta REIN wysyła do serwera komendę serwera REIN i reinicjuje pewne zmienne stanu klienta. QUOTE REIN wysyła do serwera jedynie komendę REIN, ale nie zmienia żadnych zmiennych stanu klienta.

Uwaga:

Używając komendy QUOTE do bezpośredniego wpisywania komend serwera, należy zachować ostrożność, aby nie przeprowadzić niepożądanych operacji. Zazwyczaj komenda QUOTE wykorzystywana jest jedynie w wyjątkowych sytuacjach, w których nie można użyć innych komend klienta. Przykładem jest konieczność posłużenia się specjalnymi komendami serwera iSeries, takimi jak CTRL.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

REINITIALIZE (Reinicjowanie sesji pomiędzy systemami - Reinitialize Session between Systems) **Komenda klienta FTP**

```
REInitialize
```

Jeśli serwer obsługuje komendę REINITIALIZE, działanie sesji USER z serwerem jest kończone. Serwer wraca do stanu, w jakim był po nawiązaniu połączenia i użytkownik musi się ponownie zalogować do systemu, aby kontynuować pracę.

Zanim sesja USER zostanie zakończona, wszystkie rozpoczęte przesyłania plików są doprowadzane do końca.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

RENAME (Zmiana nazwy pliku w systemie zdalnym - Rename a File on a Remote System) **Komenda 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 serwerze iSeries plik, którego nazwa jest zmieniana, nie może zostać przeniesiony do innego systemu plików.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

RESET (Resetowanie - Reset)**Komenda klienta FTP**

Aby wyczyścić kolejkę odpowiedzi serwera, można użyć komendy RESET klienta FTP:

```
REset
```

Komenda ta używana jest do ponownego zsynchronizowania sekwencji komend i odpowiedzi serwera z serwerem zdalnym FTP. Po naruszeniu protokołu FTP przez serwer zdalny resynchronizacja może być niezbędna.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

RMDIR (Usuwanie katalogu - Remove Directory)**Komenda klienta FTP**

```
RMdir nazwa_ścieżki
```

nazwa_ścieżki

Nazwa znajdujących się w systemie zdalnym: katalogu plików, biblioteki lub wskaźnika grupy plików zależnej od systemu. W hierarchicznym systemie plików (HFS) usuwać można jedynie puste katalogi. Do usuwania bibliotek serwer nie wymaga żadnych warunków.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

SECDData (Konfigurowanie ochrony danych - Setting data security protection)**Komenda klienta FTP**

Aby określić poziom ochrony, który ma być stosowany dla połączeń danych, gdy z systemem zdalnym jest już ustanowione chronione połączenie sterujące, należy użyć komendy SECDData w następujący sposób:

```
SECDData [ C | P ]
```

Uwaga: SData jest synonimem dla tej komendy.

C

Poziom ochrony kanału danych jest ustawiany na "jawny". Takie połączenie **nie** jest chronione. Może ono być używane do przesyłania danych wcześniej zaszyfrowanych lub nieistotnych.

P

Poziom ochrony kanału danych jest ustawiany na "poufny". Takie połączenie jest bezpieczne. Zanim jakiegokolwiek dane zostaną przesłane tym połączeniem, pomiędzy klientem a serwerem 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. Komenda serwera PROT jest wywoływana na serwerze za każdym razem, gdy komenda SECDATA pomyślnie ustawi poziom ochrony danych.
5. Podczas ustawiania poziomu ochrony danych, komenda SECData wysyła do serwera komendy PBSZ i PROT. Komenda SECData ustawia także zmienną klienta przy każdym pomyślnym wywołaniu komendy PROT. Zmienna ta reprezentuje ostatni poziom ochrony danych (C lub P) zaakceptowany przez serwer. 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.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

SECOpen (Konfigurowanie ochrony danych - Setting data security protection) Komenda klienta FTP

Komenda klienta FTP SECOpen otwiera chronione połączenie sterujące z serwerem FTP, używając określonych opcji ochrony. Składnia komendy jest następująca:

```
SECOpen nazwa_systemu [numer_portu] [ opcja_ochrony ]
```

Uwaga: SOpen jest synonimem dla SECOPEN.

nazwa_systemu

Nazwa lub adres internetowy zdalnego systemu.

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

Określenie rodzaju używanej ochrony.

(SSL

Do połączeń z serwerem FTP wykorzystywana jest ochrona za pomocą SSL. Podczas nawiązywania połączenia używana jest komenda serwera AUTH (Autoryzacja - Authorization).

(IMPLICIT

Wykorzystywana jest "niejawna" ochrona SSL/TLS połączenia z serwerem FTP. W "niejawnej" ochronie SSL połączenia z serwerem pomijane jest wysyłanie do serwera komend AUTH, PBSZ i PROT. W tym przypadku serwer musi być skonfigurowany, tak aby oczekiwał na negocjację połączenia za pomocą SSL/TLS, występującą dla określonego numeru portu.

Po zastosowaniu "niejawnej" ochrony za pomocą SSL serwer zadziała tak, jakby klient przesłał te komendy z niżej podanymi parametrami:

- AUTH SSL
- PBSZ 0
- PROT P

Uwaga:

Jeśli nie zostaną podane parametry opcje_ochrony, wtedy przyjmowany jest parametr (SSL. Kiedy używany jest port o numerze 990, przyjmowany jest parametr (IMPLICIT.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

SENDPASV (Określenie, czy wysłać komendę PASV - Specify Whether to send a PASV Subcommand)

Komenda klienta FTP

Aby określić, czy komenda PASV ma być przesłana do serwera FTP podczas przesyłania danych lub wydawania komend DIR i LS, wpisz komendę SENDPASV 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.

Wartością domyślną systemu iSeries (ON - Włączony) jest wysyłanie komendy PASV. Gdy parametr SENDPASV jest wyłączony, serwer nie wysyła komendy PASV.

Uwagi:

1. Ta komenda spełnia wymagania dokumentu RFC 1579, "Firewall-Friendly FTP" (FTP przyjazny dla firewalle). Użycie komendy PASV do nawiązania połączenia dla danych jest lepszą metodą, gdy dane muszą być przesyłane poprzez firewall. W niektórych scenariuszach przesyłanie danych poprzez 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 wysłania komendy PASV.
3. Gdy SENDPASV ma wartość Wyłączony lub jest nieaktywny oraz gdy parametr SENDPORT ma wartość Włączony, to wówczas serwer wysyła komendę PORT. Patrz sekcja SENDPORT (Określenie, czy wysyłać komendę PORT- Specify Whether to Sends a PORT Subcommand).
4. Serwery FTP, które nie obsługują PASV, nie spełniają warunków RFC 1123.

Ograniczenia

W przypadku połączenia z serwerem FTP poprzez serwer SOCKS, komenda SENDPASV może być użyta jedynie przed uruchomieniem przesyłania lub wydaniem komendy wyświetlenia zawartości katalogu. Jeśli komenda SENDPASV zostanie użyta po jednej z tych komend, klient nie będzie mógł nawiązać połączenia z serwerem FTP.

Gdy klient wyśle komendę przesyłania danych lub wyświetlenia zawartości katalogu, połączenie z serwerem FTP poprzez serwer SOCKS powinno zostać zamknięte przed ponownym użyciem komendy SENDPASV.

Komendy SENDPASV można użyć, gdy nie ma połączenia klienta FTP z serwerem.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

SENDPORT (Określenie, czy wysyłać komendę PORT - Specify Whether to Sends a PORT Subcommand)

Komenda klienta FTP

Określa, czy komenda PORT ma być przesłana do serwera FTP podczas przesyłania danych lub wydawania komend DIR i LS. Wpisz komendę SENDPASV klienta FTP:

```
SENDPOrt [ 0 | 1 ]
```

Jeśli nie zostanie wpisany żaden parametr, 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. Komendy SENDPORT należy używać jedynie wtedy, gdy bez niej nie można nawiązać połączenia z serwerem. Niewłaściwe użycie komendy SENDPORT może wywołać błędy.
2. Wskazane może być niewysyłanie komendy PORT do tych systemów, które ignorują komendy PORT, ponieważ wprowadzają one w błąd podając, że komenda ta została zaakceptowana.
3. Serwer nie wysyła komendy PORT, gdy opcja SENDPASV ma wartość Włączony. Patrz sekcja SENDPASV (Określenie, czy wysłać komendę PASV - Specify Whether to send a PASV Subcommand).

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

SENDSITE (Określenie, czy wysłać komendę SITE - Specify Whether to Send a SITE Subcommand)

Komenda klienta FTP

Aby określić, czy komenda SITE z informacjami o formacie rekordu ma być wysyłana automatycznie podczas przeprowadzania operacji PUT lub MPUT, wpisz komendę SENDSITE klienta FTP w następującym formacie:

```
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 komendy SITE (zawierającej informacje o formacie rekordu) przed wysłaniem komend PUT i MPUT. Ustawienie to powinno być używane podczas przesyłania plików do serwera IBM Virtual Machine, który wykorzystuje informacje o formacie rekordu wysyłane przez komendę SITE.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

SITE (Wysłanie informacji używanych przez system zdalny - Send Information Used by a Remote System)

Komenda klienta FTP

Komenda SITE jest stosowana do wysłania informacji wykorzystywanych przez serwer do udostępniania usług typowych dla systemu zdalnego. Jest ona używana w następującym formacie:

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. Komenda NAMEFMT używana jest przez komendę SITE do wskazania serwerowi, czy nazwy mają format NAMEFMT 0, czy NAMEFMT 1.

Więcej informacji zawiera sekcja SENDSITE (Określenie, czy wysyłać komendę SITE - Specify Whether to Send a SITE Subcommand).

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

STATUS (Pobranie informacji o statusie z systemu zdalnego - Retrieve Status Information from a Remote System)

Komenda klienta FTP

STAtus [*nazwa*]

nazwa

Nazwa zdalnego katalogu lub pliku, dla którego zażądano informacji o statusie. Nie jest to parametr wymagany.

Uwaga: Aplikacja serwera FTP iSeries nie obsługuje tego parametru.

Jeśli nie podano żadnego parametru, serwer 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.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

STRUCT (Określenie struktury plików - Specify File Structure)

Komenda klienta FTP

Komenda STRUCT klienta FTP służy do określania struktury wysyłanych danych. Jest ona używana w następującym formacie:

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.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

SUNIQUE (Sterowanie nadpisywaniem plików - Control Overwriting of Files) **Komenda klienta FTP**

Komenda SUNIQUE klienta FTP służy do sprawdzania, czy plik jest nadpisywany za pomocą komendy PUT lub MPUT. Jest ona używana w następującym formacie:

```
SUnique [ 0 | 1 ]
```

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 wysła nazwę tworzonego pliku z powrotem do użytkownika.

Uwaga:

Jeśli system zdalny jest systemem iSeries, serwer tworzy nazwy Zbiór.Podzbiór przez dodanie liczb na końcu nazwy podzbioru *pliku_lokalnego* podanego w komendzie PUT lub MPUT. Tak więc, jeśli nazwa *NOWYZBIÓR.NOWYPODZBIÓR* istnieje już w systemie zdalnym, zdalny serwer iSeries tworzy nazwę *NOWYZBIÓR.NOWYPODZBIÓR1* i zapisuje w niej dane.

Nazwy plików dla innych systemów plików, takich jak HFS, działają podobnie. Jeśli nazwa już istnieje, tworzony jest nowy plik, który składa się z podanej nazwy pliku i końcówki liczbowej. Tak więc, jeśli nazwa *nazwa_xfs* istnieje już w systemie zdalnym, zdalny system iSeries tworzy nazwę *nazwa_xfs1*.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

SYSCMD (Prześlij komendę CL iSeries do lokalnego systemu iSeries - Pass an iSeries 400 CL Command to Your Local iSeries 400 System) **Komenda klienta FTP**

Aby uruchomić komendę języka CL w lokalnym systemie iSeries bez opuszczania środowiska FTP, można użyć komendy SYSCMD klienta FTP w następującym formacie:

```
SYSCmd wiersz_komend
```

wiersz_komend

Komenda języka CL serwera iSeries. 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 istnieje konieczność przejrzenia komunikatów niskiego poziomu, które są wynikiem wydania komend języka CL lub wpisania wielu komend CL, przed powrotem do środowiska FTP, należy użyć komendy CALL QCMD systemu iSeries.

Na przykład, aby uzyskać ekran Wpisywanie komend (Command Entry) systemu iSeries, należy wpisać:

```
SYSCMD CALL QCMD
```

Na ekranie Wpisywanie komend (Command Entry) systemu AS/400 można następnie uruchomić aplikacje lub wpisywać komendy 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 języka CL iSeries można wpisać po naciśnięciu klawisza F21 (Wiersz komend CL) na głównym ekranie FTP. Serwer nie akceptuje klawisza F21, gdy do punktu wyjścia Client Request Validation FTP dodano program obsługi wyjścia.

Uwagi:

1. Większość systemów serwerów ma przedział czasu oczekiwania, który kończy sesję, gdy w podanym czasie brak aktywności w systemie. Jeśli podana komenda nie działa dłużej niż przedział czasu oczekiwania, serwer zakończy połączenie z klientem.
2. Serwer iSeries obsługuje znak wykrzyknika (!) jako synonim komendy SYSCMD.
3. Komenda SYSCMD przekazuje do systemu iSeries jako komendę języka CL dokładnie to, co wprowadzi użytkownik.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

TYPE (Określenie typu przesyłania plików - Specify File Transfer Type) Komenda klienta FTP

Aby określić typ przesyłania plików lub reprezentację znaków, z jaką ma odbywać się przesyłanie, należy użyć komendy TYPE klienta FTP w następującym formacie:

```
TYpe [ A  
      B [ 1 | 2 | 3 [A|R] | 4 [A|R] | 5 | 6 | 7 ]  
      C nr_ccsid  
      E  
      F [ 1 ]  
      I ]
```


A

Określa typ przesyłania jako typ domyślny (ASCII). Parametr ten ma takie samo działanie, jak komenda ASCII. Serwer nie przypisuje do pliku żadnej kontroli formatu pionowego. 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

Tradycyjny chiński (5550 - CCSID 938)

C nr_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 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

IBM EBCDIC Kanji (CCSID 5035)

F 1

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 wyświetli aktualne ustawienia komendy TYPE.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

USER (Wysłanie ID użytkownika do systemu zdalnego - Send Your User ID to the Remote System)
Komenda 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.

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

VERBOSE (Sterowanie wyświetlaniem komunikatów odpowiedzi o błędach - Control of Text Display of Error Reply Messages)
Komenda klienta FTP

Aby sterować ekranami odpowiedzi serwera FTP, należy użyć komendy klienta VERBOSE. Komenda VERBOSE przestawia przełącznik verbose. Gdy parametr verbose jest włączony, wyświetlane są pełne odpowiedzi serwera, łącznie z kodami odpowiedzi. Gdy jest on wyłączony, pewne odpowiedzi serwera i kody odpowiedzi nie są wyświetlane.

Verbose

Idź do:

- Komendy klienta FTP
- Konwencje składni komend klienta FTP

Programy obsługi wyjścia FTP



Klient i serwer FTP komunikują 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.

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 zapoznać się z sekcją Instalowanie i rejestrowanie programów obsługi wyjścia. Jeśli programy obsługi wyjścia nie są już potrzebne, należy je usunąć zgodnie z instrukcjami podanymi w sekcji Usuwanie programu obsługi wyjścia, aby przerwać ich funkcjonowanie 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
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_QTOD_SERVER_REQ	TFTP	X			

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.



Punkt wyjścia potwierdzenia żądania: klient i serwer

Punkty wyjścia potwierdzenia żądania mogą być wykorzystane do ograniczenia operacji dokonywanych przez użytkowników 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.

Uwaga:

Odkąd punkty wyjścia i klienta, i serwera FTP współużytkują ten sam format punktów wyjścia, wystarczy napisać pojedynczy program do obsługi ich obu.

Jeśli implementowany jest anonimowy użytkownik FTP, należy napisać program obsługi wyjścia potwierdzenia żądania serwera FTP, w celu ograniczenia uprawnień anonimowych użytkowników FTP do komend pobierania danych i zabronienia im uruchamiania komend CL.

Co powinien zawierać program:

- obsługę wyjątków,
- debugowanie,
- protokołowanie.

Akceptowane i odrzucone komendy

Program obsługi wyjścia potwierdzenia żądania serwera 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:

1. Tworzenie katalogu/biblioteki
2. Usuwanie katalogu/biblioteki
3. Ustawianie bieżącego katalogu
4. Wyświetlanie nazw plików
5. Usuwanie plików
6. Wysyłanie plików
7. Otrzymywanie plików
8. Zmiana nazwy pliku
9. Wykonanie komendy CL

Aby na stałe i bezwarunkowo odrzucić 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 umiał obsłużyć, to serwer FTP przerwie sesję.

Przykładowe programy

Poniżej udostępniono przykładowe programy ułatwiające konfigurowanie anonimowego FTP na serwerze. Programy te są tylko ilustracją. Zawierają one za mało opcji, aby można je było uruchomić na maszynie produkcyjnej. Przykłady te mogą posłużyć jako punkt wyjścia do pisania własnych programów. Kopiując części kodu z przykładów można je dodać do tworzonych programów. Zaleca się uruchamianie programów przykładowych na serwerze innym niż produkcyjny.

Przykład: kod programu obsługi wyjścia potwierdzenia żądania klienta lub serwera FTP w języku CL
Przykład: kod programu obsługi wyjścia potwierdzenia żądania serwera FTP w ILE RPG

Zastrzeżenia dotyczące kodu źródłowego przykładów

Firma IBM przyznaje użytkownikowi niewyłączną licencję na prawa autorskie do korzystania z wszystkich kodów źródłowych przykładów, z których można wygenerować podobną funkcję, dopasowaną do własnych specyficznych potrzeb.

Wszystkie przykładowe kody zostały dostarczone przez firmę IBM jedynie w celach ilustracyjnych. Przykłady te nie zostały gruntownie przetestowane. Dlatego IBM nie gwarantuje niezawodności, funkcjonalności ani prawidłowego działania tych programów.

Wszelkie zawarte tutaj programy są dostarczane w stanie w jakim się znajdują ("AS IS") bez udzielania jakichkolwiek gwarancji. Domniemane gwarancje nienaruszalności praw, przydatności handlowej oraz użyteczności do określonego celu są wyraźnie odrzucone.

Przykład: kod programu obsługi wyjścia potwierdzenia żądania klienta lub serwera FTP w języku

CL: Przedstawiony przykład jest prostym programem obsługi wyjścia potwierdzenia żądania FTP. Został on napisany w języku komend CL serwera iSeries. Kod tego programu nie jest kompletny, ale stanowi podstawę do tworzenia własnego programu obsługi punktu wyjścia klienta lub serwera.

Uwaga: Aby zapoznać się z informacjami prawnymi, należy przeczytać sekcję Informacje dotyczące zastrzeżeń odnoszących się do kodu.

(Uprzednio sformatowany w poniższym przykładzie tekst nie mieści się w ramce.)

```
/*
*****
/*
/*      Przykład programu obsługi wyjścia potwierdzenia żądania serwera FTP      */
/*      dla anonimowego 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 +
                &IPLLENIN &OPINFORIN &OPLLENIN &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(&IPLLENIN) TYPE(*CHAR) LEN(4) /* Długość adresu IP                */
DCL          VAR(&OPLLENIN) TYPE(*CHAR) LEN(4) /* Długość informacji właściwych dla operacji */
DCL          VAR(&OPINFORIN) 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(&IPLLEN)   TYPE(*DEC)  LEN(5 0)
DCL          VAR(&IPADDR)   TYPE(*CHAR)
DCL          VAR(&OPLLEN)   TYPE(*DEC)  LEN(5 0)
DCL          VAR(&OPINFOR)  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 QLGCVCS (w przypadku */
/* konwersji na wielkie litery z zależności od zadania CCSID                  */
DCL          VAR(&CASEREQ)  TYPE(*CHAR)  LEN(22) +
                VALUE(X'000000010000000000000000000000000000000000000000+
                00000000')
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(&IPLLEN)     VALUE(%BINARY(&IPLLENIN))
CHGVAR      VAR(&IPADDR)     VALUE(%SUBSTRING(&IPADDRIN 1 &IPLLEN))
CHGVAR      VAR(&OPLLEN)     VALUE(%BINARY(&OPLLENIN))
/* Obsługa pola informacji właściwej dla operacji (która jest długością zmiennej) */
IF          COND(&OPLLEN = 0) THEN(CHGVAR VAR(&OPINFO) +
                                VALUE(' '))
ELSE       CMD(CHGVAR VAR(&OPINFO) VALUE(%SST(&OPINFOIN +
                                1 &OPLLEN)))

/* 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 +
                                &OPLLENIN &ERROR)
/* Uwaga: należy sprawdzić katalog "/public" jako taki 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 serwera FTP. Jest on napisany w języku programowania ILE RPG. Kod tego programu nie jest kompletny, ale jest punktem wyjścia do tworzenia własnego programu.

Uwaga: Aby zapoznać się z informacjami prawnymi, należy przeczytać sekcję Informacje dotyczące zastrzeżeń odnoszących się do kodu.

(Uprzednio sformatowany w poniższym przykładzie tekst nie mieści się w ramce.)

```
* Opis modułu *****
*
*                               FUNKCJA PROGRAMU
*
* Program ten demonstruje kilka możliwości, które może mieć klient *
* FTP i program obsługi wyjścia potwierdzenia żądania serwera 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('CLRSVAF ITS0IC400/TURVIS')
D SaveLib         C          CONST('SAVLIB LIB(ITS0IC400) -
D                               DEV(*SAVF) -
D                               SAVF(ITS0IC400/TURVIS)')
*
* Wartość używana jako wyzwalacz konia trojańskiego
*
D Savetti         C          CONST('ITSOIC400.LIB/TURVIS.FILE')
*
*
*
*
* 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)
```

Rozszerzeniem jest FILE, mimo że powinno być SAVF (tak jak to wprowadził użytkownik)

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
(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 wszystkich zatwierdzanych żądań klienta *
*****
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: została pozostawiona furtka umożliwiająca wykonanie
* wszystkich operacji. Jeśli używa się tego programu do ochrony
* systemu, należy usunąć tę możliwość!
*
C          OTHER
C          Z-ADD      AlwaysAllw      ALLOWOP
C*****      Z-ADD      NeverAllow    ALLOWOP
C          ENDSL
*
C          ENDSR
C/EJECT
*****
* Obsługa zatwierdzeń wszystkich żądań serwera FTP *
*****
C  ServerRqs    BEGSR
*
* Sprawdzanie, czy użytkownik 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
C      Library        OREQ      PublicLib
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
C      Wysłanie plików do klienta
*
* Jeśli klient wysłał GET dla zbioru składowania HESSU w bibliotece, to nastąpi odświeżenie zawartości
*
*
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
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
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 do potwierdzenia żądania aplikacji serwera FTP jest:

QIBM_QTMF_SERVER_REQ

Punktem wyjścia do potwierdzenia żądania aplikacji klienta FTP jest:

QIBM_QTMF_CLIENT_REQ

Interfejsem sterującym formatem parametrów dla tego punktu wyjścia jest:

VLRQ0100

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 (10)
5	Długość zdalnego adresu IP	Wejściowy	Binary (4)
6	Informacje właściwe dla operacji	Wejściowy	Char (*)
7	Długość informacji właściwych dla operacji	Wejściowy	Binary (4)
8	Pozwolenie 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. Możliwymi wartościami są:

0	Program klienta FTP
1	Program serwera FTP
2	Program serwera REXEC
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, to możliwe są poniższe wartości:

Wartość	ID operacji	Komenda klienta	Komenda serwera
0	Uruchomienie sesji	Open, SECOpen	Nowe połączenie
1	Utworzenie katalogu/biblioteki	*	MKD, XMDK
2	Usunięcie katalogu/biblioteki	*	RMD, XRMD
3	Ustawienie bieżącego katalogu/biblioteki	LCD	CWD, CDUP, XCWD, XCUP
4	Wyświetlenie listy plików	*	LIST, NLIST
5	Usunięcie pliku	*	DELE
6	Wysłanie pliku	APPEND, PUT, MPUT	RETR
7	Pobranie pliku	GET, MGET	APPE, STOR, STOU
8	Zmiana nazwy pliku	*	RNFR, RNT0

Wartość	ID operacji	Komenda klienta	Komenda serwera
9	Wykonanie komendy CL	SYSCMD	RCMD, ADDm, ADDV, CRTL, CRTP, CRTS, DLTF, DLTL

Uwaga:

Symbol * 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. Parametr ten jest w formacie dziesiętnym rozdzielonym kropkami (123.45.67.89), wyrównany w lewo. 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 żadaną 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 identyfikatora 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 identyfikatora 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

Informacja właściwa dla operacji zawiera komendę CL serwera iSeries, której żąda użytkownik.

Aby uzyskać więcej informacji, można zapoznać się także z następującą sekcją Uwagi dotyczące użycia formatu punktu wyjścia VLRQ0100.

VLRQ0100 Parametr 7:

Długość informacji właściwej 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. Możliwymi wartościami są:

-1	<i>Nieprzyjmowanie</i> 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	Pozwolenie na operację
2	<i>Każdorazowe przyjmowanie</i> tego identyfikatora operacji: Bezwarunkowe przyjęcie identyfikatora operacji na pozostałą część bieżącej sesji. Ten identyfikator operacji nie wywoła ponownie programu obsługi wyjścia.

Uwagi dotyczące użycia formatu punktu wyjścia VLRQ0100: VLRQ0100 jest formatem punktu wyjścia używanym zarówno przez Punkt wyjścia potwierdzania żądania klienta FTP, jak i przez Punkt wyjścia potwierdzania żądania serwera FTP.

Nieprawidłowe 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 do punktu wyjścia &1 nie zostały podane lub są niepoprawne)

Wyjątki

Jeśli podczas wywołania programu obsługi wyjścia serwer FTP napotka jakiegokolwiek 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 zbiorów QSYS.LIB składają się zawsze z wielkich liter,

^(b) - w nazwach ścieżek systemu plików QOpenSys mogą występować małe i wielkie litery i są one rozróżniane.

Punkt wyjścia logowania do serwera

Uwierzytelnianiem użytkowników serwera aplikacji TCP/IP można sterować za pomocą punktu wyjścia logowania do serwera aplikacji TCP/IP. Ten punkt wyjścia umożliwia dostęp do serwera w oparciu o adres 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 wywołuje go przy każdej próbie logowania się do serwera. Program obsługi wyjścia ustawia parametr wyjściowy kodu powrotu wskazujący, czy serwer będzie kontynuował operację logowania. Możliwe są różne kody powrotu dla przetwarzania logowania i inicjowania informacji o katalogach.

Punktem wyjścia systemu iSeries dla operacji logowania do serwera FTP jest:

QIBM_QTMF_SVR_LOGON

Dostępne są trzy formaty punktu wyjścia programu obsługi 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 TCPL0300 punktu wyjścia rozszerza format TCPL0200 o możliwość obsługi rozszerzonego hasła OS/400 oraz udostępnia dodatkowe parametry umożliwiające przetwarzanie identyfikatora CCSID dla

hasła i pól nazw katalogów; gdy 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.

Dla anonimowych użytkowników FTP należy napisać własny program obsługi wyjścia logowania do serwera, obsługujący:

1. Akceptowanie logowania od użytkowników o identyfikatorze ANONYMOUS.
2. Żądanie adresu poczty elektronicznej (e-mail) jako hasła. Można wybrać żądanie podania "poprawnego adresu e-mail" jako hasła. Termin ten jest mylący, ponieważ kryterium poprawności zastosowanym przez program obsługi wyjścia może być jedynie sprawdzenie, czy w środku łańcucha alfanumerycznego występuje symbol @. Zwykle tak jest. Dlatego ważne jest protokołowanie adresu IP użytkownika.
3. Sprawdzenie, czy symbol @ występuje w łańcuchu hasła.
4. 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,
- logowanie,
 - 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, to 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

Poniżej udostępniono przykładowe programy ułatwiające konfigurowanie anonimowego FTP na serwerze. Programy te są tylko ilustracją. Zawierają one za mało opcji, aby można je było uruchomić na maszynie

produkcyjnej. Przykłady te mogą posłużyć jako punkt wyjścia do pisania własnych programów. Kopiując części kodu z przykładów można je dodać do tworzonych programów. Zaleca się uruchamianie programów przykładowych na serwerze innym niż produkcyjny.

Przykład: kod programu obsługi wyjścia logowania do serwera FTP w języku CL

Przykład: kod programu obsługi wyjścia logowania do serwera FTP w języku C

Przykład: kod programu obsługi wyjścia logowania do serwera FTP w języku ILE RPG

Zastrzeżenia dotyczące kodu źródłowego przykładów

Firma IBM przyznaje użytkownikowi niewyłączną licencję na prawa autorskie do korzystania z wszystkich kodów źródłowych przykładów, z których można wygenerować podobną funkcję, dopasowaną do własnych specyficznych potrzeb.

Wszystkie przykładowe kody zostały dostarczone przez firmę IBM jedynie w celach ilustracyjnych. Przykłady te nie zostały gruntownie przetestowane. Dlatego IBM nie gwarantuje niezawodności, funkcjonalności ani prawidłowego działania tych programów.

Wszelkie zawarte tutaj programy są dostarczane w stanie w jakim się znajdują ("AS IS") bez udzielania jakichkolwiek gwarancji. Domniemane gwarancje nienaruszalności praw, przydatności handlowej oraz użyteczności do określonego celu są wyraźnie odrzucone.

Przykład: kod programu obsługi wyjścia logowania do serwera FTP w języku CL: Przedstawiony przykład jest prostym programem obsługi wyjścia logowania do serwera FTP. Został on napisany w języku komend CL serwera iSeries. Kod tego programu nie jest kompletny, ale jest punktem wyjścia do tworzenia własnego programu.

Uwaga: Aby zapoznać się z informacjami prawnymi, należy przeczytać sekcję Informacje dotyczące zastrzeżeń odnoszących się do kodu.

(Uprzednio sformatowany w poniższym przykładzie tekst nie mieści się w ramce.)

```
/*
*****/
/*
/*      Przykład programu obsługi wyjścia logowania do serwera FTP          */
/*      Uwaga: Ten program jest tylko przykładem i nie przeszedł 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 &USRLIN &AUTIN &AUTLENIN +
                    &IPADDRIN &IPLIN &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(&USRLIN)   TYPE(*CHAR) LEN(4) /* Długość ID użytkownika   */
DCL      VAR(&AUTIN)    TYPE(*CHAR) LEN(999)/* Łańc. uwierzytelniający */
```

```

DCL      VAR(&AUTLENIN)  TYPE(*CHAR) LEN(4) /* Dł. łańc. uwierzyteln. */
DCL      VAR(&IPADDRIN)  TYPE(*CHAR) LEN(15) /* Adres IP klienta */
DCL      VAR(&IPLLENIN)  TYPE(*CHAR) LEN(4) /* Długość adresu IP */
DCL      VAR(&RETCDOOUT) 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(&IPLLEN)    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(&IPLLEN)    VALUE(%BINARY(&IPLLENIN))

/* Sprawdzenie, czy jest to użytkownik ANONYMOUS. Pozwolenie na dostęp */
/* 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(&RETCDOOUT)) VALUE(6)
CHGVAR  VAR(&USRPRFOUT) VALUE('ANONYMOUS ')
CHGVAR  VAR(&CURLIBOUT) VALUE('PUBLIC ')
ENDDO
/* Inni użytkownicy: wykonanie normalnego przetwarzania logowania */
ELSE    CMD(CHGVAR VAR(%BINARY(&RETCDOOUT)) VALUE(1))
ENDDO
ELSE    CMD(CHGVAR VAR(%BINARY(&RETCDOOUT)) 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: Aby zapoznać się z informacjami prawnymi, należy przeczytać sekcję Informacje dotyczące zastrzeżeń odnoszących się do kodu.

(Uprzednio sformatowany w poniższym przykładzie tekst nie mieści się w ramce.)

```

/* Opis Modułu *****/
/*
/*****
/*
/* Uwaga: Ten program jest tylko przykładem i nie przechodził
/      formalnego przeglądu i testowania.
/*
/*****
/*
/* Nazwa pliku źródłowego: qtmfsvr1gn.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.                */
/*                          qtmfsvrln - Funkcja programu obsługi wyjścia */
/*                          logowania do serwera FTP.                */
/*                          CheckClientAddress - Sprawdzanie adresu IP */
/*                          inicjowanej sesji.                       */
/*  */
/* Koniec opisu modułu *****/
#define _QTMFSVRLGN_C

/*****/
/*Wszystkie pliki nagłówkowe w zakresie całego pliku znajdują się tu */
/*****/
#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" /* Plik nagłówkowy dla struktury kodów*/
/* błędów interfejsu API */
#include "qsyrusri.h" /* Plik nagłówkowy dla informacji */
/* użytkownika interfejsu 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 makr w zakresie całego pliku znajdują się tutaj*/
/*****/

/*****/
/* Wszystkie prototypy funkcji wewnętrznych znajdują się tutaj. */
/*****/

```

```

/*****/
static void qtmfsvrlogn
    (int,char *,int,char *,int,char *,int,int *,char *,char *,char *);

static int CheckClientAddress(char *, int);

/*****/
/* Wszystkie deklaracje zmiennych w zakresie całego pliku znajdują się tutaj. */
/*****/

/*****/
/*
    ** UWAGA **
*/
/* Poniższy adres IP klienta jest tylko przykładowy. Jakikolwiek podobieństwo
/* do adresu IP rzeczywistego systemu jest przypadkowe.
*/
/*****/
/* WYKLUCZAJĄCA lista systemowa - Próba logowania spod adresu IP klienta NIE
/* znajdującego się na liście 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 FTP
/* "anonymous".
*/
/*
/* 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/makra:
*/
/*
/* qtmfsvrlogn - Funkcja obsługi wyjścia logowania do serwera
*/
/*

```

```

/* Wejście: */
/* int * argv[1] - Identyfikuje aplikację dokonującą żądania */
/* (Klient FTP = 0, Serwer FTP = 1). */
/* char * argv[2] - Identyfikator użytkownika z programu klienta. */
/* (Dla serwera FTP są 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 użytkownika (otrzymywany 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,
/* początkowej 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 się do serwera aplikacji FTP. */
    /* *****/
    qtmfsvrlnn*((int *) (argv[1])), /* Identyfikator aplikacji */
    /* (Wejściowy) */
    argv[2], /* Identyfikator użytkownika (Wejściowy) */
    *((int *) (argv[3])), /* Długość identyfikatora użytkownika */
    /* (Wejściowy) */
    argv[4], /* Łańcuch uwierzytelniający (Wejściowy) */
    *((int *) (argv[5])), /* Długość łańcucha uwierzytelniającego */
    /* (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: qtmfsvrlnn
/*
/* 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/makra:                                    */
/*                                                                    */
/*      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 bufora.                   */
/*                                                                    */
/*      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 AppId)
    {
        /* 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 jako 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 */
        /* nieznanego 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 qtmfsvr1gn.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/makra:
/*     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 nie
/*                             dozwolony 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)|| /* Pierwszy znak */
      /* '.' w IP
      (strspn(ClientIPAddr_p, " ") EQ 1) /* Pierwszy znak */
      /* pusty w 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
      /* na liście "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: Aby zapoznać się z informacjami prawnymi, należy przeczytać sekcję Informacje dotyczące zastrzeżeń odnoszących się do kodu.

(Uprzednio sformatowany w poniższym przykładzie tekst 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('!0.')
C/EJECT
*****
* DEFINICJE ZMIENNYCH I LISTY UŻYWANE PRZEZ PROGRAM              *
*****
*                               C/SPACE 2                          *
*                                                                    *
* Definicje parametrów binarnych                                  *
*                                                                    *
D APPIDds          DS
D USRLENds         5      4B 0
D AUTLENds         9      8B 0
D IPLENds          13     12B 0
D RETCDds          17     16B 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           USRLENIN         999   ID użytkownika
C PARM           AUTIN            999   Długość ID użytkownika
C PARM           AUTLENIN         999   łań. uwierzytelniający
C PARM           IPADDRIN         15    Dł. łań. uwierzytelniającego
C PARM           IPLENIN         15    Adres IP klienta
* Parametry zwracane:
C PARM           RETCDOUT         15    Długość adresu IP
*                               15      Kod powrotu (Wyjście)

```



```

C      TheNet      IFEQ      InvalidNet      Błędna sieć
C      Z-ADD      0          RETCDOUT      Odrzucenie próby logowania
C      ELSE
C      Z-ADD      1          RETCDOUT      Poprawna sieć
C      ENDIF      Kontynuacja logowania
*
C      ENDIF
*
C      EVAL      *INLR = *ON
C      RETURN

```

Format TCPL0100 punktu wyjścia:

Nazwa formatu punktu wyjścia: TCPL0100

Nazwa punktu wyjścia: QIBM_QTMF_SVR_LOGON

Nazwa punktu wyjścia: QIBM_QTMX_SVR_LOGON

Grupa wymaganych parametrów:

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	Kod powrotu	Wyjściowy	Binary(4)
9	Profil użytkownika	Wyjściowy	Char(10)
10	Hasło	Wyjściowy	Char(10)
11	Początkowa biblioteka bieżąca	Wyjściowy	Char(10)

Opis parametrów

Identyfikator aplikacji INPUT; BINARY(4) Identyfikuje serwer aplikacji, z którego wysłano 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 komendy PASS (hasło). Podczas rozpoczynania pracy z systemem V5R1, jeśli uwierzytelnianie użytkownika zostało wykonane przez certyfikat klienta, ten parametr jest pusty.

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 początkowej 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 przesłane 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 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 przesyłane 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 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 przesyłany 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: Podanie tej wartości przesłoni normalne przetwarzanie hasła w OS/400. Jest to jedyne uwierzytelnianie hasła.

6

Akceptacja operacji logowania. Profil użytkownika oraz początkowa biblioteka bieżąca są przesyłane przez odpowiednie parametry wyjściowe zwrócone przez program obsługi wyjścia. Parametr wyjściowy hasła jest ignorowany.

Uwaga: Podanie tej wartości przesłoni normalne przetwarzanie hasła w OS/400. 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.

Idź do:

- Uwagi dotyczące używania formatu TCPL0100

Warto także zapoznać się z następującymi informacjami:

- format TCPL0200: ten punkt wyjścia udostępnia dodatkowe parametry sterowania procesem logowania,
- format TCPL0300: ten punkt wyjścia identyfikuje serwer aplikacji, z którego zostało wysłane żądanie,

- Punkt wyjścia logowania do serwera: Uwierzytelnianiem użytkowników serwera aplikacji TCP/IP można sterować za pomocą punktu wyjścia logowania do serwera aplikacji TCP/IP.

Uwagi dotyczące używania formatu TCPL0100: Dotyczy FTP; jeśli zwrócone parametry wyjściowe nie są poprawne, serwer FTP nie pozwala na kontynuację operacji. W tym wypadku serwer wysyła do protokołu zadania 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).

Dotyczy FTP; jeśli wystąpi jakikolwiek wyjątek podczas wywołania programu obsługi wyjścia, serwer FTP wysyła 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 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 do przetworzenia żądania logowania się.

Kod powrotu	Profil użytkownika (9)	Hasło (10)	Początkowa biblioteka (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 zwrócona
3	Wartość zwrócona	Wartość zwrócona	(Z profilu użytkownika)
4	Wartość zwrócona	Wartość zwrócona	Wartość zwrócona
5	Wartość zwrócona	Ignorowany	(Z profilu użytkownika)
6	Wartość zwrócona	Ignorowany	Wartość zwrócona

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 serwerze FTP (punkt wyjścia QIBM_QTMF_SVR_LOGON, identyfikator aplikacji 1), jeśli identyfikatorem użytkownika jest ANONYMOUS i punkt wyjścia dodaje program obsługi wyjścia, serwer 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, 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 REXEC wysyła 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 zadania 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:

Nazwa formatu punktu wyjścia: TCPL0200

Nazwa punktu wyjścia: QIBM_QTMF_SVR_LOGON

Grupa wymaganych parametrów:

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)

Opis 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 (jest pusty).

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.

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 przesyłane 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 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 przesyłany 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, to podanie tej wartości przesłania normalne przetwarzanie hasła w OS/400. 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. Informacje na temat poprawnego formatu tego parametru zawiera sekcja Format parametru informacji właściwej dla aplikacji.

Długość informacji właściwych dla aplikacji Wejściowy; Binary(4) Długość (w bajtach) informacji właściwej dla aplikacji.

Warto także zapoznać się z następującymi informacjami:

- Punkt wyjścia logowania do serwera: uwierzytelnianiem użytkowników serwera aplikacji TCP/IP można sterować za pomocą punktu wyjścia logowania do serwera aplikacji TCP/IP.

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

Przesunięcie dziesiętnie	Przesunięcie szesnastkowo	Typ	Pole
8	8	BINARY(4)	Początkowy format listy plików
12	C	BINARY(4)	Mechanizm ochrony sterowania połączeniem
16	10	BINARY(4)	Opcja szyfrowania połączenia danych
20	14	BINARY(2)	Mechanizm ochrony sterowania połączeniem
22	16	BINARY(2)	Zestaw algorytmów szyfrowania połączenia danych

Opis pól

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 CHGFTP i jest równoważne wykonaniu komendy SITE NAMEFMT 0 na serwerze FTP.

1

Użyj formatu nazewnictwa ścieżek. Ustawienie to odpowiada opcji NAMEFMT(*PATH) komendy CHGFTP 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 CHGFTP.

1

Jako początkowy bieżący katalog roboczy serwera FTP używany jest katalog osobisty. To ustawienie odpowiada opcji CURDIR(*HOMEDIR) komendy CHGFTP.

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

Należy użyć formatu listy plików serwera iSeries. Ustawienie to odpowiada opcji LISTFMT(*DFT) komendy CHGFTPA i jest równoważne wykonaniu komendy SITE LISTFMT 0 na serwerze FTP.

1

Należy użyć formatu listy plików systemu 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 gniazd (Sockets Layer - SSL); mechanizm określony przez klienta FTP w komendzie AUTH to TLS-P lub SSL.

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/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/TLS nie szyfruje domyślnie połączeń danych.)

Mechanizm ochrony sterowania połączeniem

Określa zestaw algorytmów szyfrowania SSL używanych do szyfrowania sterowania połączeniem dla sesji FTP. Wartości zestawu algorytmów szyfrowania są zdefiniowane w interfejsie API warstwy gniazd chronionych (Secure Sockets Layer - SSL). Więcej informacji dotyczących interfejsu API zawiera temat Interfejs API SSL w artykule Programowanie w Centrum informacyjnym iSeries.

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 zdefiniowane w funkcjach API dotyczących SSL. Więcej informacji dotyczących funkcji API zawiera temat Funkcje API dotyczące SSL w artykule Programowanie w Centrum informacyjnym iSeries.

Uwagi:

- Pole to jest ignorowane, jeśli mechanizm ochrony sterowania połączeniem ma wartość 0 lub opcja szyfrowania połączenia ma wartość -1.
- Ustawienie dla tego pola wartości innej niż 0 lub wartość określona 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.

Format TCPL0300 punktu wyjścia:

Nazwa formatu punktu wyjścia: TCPL0300

Nazwa punktu wyjścia: QIBM_QTMF_SVR_LOGON

Nazwa punktu wyjścia: QIBM_QTMX_SVR_LOGON

Grupa wymaganych parametrów:

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)

1	Identyfikator aplikacji	Wejściowy	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)

Opis 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 komendy PASS (hasło), chyba że uwierzytelnianie użytkownika zostało wykonane przez certyfikat klienta i w takim przypadku dla tego parametru przekazany 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. Łańcuch jest w formacie dziesiętnym, wyrównany w lewo.

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 przesłane 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 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 przesłany 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, to podanie tej wartości przesłania normalne przetwarzanie hasła w OS/400. 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 wartość systemowa QPWDLVL jest ustawiona na 0 lub 1 - można podać do 10 znaków; jeśli na 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 określonej 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 Wyjściowy; 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.

Informacja właściwa dla aplikacji

Wejściowy/Wyjściowy; Char(*) Informacja wykorzystywana do przesyłania ustawień logowania właściwych dla aplikacji. Informacje na temat poprawnego formatu tego parametru zawiera sekcja Format parametru informacji właściwej dla aplikacji.

Długość informacji właściwej dla aplikacji

Wejściowy; Binary(4) Długość (w bajtach) informacji właściwej dla aplikacji.

Warto także zapoznać się z następującymi informacjami:

- Punkt wyjścia logowania do serwera: uwierzytelnianiem użytkowników serwera aplikacji TCP/IP można sterować za pomocą punktu wyjścia logowania do serwera aplikacji TCP/IP.

Usuwanie programu obsługi wyjścia

Aby usunąć zainstalowany program obsługi wyjścia:

1. W wierszu komend systemu iSeries 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. Wpisz **8** w polu Opc na lewo od pozycji punktu wyjścia i naciśnij klawisz **Enter**.
4. Na ekranie **Praca z programem obsługi wyjścia** wpisz **4** (Usuń).
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.

Metody przesyłania danych

Przed rozpoczęciem przesyłania plików należy wybrać właściwy format ich przesyłania. Można użyć domyślnego formatu, ASCII lub podać inny format. ASCII jest standardem kodowania znaków w sieci Internet. EBCDIC jest standardem dla serwera iSeries. Odpowiedni format należy wybrać po uwzględnieniu poniższych wskazówek:

- Format ASCII służy do przesyłania plików, które zawierają tylko tekst (pliki "tekstowe").
- Format EBCDIC służy do przesyłania danych EBCDIC pomiędzy systemami obsługującymi typ 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 iSeries.

Po wybraniu formatu przesyłania plików, można rozpocząć przesyłanie plików za pomocą FTP.

Niżej wymienione sekcje zawierają dodatkowe informacje na temat specyficznych typów plików:

- Przesyłanie pomiędzy serwerami iSeries plików zawierających upakowane dane dziesiętne
- Przesyłanie zbiorów *SAVF
- Przesyłanie dokumentów QDLS
- Przesyłanie plików w systemach plików "root", QOpenSys i QLANSrv
- Przesyłanie plików za pomocą systemu plików QfileSvr.400
- Przesyłanie zbiorów Qsys.lib
- Uwagi dotyczące tworzenia zbiorów
- Konwersje CCSID

Przesyłanie pomiędzy serwerami iSeries plików zawierających upakowane dane dziesiętne



FTP nie obsługuje konwersji specjalnych formatów liczbowych, takich jak upakowane lub nieupakowane dane dziesiętne.

Przesyłanie pomiędzy serwerami iSeries upakowanych lub nieupakowanych danych dziesiętnych jest obsługiwane w trakcie wykorzystywania typu przesyłania TYPE I (BINARY) lub TYPE E (EBCDIC) w trybie transmisji BLOCK; wymienione rodzaje przesyłania wysyłają dane w zastanej postaci, bez jakiegokolwiek konwersji. Wyniki innych rodzajów przesyłania są nieprzewidywalne.

Przed przesyłaniem 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.

Zanim upakowane lub nieupakowane dane dziesiętne będą mogły być przesłane do lub z innej architektury systemowej (takiej jak S/390^R lub UNIX), należy dokonać konwersji do postaci możliwej do druku.



Przesyłanie zbiorów *SAVF



Zbiory *SAVF muszą być przesyłane jako obrazy, dlatego przed uruchomieniem komend GET lub PUT należy wywołać komendę FTP BINARY.

Podczas przesyłania zbioru *SAVF z użyciem formatu nazewnictwa 0, zbiór składowania musi być wcześniej utworzony w systemie odbierającym. Aby zwiększyć wydajność i zachować integralność, zalecane jest także wcześniejsze tworzenie zbiorów w innych sytuacjach.

Przesyłanie zbioru składowania może być przydatne tylko w przypadku, gdy serwerami wysyłającymi i odbierającymi są serwery iSeries, a to z tego względu, że zbiór ten ma format specyficzny dla systemu iSeries. Zbiór składowania może być wysłany do serwera innego niż iSeries i przechowywany tam w celu składowania. Taki zbiór może być przesłany później do serwera iSeries za pomocą FTP.

Przykład: przesyłanie zbioru *SAVF z systemu VM do serwera iSeries

Poniższy przykład przedstawia sposób przesyłania zbioru *SAVF z systemu VM do iSeries przy użyciu formatu NAMEFMT 0 i 1. Sesja FTP została już uruchomiona, komenda BINARY wywołana i określono format NAMEFMT 0.

Najpierw zbiór P162484 SAVF310L przesyłany jest z dysku A systemu VM do serwera iSeries. FTP systemu VM wymaga wstawienia kropki pomiędzy nazwą zbioru a typ pliku. Następnie podana zostaje nazwa zbioru P162484 w bibliotece P162484 systemu iSeries i określany jest parametr REPLACE, tak jakby zbiór był wcześniej utworzony, nawet jeśli nie był poprzednio używany. Korzystając z formatu NAMEFMT 0 należy pamiętać, że wcześniejsze utworzenie zbioru jest obowiązkowe.

Format NAMEFMT zostanie zmieniony na 1 i całe przesyłanie zbioru jest powtarzane z nowym formatem nazwy. W związku z tym, że plik istnieje po wykonaniu poprzedniego kroku, ponownie zostaje podany jest parametr REPLACE.

Uwagi:

- Jeśli przed przeprowadzeniem przesyłania za pomocą formatu NAMEFMT 0 nie utworzono wcześniej zbioru w systemie iSeries, przesyłanie będzie wyglądało na zakończone pomyślnie. Sprawdzenie zbioru w systemie iSeries pozwoli upewnić się, że utworzony został zbiór fizyczny (*PF), a nie zbiór składowania (*SAVF).
- W zależności od tego, jak zbiór *SAVF był wcześniej wysyłany do tego systemu, konieczne może być wykonanie przetwarzania wstępnego w systemie VM:
 - jeśli zbiór *SAVF był wysłany za pomocą FTP, wystarczy wywołać komendę GET, aby przesłać go z powrotem do serwera iSeries,
 - jeśli do wysłania zbioru *SAVF użyta została komenda Wysłanie pliku sieciowego (Send Network File - SNDNETF), najpierw trzeba dokonać konwersji zbioru, w systemie VM, z formatu rekordów o zmiennej długości (RECFM) na RECFM o stałej długości. Powinno się to zrobić zanim FTP zostanie użyty do przesłania zbioru z powrotem do serwera iSeries. Aby tego dokonać, należy w systemie VM użyć komendy COPYFILE. Na przykład:

```
COPYFILE P162484 SAVF310L A = = = (RECFM F
```

```
> GET P162484.SAVF310L P162484/P162484 (REPLACE
200 Żądanie portu OK.
150 Wysłanie zbioru 'P162484.SAVF310L'
250 Przesyłanie zakończone pomyślnie.
384912 bytes transferred in 3.625 seconds. Transfer rate 106.183 KB/sec

> namefmt 1
202 Komenda SITE nie jest wymagana; można kontynuować
Format NAMEFMT klienta to 1.
> GET P162484.SAVF310L/QSYS.LIB/P162484.LIB/P162484.savf (REPLACE
200 Żądanie portu OK.
150 Wysłanie zbioru 'P162484.SAVF310L'
250 Przesyłanie zakończone pomyślnie.
384912 bytes transferred in 3.569 seconds. Transfer rate 107.839 KB/sec
Wpisz komendę FTP.
====>
```

Rysunek 1. Przesyłanie zbioru *SAVF z systemu VM do serwera iSeries przy użyciu formatu NAMEFMT 0 i NAMEFMT 1.



Przesyłanie dokumentów QDLS



Kiedy przesyłany jest dokument QDLS, atrybut pozycji katalogu QDLS, który wskazuje na typ dokumentu, przyjmuje na odbierającym serwerze iSeries wartość domyślną równą PCFILE. Dotyczy to wszystkich typów dokumentów z wyjątkiem dokumentów z tekstem w formacie pośrednim (revisable-form text - 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



Kiedy w systemach plików "root", QOpenSys, QLANSrv, QDLS i QOPT przesyłane są pliki, 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. Pliki przesłane do systemu plików QLANSrv są znakowane stroną kodową zdefiniowaną w opisie serwera sieciowego, odpowiadającego katalogowi zawierającemu ten plik.

Konwersja danych oraz przypisania identyfikatora CCSID zmieniają się w zależności od wybranego trybu (TYPE). Dodatkowe informacje na ten temat znajdują się w sekcji Znakowanie strony kodowej CCSID dla plików serwera iSeries. TYPE E nie jest obsługiwany przez system plików QLANSrv.

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 pliku.



Przesyłanie plików za pomocą systemu plików QfileSvr.400



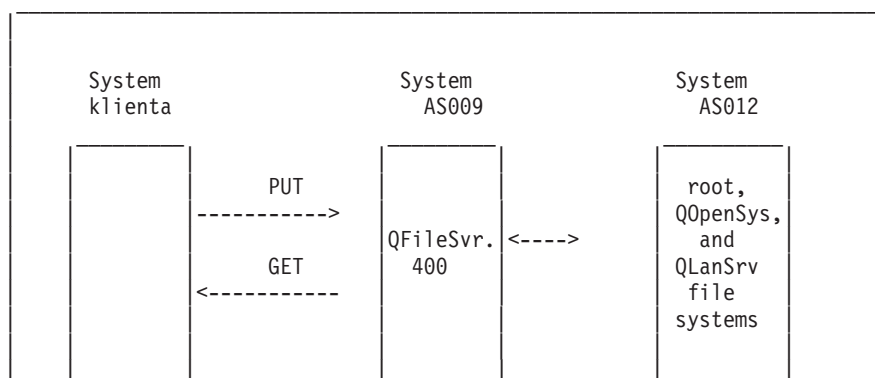
System plików QFileSvr.400 zapewnia dostęp do innych systemów plików w zdalnych serwerach iSeries. Obsługuje on przesyłanie plików w systemach plików "root", QOpenSys, QLANSrv, QDLS i QOPT. Nie umożliwia natomiast przesyłania plików w systemie QSYS.LIB.

W czasie przesyłania plików konieczne jest użycie trybu strumieniowego (MODE S) oraz struktury pliku (STRUCT F). Na rysunku 9-30 przedstawiono przesyłanie pliku FILE.ABC do i z trzech różnych systemów plików systemu AS012 za pomocą systemu plików QFileSvr.400 systemu AS009.

Po połączeniu z serwerem AS009 przesyłanie pliku realizują komendy klienta FTP.

Uwaga:

W systemach AS009 i AS012 identyfikator użytkownika oraz hasło muszą być takie same.



Rysunek 9-30. 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
CD /QFileSvr.400/AS012/QLANSrv/NWS/LANSRV/DSK/K/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
DELETE /QFileSvr.400/AS012/QLANSrv/NWS/LANSRV/DSK/K/FLSDIR/FILE.ABC
QUIT
```

Rysunek 9-31. Komendy wywoływane podczas przesłania plików za pomocą systemu plików QFileSvr.400



Przesyłanie zbiorów QSYS.LIB



Niżej przedstawione Tabela 1 i Tabela 2 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:

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 wysłanego 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 na ten temat można uzyskać za pomocą komendy iSeries Wyświetlenie opisu zbioru (Display File Description - DSPFD).

Automatyczne tworzenie zbioru w serwerze iSeries

W momencie otrzymania zbioru serwer iSeries automatycznie tworzy zbiór fizyczny, o ile jeszcze nie istnieje. Zaleca się, aby użytkownik wcześniej utworzył zbiór na serwerze.

Typy 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 podzbiórami, utworzyć zbiór za pomocą komend MGET i MPUT. Jeśli zbiór nie zostanie wcześniej utworzony, serwer FTP tworzy 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. Wsześniejsze utworzenie zbioru, z wielkością rekordu przystosowaną do wszystkich podzbiorów, zapobiegnie powstaniu takiego błędu.

Tabela 1: Tryb przesyłania strumieniowego dla systemu plików QSYS.LIB

Istnieje biblioteka	Istnieje zbiór	Istnieje podzbiór	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	Nie dotyczy	Nie dotyczy	Przesyłanie zostaje odrzucone i wysyłany jest komunikat.
Tak	Tak	Nie	Nie dotyczy	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	Nie dotyczy	Tak	Tak	Tworzony jest podzbiór, do którego zapisywane są dane.
Tak	Tak	Nie	Nie	Nie dotyczy	Nie	Przesyłanie zostaje odrzucone i wysyłany jest komunikat.

Istnieje biblioteka	Istnieje zbiór	Istnieje podzbiór	Wybrano zastąpienie	Długość rekordu jest zgodna	Wielkość zbioru jest zgodna	Rezultat
Tak	Nie	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy	Tworzony jest zbiór z długością rekordu równą maksymalnej długości rekordu przysłanego zbioru. Tworzony jest podzbiór, do którego zapisywane są dane.
Nie	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy	Nie dotyczy	Przesyłanie zostaje odrzucone i wysyłany jest komunikat. Należy użyć komendy CRTLIB do utworzenia biblioteki na zdalnym serwerze iSeries.

Tabela 2: Tryb przesyłania obrazów dla systemu plików QSYS.LIB

Istnieje biblioteka	Istnieje zbiór	Istnieje podzbiór	Wybrano zastąpienie	Rezultat
Tak	Tak	Tak	Tak	Dane zapisane w podzbiórze.
Tak	Tak	Tak	Nie	Przesyłanie zostaje odrzucone i wysyłany jest komunikat.
Tak	Tak	Nie	Nie dotyczy	Tworzony podzbiór i dane
Tak	Nie	Nie dotyczy	Nie dotyczy	
Nie	Nie dotyczy	Nie dotyczy	Nie dotyczy	



Otrzymywanie plików tekstowych w systemie plików QSYS.LIB:



Ponieważ system plików iSeries QSYS.LIB wewnętrznie obsługuje strukturę rekordów, serwer FTP iSeries przekształca otrzymane pliki w strukturę rekordów, a pliki wysłane z serwera iSeries w strukturę plików FTP. Pliki tekstowe otrzymane przez serwer iSeries są przekształcane przez FTP w strukturę rekordów przez FTP w następujący sposób:

- kiedy FTP otrzymuje zbiór, a taki zbiór już istnieje w serwerze iSeries, wykorzystywana jest długość rekordu istniejącego zbioru,
- kiedy FTP tworzy nowy zbiór, wykorzystuje długość (wykluczając spacje) najdłuższego wiersza lub rekordu zbioru jako długość rekordu.

Pliki tekstowe wysyłane z serwera iSeries przez FTP są przekształcane w strukturę plików poprzez usunięcie odstępów z każdego wiersza lub rekordu i wysłanie przyciętego rekordu.



Uwagi dotyczące tworzenia zbiorów



Zbiory, które będą przesyłane do systemu plików QSYS.LIB systemu iSeries, powinno się utworzyć wcześniej. Dzięki temu dane będą przesłane bez ich naruszania, wiarygodnie i z dużą wydajnością.

Należy się upewnić, że dla całego zbioru przydzielono wystarczającą ilość rekordów. W systemie iSeries służy do tego parametr 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 komendy QUOTE. Natomiast w systemie klienta FTP za pomocą komendy SYSCMD.



Konwersje CCSID



Serwer iSeries korzysta z informacji identyfikatora CCSID (Coded Character Set Identifier) do interpretowania danych wejściowych i udostępniania danych wyjściowych do wyświetlenia we właściwym formacie. Danymi wejściowymi mogą być dane typu ASCII lub EBCDIC. Niżej wymienione sekcje zawierają szczegółowe informacje na temat konwersji CCSID:

- Określanie tabel odwzorowań
- Znakowanie strony kodowej CCSID dla plików serwera iSeries
- Uwagi dla FTP dotyczące obsługi języków narodowych



Określanie tabel odwzorowań:



Tabele odwzorowań ASCII dla klienta FTP podaje się 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 **PF4**. Pojawi się ekran **Uruchomienie przesyłania plików TCP/IP** (Start TCP/IP File Transfer (FTP)).
3. Naciśnij **F10**. Wyświetlą się podpowiedzi dla wychodzących i przychodzących tabel ASCII/EBCDIC.

```

                Uruchomienie przesyłania plików TCP/IP
                (Start TCP/IP File Transfer (FTP))
Podaj wybór, naciśnij klawisz Enter.

System zdalny . . . . .

Adres internetowy . . . . .
Identyfikator kodowanego zestawu znaków      *DFT      1-65533, *DFT

                Parametry dodatkowe

Wychodząca tabela EBCDIC/ASCII .  *CCSID      Nazwa, *CCSID, *DFT
Biblioteka . . . . .                Nazwa, *LIBL, *CURLIB
Przychodząca tabela ASCII/EBCDIC *CCSID      Nazwa, *CCSID, *DFT
Biblioteka . . . . .                Nazwa, *LIBL, *CURLIB

                Dół
F3=Wyjście  F4=Podpowieź  F5=Odśwież  F12=Anuluj  F13=Jak używać ekranu
F24=Więcej klawiszy

```

Rysunek 1. 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). Wartość CCSID można także określić zarówno dla przesyłań przychodzących, jak i wychodzących. Zastosowanie wartości CCSID zostało omówione w sekcji Uwagi dla FTP dotyczące obsługi języków narodowych.

Uwagi:

- Dla parametru CCSID komendy CHGFTP wartości CCSID zestawu znaków dwubajtowych (DBCS) są niedopuszczalne. Wartości CCSID DBCS mogą być określone za pomocą komendy TYPE (Określenie typu przesyłania plików - Specify File Transfer Type).
- Firma IBM dodaje obsługę odwzorowań w FTP, aby zapewnić kompatybilność z wydaniem wcześniejszymi niż V3R1. Użycie tabel odwzorowań dla przychodzących przesyłań plików TYPE A, wynika z utraty znakowania CCSID, kiedy tworzony jest plik docelowy. Firma IBM zaleca stosowanie obsługi CCSID dla zwykłych operacji.



Znakowanie strony kodowej CCSID dla plików serwera iSeries:



Kiedy FTP tworzy na serwerze iSeries nowy plik, jest on znakowany identyfikatorem CCSID lub stroną kodową tego identyfikatora, aby móc identyfikować znajdujące się w nim dane znakowe. Podczas zastępowania lub dopisywania danych do istniejącego pliku, znacznik pliku nie jest zmieniany. Poniższa tabela prezentuje, w jaki sposób FTP przypisuje te wartości różnym systemom plików i różnym rodzajom przesyłania.

Tabela 1: Znakowanie strony kodowej CCSID dla plików iSeries

System plików odbierający	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 ccoid jest typu ASCII, wtedy odpowiednio domyślnie EBCDIC CCSID.	65535	65535
"root", QOpenSys, QDLS, QOPT	Domyślny identyfikator CCSID równy ASCII.	Wartość 'ccoid' określona w komendzie TYPE C numer_ccoid.	Identyfikator CCSID zadania jeśli nie jest to 65535. Jeśli identyfikator CCSID zadania to 65535, przypisywany jest domyślny CCSID zadania.	Domyślny identyfikator CCSID równy ASCII.
QLanSrv	Strona kodowa ASCII opisu serwera sieciowego dla katalogu plików.	Strona kodowa ASCII opisu serwera sieciowego dla katalogu plików.	Nie obsługiwane.	Strona kodowa ASCII opisu serwera sieciowego dla katalogu plików.

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 CHGFTP. Przypisania pliku w systemie QFileSvr.400 zależą od systemu plików otrzymującego ten plik.



Uwagi dla FTP dotyczące obsługi języków narodowych:



Podczas korzystania z FTP w środowisku z różnymi językami podstawowymi należy uwzględnić poniższe uwagi.

- Jeśli dane są przesyłane z użyciem TYPE E (lub EBCDIC), to są składowane w niezmienionej postaci, więc będą miały stronę kodową EBCDIC pliku, z którego pochodzą. Może to spowodować przypisanie do pliku nieprawidłowego identyfikatora CCSID, jeśli języki podstawowe dwóch serwerów iSeries są różne.

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 docelowy już istnieje, wtedy dane będą zapisane w niezmienionej postaci z CCSID istniejącego zbioru, która może nie 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 TCP3C14: Unable to convert data from CCSID &1 to CCSID &2 (Niemożliwa konwersja z identyfikatora CCSID &1 na CCSID &2). 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. Identyfikator CCSID 850, który zawiera kodowany zestaw znaków IBM Personal Computer Latin-1, jest identyfikatorem CCSID ASCII, dla którego możliwe są konwersje do wszystkich prawidłowych wartości CCSID.
- 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 napotyka się trudności, 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. Także 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 ta, która jest w systemie wysyłającym zbiór.



Systemy plików i konwencje nazewnictwa

Serwer FTP organizuje jednostki informacji systemu plików w struktury wielowarstwowe, podobne do drzewa.

Systemy plików OS/400 obsługiwane przez protokół FTP zależą od wersji serwera iSeries. Systemy plików w systemie OS/400 mogą używać innych terminów dla danych i ich struktur hierarchicznych.

Konwencje nazewnictwa

Każdy system plików OS/400 ma własny 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 OS/400 obsługiwanych przez FTP opisane są w książce IFS (Zintegrowany system plików). Więcej informacji znajduje się w sekcji Systemy plików i zarządzanie nimi. Informacje dotyczące nazewnictwa plików w serwerach innych niż iSeries może dostarczyć serwer. W tym celu należy wpisać komendę QUOTE HELP.

Parametr NAMEFMT serwera FTP

Kiedy uruchamiana jest sesja serwera FTP, parametr NAMEFMT przyjmuje wartość "0". Wartość NAMEFMT można zmienić za pomocą komendy SITE.

Serwer automatycznie przełącza wartość domyślną parametru NAMEFMT z 0 na 1, kiedy "pierwszy" parametr pliku lub nazwy ścieżki otrzymany z komendą:

- zaczyna się znakiem ukośnika (/) lub tyldy (~) albo
- jest pusty (z wyjątkiem komend LIST i NLST).

Późniejsze komendy serwera, zawierające parametr pliku lub nazwy ścieżki, nie wpłyną na wartość parametru NAMEFMT. Dodatkowo, poza zmianą wartości parametru NAMEFMT, odpowiedź serwera na komendę będzie zawierała komunikat informujący o zmianie jej wartości.

Na przykład wartość NAMEFMT serwera zmieni się na "1", jeśli pierwszą komendą serwera zawierającą plik lub nazwę ścieżki jest:

```
CWD /DIR1/DIR2A
```

Odpowiedź serwera będzie miała postać:

```
250-NAMEFMT ustawione na 1.  
250 Bieżący katalog został zmieniony na /DIR1/DIR2A.
```

Uwaga:

Umożliwia to typowej przeglądarce WWW, która wymaga ustawienia NAMEFMT na 1, współdziałanie z serwerem FTP iSeries, bez potrzeby wydawania komendy SITE NAMEFMT 1.

Dodatkowe informacje na temat NAMEFMT zawiera sekcja Systemy plików i konwencje nazewnictwa.

Instrukcje dotyczące używania komendy NAMEFMT w pracy z systemami plików zawiera sekcja NAMEFMT (Wybranie formatu nazewnictwa plików - Select File Naming Format).

Systemy plików OS/400 obsługiwane przez protokół FTP

Systemy plików obsługiwane przez protokół FTP różnią się w zależności od wersji wydania serwera iSeries.

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.

Bazowy system plików ("root")

System plików /. Ten system plików wykorzystuje w pełni możliwość obsługi plików strumieniowych i hierarchiczną strukturę katalogów zintegrowanego systemu plików. Ma on cechy systemów plików DOS i OS/2^R.

System plików QOpenSys

System plików systemów otwartych. Jest on zgodny ze standardami systemów otwartych opartych na systemie UNIX, takich jak POSIX i 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.

System plików 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 OS/400. Zapewnia dostęp do innych systemów plików, które znajdują się w zdalnych serwerach iSeries. Protokół FTP nie udostępnia QSYS.LIB, QDLS ani QOPT, które używają systemu plików QFileSvr.400.

Aby uzyskać pełne informacje o systemach plików obsługiwanych przez protokół FTP, należy zapoznać się z dokumentem Zintegrowany system plików.

Komunikaty o statusie odpowiedzi serwera FTP

Po wpisaniu komendy w sesji klienta FTP komunikaty o statusie zwracane są przez serwer za pomocą 3-cyfrowego kodu: xyz.

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 nie przyjął komendy. 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 w relacji z żądaniami przesyłania plików.

Trzecia cyfra (z) określa wyższy poziom szczegółów informacji o kategorii funkcjonalnej.

Najczęściej spotykane kody odpowiedzi i ich znaczenie zostały opisane poniżej. Tekst komunikatu może być różny dla różnych serwerów.

Kod	Znaczenie
110	Restart od znacznika
120	Usługa będzie gotowa w ciągu nnn minut
125	Połączenie danych jest już otwarte; rozpoczyna się przesyłanie
150	Uruchomienie pliku OK; otwieranie 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	Łącze danych jest zamykane; działanie na pliku pomyślnie zakończone
230	Użytkownik zalogowany
250	Działanie na pliku pomyślnie zakończone; działanie zakończone
257	Utworzono nazwę ścieżki
331	Wymagane hasło
332	Wymagane konto
425	Nie można otworzyć łącza danych

Kod	Znaczenie
426	Połączenie zamknięte; przesyłanie zakończone niepomyślnie
450	Żądane działanie na pliku nie zostało podjęte; plik jest zajęty
451	Żądane działanie nieprawidłowo przerwane; 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
503	Zła sekwencja komend
504	Komenda nie została zaimplementowana dla tego parametru
530	Próba wpisania się do systemu została odrzucona
532	Do przechowywania plików wymagane konto
550	Żądane działanie nie zostało podjęte; plik nie znaleziony (lub brak dostępu)
551	Żądane działanie nieprawidłowo przerwane; nieznan typ strony
552	Żądane działanie na pliku nieprawidłowo przerwane; przekroczono przypisaną pojemność pamięci
553	Żądane działanie nie zostało podjęte; niedozwolona nazwa pliku

Konwencje składni komend serwera FTP

Komendy serwera FTP opisane w tej sekcji wykorzystują następujące konwencje 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 (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

Komendy klienta FTP opisane w tej sekcji wykorzystują następujące konwencje 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.

Więcej informacji dotyczących składni:

- Umieszczanie parametrów komend: odsyłacz do informacji o zaznaczaniu parametrów za pomocą apostrofów (') lub cudzysłówów (").
- Nazwy plików dla komend klienta służących do przesyłania danych: odsyłacz do informacji o domyślnych nazwach plików.
- Nazwy plików do przesyłania: odsyłacz do informacji o parametrach plik_lokalny i plik_zdalny.

Umieszczanie parametrów komend

Parametry komend można ująć w znaki apostrofu (') lub cudzysłowu ("). Aby umieścić apostrof w parametrze ujętym również w apostrofy, należy wpisać go jako dwa następujące po sobie apostrofy ("). Należy wpisać go jako pojedynczy apostrof w parametrze ujętym w cudzysłowy (").

Podobnie, jeśli cudzysłów (") ma znajdować się w parametrze, należy wpisać go w jeden z następujących sposobów:

- pojedynczy 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'
  oznaczają ABC'12"345
```

Więcej informacji dotyczących składni:

- Konwencje składni komend klienta FTP

Nazwy plików dla komend klienta służących do przesyłania danych

Jeśli nazwa pliku docelowego dla komend PUT, APPEND i GET nie zostanie podana, klient FTP używa domyślnych nazw plików. Ponieważ w komendach MPUT i MGET można podać nazwy plików źródłowych, serwer FTP tworzy także nazwy plików docelowych dla MPUT i MGET. Aby zapoznać się ze składnią tych komend, należy przyjrzeć się tabeli Komendy służące do przesyłania danych. Kolumna tabeli z nagłówkiem *Docelowy* jest parametrem, dla którego nadawana jest domyślna nazwa.

Komenda	Źródłowy	Docelowy	Inne
APPEND	nazwa_pliku_lokalnego	[nazwa_pliku_serwera]	
PUT	nazwa_pliku_lokalnego	[nazwa_pliku_serwera]	
GET	nazwa_pliku_serwera	[nazwa_pliku_lokalnego]	[(Replace)]
MPUT	nazwa_pliku_lokalnego		
MGET	nazwa_pliku_serwera		[(Replace)]

PUT i APPEND

Zasady tworzenia nazw domyślnych dla komend PUT i APPEND dzielą się na dwie kategorie:

- dla serwerów iSeries
 - 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 biblioteki dokumentów, nosi on jedną z dwu następujących nazw:
 - nazwę domyślną, którą jest nazwa znajdująca się po ostatnim ukośniku w nazwie pliku źródłowego,
 - tę *samą* nazwę, co nazwa pliku źródłowego, jeśli nie zawiera żadnego ukośnika.
- dla serwerów innych niż iSeries
 - Jeśli plik źródłowy należy do systemu plików zawierającego biblioteki, domyślna nazwa składa się z *nazwy zbioru, kropki i nazwy 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.

Jeśli serwer jest serwerem iSeries, wówczas generuje on nazwę domyślną w komendach, wykorzystując zasady, których użyto dla komendy PUT.

GET i MGET

Jeśli serwer nie jest serwerem iSeries, domyślna nazwa dla komend GET i MGET oparta jest na części nazwy pliku źródłowego, która znajduje się po ostatnim ukośniku. Jeśli nazwa źródłowa nie zawiera ukośników, jako nazwa domyślna używana jest cała nazwa źródłowa. Oto zasady tworzenia nazw domyślnych:

- Jeśli system plików klienta jest *systemem plików bibliotek* (baza danych iSeries), 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, serwer dodaje do zbioru odpowiednie rozszerzenia i części nazwy dotyczące 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. Serwer wyświetla domyślne nazwy, 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_zdalne

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 zmienić za pomocą komendy LCD. Katalog roboczy w systemie zdalnym można zmienić za pomocą komendy CD.

Format parametrów nazwy pliku lokalnego musi być zgodny z regułami nazewnictwa plików systemu iSeries. Nazwy pliku zdalnego muszą być zgodne z zasadami tworzenia nazw obowiązującymi w systemie zdalnym.

Więcej informacji dotyczących składni:

- Umieszczanie parametrów komend: aby zaznaczyć parametry, można użyć apostrofów (') lub cudzysłowów (").
- Nazwy plików dla komend klienta służących do przesyłania danych: odsyłacz do informacji o domyślnych nazwach plików dla komend klienta służących do przesyłania danych.
- Konwencje składni komend klienta FTP: w sekcji tej opisane są zasady składni komend klienta FTP.

Rozwiązywanie problemów dotyczących FTP

Niżej wymienione sekcje zawierają podstawowe informacje dotyczące rozwiązywania problemów dotyczących FTP.

Określanie problemów dotyczących FTP

Należy obejrzeć listę czynności w celu określenia, czy protokół SMTP działa poprawnie.

Materiały wymagane do raportowania problemów z FTP

W sekcji tej podano, jakich informacji może wymagać przedstawiciel obsługi.

Śledzenie serwera FTP

Wykorzystanie komendy DBUG do śledzenia problemów na serwerze FTP.

Śledzenie klienta FTP

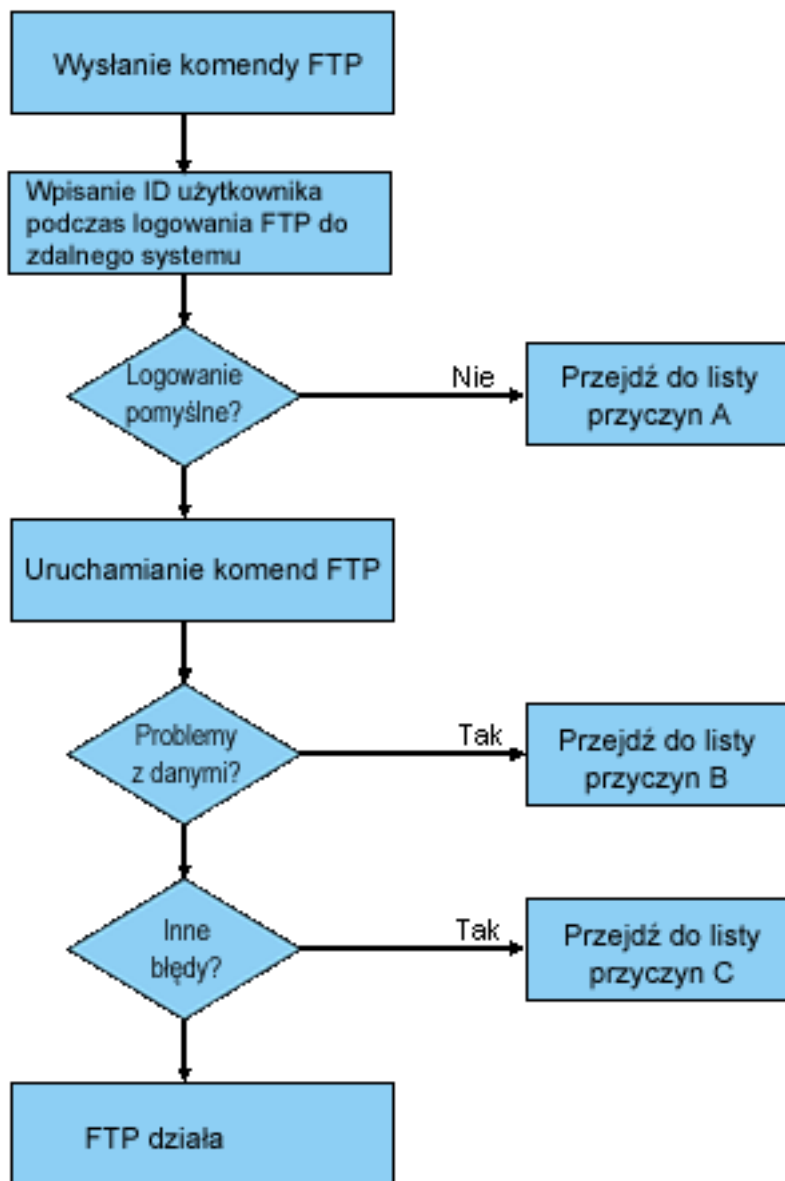
Wykorzystanie komendy DEBUG do śledzenia problemów związanych z klientem FTP.

Praca z zadaniami i protokołem zadania serwera FTP

Otrzymywanie buforowego pliku protokołu zadania serwera FTP do poszukiwania błędów.

Określanie problemów dotyczących FTP

Jeśli podczas korzystania z FTP wystąpi błąd, poniższy diagram przepływów umożliwi zidentyfikowanie przyczyny błędu, jeżeli przyczyna ta nie została zidentyfikowana za pomocą diagramu przepływów dla ogólnych problemów TCP/IP. Listy przyczyn powstania błędów umożliwiają zidentyfikowanie przyczyny problemu.



*

Analiza problemów dotyczących FTP

Lista przyczyn A

1. Czy występuje długa przerwa pomiędzy połączeniem z serwerem FTP iSeries a wyświetleniem podpowiedzi dla identyfikatora użytkownika? Jeśli tak, to należy sprawdzić konfigurację serwera nazw domen w systemie iSeries. Serwer FTP wyśle zapytanie DNS natychmiast po zrealizowaniu nowego połączenia. Problemy z systemem DNS mogą być przyczyną zawieszenia się serwera na kilka minut zanim odpowiedź zostanie otrzymana.

2. Sprawdź, czy program obsługi wyjścia został dodany do punktu wyjścia logowania do serwera FTP. Informacje na ten temat zawiera sekcja Punkt wyjścia logowania do serwera. 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 wykonanie restartu 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, czy tabele odwzorowań w systemie klienta i systemie serwera są zgodne. Sprawdzenie takie jest konieczne tylko w przypadku, gdy korzystasz z własnej tabeli odwzorowania.
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. Dla serwera iSeries długość czasu oczekiwania można ustawić za pomocą komendy QUOTE TIME.
3. Aby sprawdzić, czy interfejs *LOOPBACK jest aktywny, skorzystaj z komendy NETSTAT. Odtwórz sytuację, która spowodowała pojawienie się problemu, wykonując FTP LOOPBACK (wewnątrz systemu iSeries).
 - Jeśli nie można odtworzyć sytuacji, która spowodowała pojawienie się problemu, oznacza to, że jest to prawdopodobnie problem systemu zdalnego.
 - Jeśli można odtworzyć sytuację, która spowodowała pojawienie się problemu, wykonaj poniższe kroki:
 - a. Jeśli jest to problem związany z serwerem FTP, uruchom śledzenie serwera FTP, używając komendy TRCTCPAPP.
 - b. Odtwórz sytuację, która spowodowała pojawienie się problemu.
 - c. Zakończ połączenie FTP. Informacje na ten temat zawiera sekcja 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 związanego z plikiem jest nazwą użytkownika, który wprowadził komendę TRCTCPAPP.
4. Wyniki śledzenia znajdują się w zbiorze buforowym w domyślnej kolejce wyjściowej systemu, związanej z zadaniem serwera FTP.
- f. Wyślij zbiór buforowy.

- g. Jeśli problem dotyczy klienta FTP iSeries, śledzenie można wykonać, korzystając z komendy klienta DEBUG 100.
- h. Jeśli klient FTP jest uruchomiony interaktywnie, naciśnij klawisz F6 (Print - Drukuj), aby utworzyć zbiór buforowy zawierający historię wprowadzonych komend klienta FTP i odpowiedzi serwera FTP na te komendy. Jeśli klient FTP jest uruchomiony w trybie wsadowym nienadzorowanym, historia komend i odpowiedzi serwera zapisywana jest do podanego zbioru wyjściowego. Więcej informacji zawiera sekcja "FTP jako zadanie wsadowe".

Materiały wymagane do raportowania problemów dotyczących FTP

Dowolny problem związany z FTP zgłaszany do IBM powinien zawierać:

- Wyniki śledzenia komunikacji od momentu awarii (wymagane tylko dane TCP/IP) sformatowane dwukrotnie: w kodzie ASCII i w kodzie 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 serwera lub klienta FTP.
- Dane śledzenia debugowania klienta FTP i serwera FTP.
- W razie pojawienia się problemów związanych z klientem FTP zbiór buforowy zawierający sesję klienta FTP (który można uzyskać naciskając klawisz Drukuj (F6) w sesji FTP).
- Jeśli problem jest związany z integralnością danych, należy wysłać zbiór, podzbiór lub bibliotekę będącą przyczyną problemu, a także opis zbioru, podzbioru lub biblioteki.

Śledzenie serwera FTP

Serwer FTP można śledzić z dowolnego serwera iSeries lub innego, na którym jest uruchomiony protokół TCP/IP. Istnieją dwa 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 komendy

Poniżej znajduje się przykład użycia komendy DBUG serwera FTP:

```

                                Protokół FTP
                                (File Transfer Protocol)

Poprzednie komendy i komunikaty FTP:
  Łączenie z hostem o nazwie xxxxxnnn.xxxxxxxx.xxx.xxx i adresie
  n.nnn.nn.nnn za pomocą portu 21.
  220-QTCP pod nazwą xxxxxnnn.nnnnnnnn.nnn.nnn.
  220 Połączenie zostanie zamknięte, jeśli będzie bezczynne przez ponad 5 minut.
  215 OS/400 jest zdalnym systemem operacyjnym. Wersja TCP/IP
  "V4R4M0".
>
  331 Wpisz hasło.
  230 TEST zalogowany.
  250 Obecnie używany format nazewnictwa "0".
  257 Biblioteka bieżąca to "QGPL".
```

```
Wpisz komendę FTP.  
====> quote debug
```

```
F3=Wyjście F6=Drukuj F9=Pobierz  
F17=Pocz.strony F18=Dół strony F21=Wiersz komend CL
```

Aby uruchomić śledzenie serwera FTP:

1. Wpisz QUOTE DEBUG.

```
                                Protokół FTP  
                                (File Transfer Protocol)  
  
Poprzednie komendy i komunikaty FTP:  
Łączenie z hostem o nazwie xxxxxxxx.xxxxxxx.xxx.xxx i adresie  
n.nnn.nn.nnn za pomocą portu 21.  
220-QTCP pod nazwą xxxxxxxx.xxxxxxx.xxx.xxx.  
220 Połączenie zostanie zamknięte, jeśli będzie bezczynne przez ponad 5 minut.  
215 OS/400 jest zdalnym systemem operacyjnym. Wersja TCP/IP  
"V4R4M0".  
>  
331 Wpisz hasło.  
230 TEST zalogowany.  
250 Obecnie używany format nazewnictwa "0".  
257 Biblioteka bieżąca to "QGPL".  
> quote debug  
250 Tryb debugowania jest włączony.  
Wpisz komendę FTP.  
====> quote debug  
  
F3=Wyjście F6=Drukuj F9=Pobierz  
F17=Pocz.strony F18=Dół strony F21=Wiersz komend CL
```

2. Wykonaj operacje FTP, które chcesz śledzić.
3. Ponownie wpisz QUOTE DEBUG, 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, wpisz następującą komendę:
DPSYSVAL QPRTDEV
Zostanie wyświetlony ekran podobny do poniższego:

```
                                Wyświetlenie wartości systemowej  
                                (Display System Value)  
Wartość systemowa. . . . : QPRTDEV  
Opis . . . . . : Opis drukarki  
Drukarka . . . . . : PRT01 Nazwa
```

Nazwa drukarki jest także nazwą domyślnej systemowej kolejki wyjściowej.

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 (Work with Output Queue)								
Kolejka: PRT01			Biblioteka: QGPL			Status: RLS		
Wpisz opcje i naciśnij klawisz Enter.								
1=Wyslij		2=Zmień		3=Wstrzymaj		4=Usuń		5=Wyświetl
6=Zwolnij		7=Komunikaty						
8=Atrybuty			9=Praca ze statusem drukowania					
Opc	Zbiór	Użytkownik	Dane użytk.	Status	Stron	Kopii	Typ form.	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.

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), dostępna od wersji V4R4, 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:

- Informacje śledzenia można przechwytywać dla aplikacji serwera FTP na systemie iSeries. Informacje te można filtrować za pomocą zdalnego adresu IP i portu lub profilu użytkownika iSeries. 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 zadania (zadań) serwera FTP. Przypuśćmy, że ostatnio wpisaną komendą była: >

```
TRCTCPAPP APP(*FTP) SET(*ON) USER(JOEC00L)
```

Odpowiedzią na tę komendę będzie seria komunikatów podobnych do poniższych:

```
TCP45B7 TRCTCPAPP APP(*FTP) SET(*ON) USER(JOEC00L)
      MAXSTG(*DFT) TRCFULL(*WRAP)
TCP45B1 Tracing active for *FTP.
TCP45B2 Data capture begun for *FTP.
TCP45B3 Data buffer wrapped for *FTP.
```

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. Aby włączyć śledzenie klienta FTP, parametr trybu debugowania należy ustawić na wartość 100.

```
DEBUg [tryb 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. (Po zakończeniu śledzenia formatowanie jego wyników może zająć dużo czasu).

Uwaga:

Śledzenie klienta FTP powinno być używane jedynie do raportowania błędów w programach do firmy IBM. Funkcja ta może mieć duży wpływ 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.

Praca z zadaniami i protokołem zadania serwera FTP

Kopia protokołu zadania serwera FTP może być pomocna w uzyskaniu dodatkowych informacji o błędach, które pojawiły się w serwerze FTP. Serwer FTP automatycznie zapisuje w pliku buforowym protokół zadania serwera, jeśli kończy się ono błędem.

Protokół zadania serwera może być zapisany w pliku buforowym bez zakańczania działania serwera poprzez wywołanie poniższej komendy z poziomu klienta FTP:

```
QUOTE RCMD DSPJOBLOG
```

Jeśli komenda ta zostanie wprowadzona bezpośrednio po pojawieniu się błędu, można otrzymać kopię komunikatów o błędach zapisanych w protokole zadania serwera. Protokół zadania można przejrzeć korzystając z komendy WRKSPLF.

Metoda powyższa jest polecana w sytuacjach, gdy komunikat odpowiedzi wracający od klienta do serwera dostarcza niewiele informacji o błędzie, który wystąpił na serwerze. Dzięki tej metodzie można uzyskać szczegółowe informacje dotyczące błędów we/wy, które pojawiły się na serwerze.

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:

```
CHGJOB JOB(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:

```
CHGJOB JOB(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 - CHGJOB) w następujący sposób:

```
CHGJOB JOB(QUSRSYS/QTMFTPS) LOG(4 00 *SECLVL)
```

Aby otrzymywać buforowy protokół zadania tylko wtedy, gdy serwer kończy działanie, należy użyć komendy CHGJOB w następujący sposób:

```
CHGJOB JOB(QUSRSYS/QTMFTPS) LOG(4 00 *NOLIST)
```

Zadania serwera FTP i nazwy zadań

Zadania serwera FTP są uruchamiane, gdy uruchamiana jest komenda STRTCP, a parametr FTP AUTOSTART jest ustawiony na *YES lub kiedy uruchamiana jest komenda STRTCP SVR z parametrem SERVER ustawionym na *FTP lub *ALL. Te zadania są uruchamiane w podsystemie QSYSWRK, a ich celem jest monitorowanie użytkowników odwiedzających serwer FTP. Format nazw tych zadań ma postać QTFTPnnnnn. Sekwencja nnnnn jest numerem zadania serwera FTP, wprowadzonego do tego serwera.

Aby pracować z zadaniami serwera FTP, należy podać następującą komendę CL:

```
WRKACTJOB JOB(QTFTP*)
```


IBM