IBM

eserver

iSeries

Ochrona

Wersja 5

SC85-0124-08

IBM

@server

iSeries

Ochrona

Wersja 5

SC85-0124-08

Uwaga

Przed użyciem tych informacji oraz produktu, którego dotyczą, należy przeczytać Dodatek H, “Uwagi”, na stronie 633.

Wydanie dziewiąte (sierpień 2005)

| To wydanie ma zastosowanie dla wersji 5, wydania 3 modyfikacji 0 systemu IBM Operating System/400 (numer produktu
| 5722-WSV) oraz wszystkich późniejszych wydań i modyfikacji, chyba że w nowym wydaniu zostanie zaznaczone inaczej. Ta
| wersja może nie pracować na wszystkich komputerach o zredukowanej liczbie instrukcji (RISC), a także na modelach CISC.

| Zastępuje SC85-0124-07.

Spis treści

Rysunki

Tabele

Informacje na temat podręcznika Ochrona (SC85-0124)

Ta książka udostępnia informacje na temat planowania, konfigurowania, zarządzania i kontrolowania ochrony w systemie iSeries. Opisuje wszystkie opcje ochrony systemu oraz ich powiązania z innymi aspektami dotyczącymi systemu, takimi jak zarządzanie pracą, składowanie i odtwarzanie oraz projektowanie aplikacji.

Ta książka nie udostępnia pełnych instrukcji dotyczących konfigurowania ochrony systemu. Przykłady prezentujące krok po kroku konfigurowanie ochrony zawiera Centrum informacyjne iSeries (patrz “Informacje wstępne i pokrewne” na stronie xvi) oraz podręcznik *Wskazówki i narzędzia dotyczące ochrony iSeries*, SC85-0032-07. Informacje dotyczące planowania i konfigurowania Podstawowa ochrona systemu i jej planowanie znajdują się także w Centrum informacyjnym (patrz “Informacje wstępne i pokrewne” na stronie xvi).

Ta książka nie udostępnia pełnych informacji na temat planowania dla użytkowników programu IBM Lotus Domino. Informacje dla użytkowników produktu Lotus Domino znajdują się pod adresem URL http://www.lotus.com/ldd/doc. Ten serwis WWW zawiera informacje dotyczące produktów IBM Lotus Notes, Lotus Domino i IBM Lotus Domino for iSeries. Z tego serwisu WWW można pobrać informacje w formacie bazy danych Domino (.NSF) lub w formacie Adobe Acrobat (.PDF), przeszukać bazy danych oraz dowiedzieć się, jak otrzymać wydrukowane podręczniki.

Ta książka nie zawiera pełnych informacji na temat aplikacyjnych interfejsów programistycznych (application programming interfaces - API), które udostępniane są w celu zapewnienia dostępu do informacji o ochronie. Interfejsy API opisane są w Centrum informacyjnym. Ten temat nie zawiera informacji na temat sieci Internet. Informacje zawierające uwagi dotyczące podłączania systemu do sieci Internet zawierają temat IBM SecureWay: iSeries a Internet w Centrum informacyjnym (patrz “Informacje wstępne i pokrewne” na stronie xvi). .

Listę pokrewnych publikacji zawiera sekcja “Informacje pokrewne” na stronie 637.

Dla kogo przeznaczona jest ta książka

Podstawowymi odbiorcami tej książki są administratorzy ochrony.

Rozdział 9, “Kontrolowanie ochrony na systemie iSeries”, na stronie 233 przeznaczony jest dla administratorów zajmujących się kontrolą ochrony w systemie.

W tej książce przyjęto, że użytkownik potrafi uruchamiać komendy w systemie. Aby skorzystać z niektórych przykładów, użytkownik musi wiedzieć jak:

- edytować i tworzyć programy CL,
- używać programów zapytań, takich jak program licencjonowany Query/400.

Informacje zawarte w poniższych rozdziałach mogą pomóc zrozumieć programistom aplikacji oraz programistom systemowych związki między ochroną, aplikacją a systemem:

Rozdział 5, “Ochrona zasobów”, na stronie 113

Rozdział 6, “Ochrona zarządzania pracą”, na stronie 179

Rozdział 7, “Projektowanie ochrony”, na stronie 199

Rozdział 8, “Składowanie i odtwarzanie informacji o ochronie”, na stronie 223

Konwencje i terminologia użyte w tej książce

Ekrany systemu iSeries zamieszczone w tym podręczniku mogą być wyświetlane tak, jak wyglądają w programie iSeries Navigator będącym częścią produktu iSeries Access for Windows na komputerze osobistym. Ekrany przykładowe w tym podręczniku mogą być także wyświetlane w postaci, w jakiej byłyby prezentowane w przypadku braku programu iSeries Navigator.

Więcej informacji na temat używania programu iSeries Navigator zawiera Centrum informacyjne iSeries (patrz “Informacje wstępne i pokrewne”).

Informacje wstępne i pokrewne

Centrum informacyjne iSeries można wykorzystać jako źródło wiedzy na temat systemu iSeries. Dostęp do niego można uzyskać w następujący sposób:

- przez Internet pod adresem URL:
  `http://www.ibm.com/eserver/iseries/infocenter`,
- na dysku CD-ROM: SK3T–5495–00, Centrum informacyjne iSeries. Ten pakiet zawiera także wersje PDF podręczników systemu iSeries (SK3T–5496–00, Centrum informacyjne iSeries: Podręczniki uzupełniające), który zastępuje bibliotekę elektroniczną.

Centrum informacyjne iSeries zawiera doradców oraz istotne tematy, które dotyczą komend CL, interfejsów API, partycji logicznych, technologii klastrowej, języka Java, protokołu TCP/IP, serwerów sieci WWW oraz sieci chronionych. Zawiera także odsyłacze do związanej z tym tematem dokumentacji technicznej IBM Redbooks oraz odsyłacze do innych serwisów WWW firmy IBM, takich jak Technical Studio oraz do strony głównej IBM.

Z każdym zamówieniem sprzętu dostarczane są następujące dyski CD-ROM:

- **SK3T-4096-00, iSeries Installation and Service Library**; ten dysk zawiera podręczniki PDF wymagane podczas instalowania i obsługi systemu IBM @server iSeries,
- *CD-ROM iSeries - Konfigurowanie i obsługa*, SK3T-5498-02. ten dysk CD-ROM zawiera program IBM iSeries Access for Windows oraz kreator EZ-Setup; program iSeries Access Express oferuje pełen zestaw możliwości klienta i serwera do podłączania komputerów PC z serwerami iSeries; kreator EZ-Setup umożliwia automatyzację wielu czynności związanych z konfigurowaniem serwerów iSeries.

Listę pokrewnych publikacji zawiera sekcja “Informacje pokrewne” na stronie 637.

Program iSeries Navigator

Centrum informacyjne iSeries można wykorzystać jako źródło informacji technicznych na temat systemu iSeries.

Dostęp do Centrum informacyjnego można uzyskać na dwa sposoby:

- ze strony WWW:
  `http://www.ibm.com/eserver/iseries/infocenter`
- z dysku CD-ROM *Centrum informacyjne iSeries*, SK3T-5495-04; ten dysk dostarczany jest razem z nowym sprzętem iSeries lub aktualizacją oprogramowania IBM Operating System/400; dysk CD-ROM można także zamówić ze strony IBM Publications Center:
  `http://www.ibm.com/shop/publications/order`.

Centrum informacyjne iSeries zawiera nowe i zaktualizowane informacje dotyczące systemu iSeries, jak instalowanie oprogramowania i sprzętu, systemu Linux, produktu WebSphere, języka Java, wysokiej dostępności, baz danych, partycji logicznych, komend CL i interfejsów API. Dodatkowo udostępnia doradców oraz wyszukiwarki asystujące podczas planowania, rozwiązywania problemów oraz konfigurowania sprzętu i oprogramowania systemu iSeries.

Z każdym nowym zamówieniem dostarczana jest płyta *CD-ROM iSeries - Konfigurowanie i obsługa*, SK3T-5498-02. Ten dysk CD-ROM zawiera produkt IBM @server iSeries Access for Windows i kreatora EZ-Setup. Produkt iSeries Access Family oferuje pełen zestaw możliwości klienta i serwera do podłączania komputerów PC z serwerami iSeries. Kreator EZ-Setup umożliwia automatyzację wielu czynności związanych z konfigurowaniem serwerów iSeries.

Jak wysyłać uwagi

Kontakt z użytkownikiem jest istotny, ponieważ ułatwia dostarczanie precyzyjnych i stojących na wysokim poziomie informacji. Jeśli są jakieś uwagi dotyczące tej książki lub jakiejkolwiek innej dokumentacji iSeries, można:

- jeśli użytkownik preferuje wysyłanie uwag pocztą, skorzystać z formularza uwag czytelników oraz adresu wydrukowanego z tyłu książki; jeśli formularz wysyłany jest z kraju lub regionu innego niż Stany Zjednoczone, można przekazać go do lokalnego oddziału IBM lub do przedstawiciela IBM,
- wysłać uwagi faksem pod jeden z poniższych numerów:
  - Stany Zjednoczone, Kanada i Puerto Rico: 1-800-937-3430
  - inne kraje lub regiony: 1-507-253-5192
- wysłać uwagi w postaci elektronicznej pod jeden z poniższych adresów poczty elektronicznej:
  - uwagi dotyczące książek:

    RCHCLERK@us.ibm.com
  - uwagi dotyczące Centrum informacyjnego iSeries:

    RCHINFOC@us.ibm.com

Uwagi powinny zawierać:

- tytuł książki lub artykułu z Centrum informacyjnego iSeries,
- numer książki,
- numer strony lub tytuł rozdziału książki, którego komentarz dotyczy.

Co nowego w wersji V5R3

Dwie nowe, ogólne wartości systemowe ochrony

Za pomocą dwóch nowych wartości systemowych ochrony, Skanowanie systemów plików (Scan File Systems - QSCANFS) i Sterowanie skanowaniem systemów plików (Scan File Systems Control - QSCANFSCTL), użytkownik może uruchomić narzędzia, które skanują pliki rezydujące w zintegrowanym systemie plików. Po wykryciu wirusa, można podjąć odpowiednie działania eliminujące go.

Wartość systemowa Skanowanie systemów plików (Scan File Systems - QSCANFS) umożliwia określenie zintegrowanego systemu plików, którego obiekty mają być przeskanowane. Skanowanie zintegrowanego systemu plików jest włączane, gdy programy obsługi wyjścia są rejestrowane za pomocą punktów wyjścia związanych ze skanowaniem zintegrowanego systemu plików.

Wartość systemowa Sterowania skanowaniem systemów plików (Scan File Systems Control - QSCANFSCTL) steruje skanowaniem zintegrowanego systemu plików, które jest włączane, gdy programy obsługi wyjścia są rejestrowane za pomocą dowolnego punktu wyjścia związanego ze skanowaniem zintegrowanego systemu plików.

Nowa wartość systemowa sterująca kontrolą

Wartość systemowa Rozszerzenie poziomu kontroli (Auditing Level Extension - QAUDLVL2), razem z wartością Poziom kontroli (Auditing Level - QAUDLVL) określa, które zdarzenia związane z ochroną są protokołowane w kronice kontroli ochrony (QAUDJRN) dla wszystkich użytkowników systemu. Wartość systemowa QAUDLVL2 jest wymagana, gdy potrzebnych jest więcej niż szesnaście wartości kontroli.

Nowe pola parametrów dla profilu użytkownika

Parametr Lokalne zarządzanie hasłem określa, czy hasło profilu użytkownika powinno być zarządzane lokalnie. Jeśli użytkownik nie chce, aby hasło było zarządzane lokalnie, to jego wartość nadal jest przesyłana do innych produktów IBM, które wykonują synchronizację hasła. Jeśli hasła nie są zarządzane lokalnie, wartością hasła lokalnego jest wartość *NONE.

Parametr Powiązania EIM określa, czy do identyfikatora EIM dla użytkownika mają być dodawane powiązania EIM (Enterprise Identity Mapping).

Rozdział 1. Wprowadzenie do ochrony systemu iSeries

Rodzina systemów @server obejmuje szeroki zakres użytkowników. Mały system może mieć od trzech do pięciu użytkowników, natomiast duży może mieć ich kilka tysięcy. Niektóre instalacje mają wszystkie stacje robocze ulokowane w jednym, relatywnie bezpiecznym miejscu. Inne mają bardzo rozproszonych użytkowników, nawet takich, którzy łączą się telefonicznie oraz użytkowników pośrednich, podłączonych przez komputery osobiste lub sieci systemowe.

Ochrona systemu iSeries jest wystarczająco elastyczna, aby spełnić wymagania szerokiego zakresu użytkowników i sytuacji. Użytkownik musi zrozumieć dostępne funkcje i opcje, tak aby mógł je zaadoptować do własnych wymagań ochrony. Ten rozdział udostępnia przegląd opcji ochrony w systemie.

Ochrona systemu ma trzy ważne cele:

Poufność:
- zabezpieczanie przed ujawnieniem informacji niepowołanym osobom,
- ograniczanie dostępu do poufnych informacji,
- zabezpieczanie przed ciekawskimi użytkownikami systemu oraz osobami postronnymi.

Integralność:
- zabezpieczanie przed nieuprawnionymi zmianami danych,
- zapewnienie, że dane są przetwarzane tylko przez uprawnione do tego programy,
- zapewnianie, że dane są nienaruszone.

Dostępność:
- zabezpieczenie przed przypadkowymi zmianami lub zniszczeniem danych,
- zabezpieczanie przed próbami naruszenia lub zniszczenia zasobów systemowych przez osoby postronne.

Ochrona systemu często związana jest z zagrożeniami zewnętrznymi, takimi jak hakerzy lub konkurencja. Jednak zabezpieczenie przed przypadkowymi awariami powodowanymi przez uprawnionych użytkowników systemu często jest największą korzyścią z dobrze zaprojektowanej ochrony systemu. W systemie bez dobrze skonfigurowanych opcji ochrony naciśnięcie złego klawisza może spowodować usunięcie ważnych informacji. Ochrona systemu może zapobiec tego typu wypadkom.

Nawet najlepsze funkcje ochrony systemu nie mogą dawać dobrych wyników bez dobrego planowania. Ochrona, która jest skonfigurowana w małych fragmentach, bez planowania, może być zagmatwana. Taką ochronę trudno jest obsługiwać oraz kontrolować. Planowanie nie oznacza projektowania ochrony dla każdego zbioru, programu i urządzenia. Oznacza ustanowienie ogólnego podejścia do ochrony systemu oraz komunikowania i narzucenie pewnych zasad projektantom aplikacji, programistom i użytkownikom systemu.

Podczas planowania ochrony systemu oraz decydowania o potrzebnej ochronie, należy rozważyć następujące pytania:
- Czy istnieje strategia przedsiębiorstwa lub standard, który wymaga pewnego poziomu ochrony?
- Czy kontrolerzy przedsiębiorstwa wymagają niektórych poziomów ochrony?
- Jak ważny dla przedsiębiorstwa jest system oraz dane?
- Jak ważne jest zabezpieczanie przed błędami udostępniane przez opcje ochrony?
- Jakie są wymagania ochrony przedsiębiorstwa na przyszłość?

Aby ułatwić instalowanie, wiele możliwości ochrony systemu jest nieaktywnych w dostarczanym systemie. W tej książce zawarto zalecenia dotyczące doprowadzania systemu do rozsądnego poziomu ochrony. Podczas analizowania tych zaleceń należy rozważyć wymagania ochrony dotyczące konkretnej instalacji.

Ochrona fizyczna

Ochrona fizyczna obejmuje zabezpieczanie jednostki systemowej, urządzeń systemowych oraz nośników składowania przed przypadkowym lub umyślnym uszkodzeniem. Większość podejmowanych środków ochrony fizycznej jest niezależnych od systemu. Jednak system wyposażony jest w blokadę, która zabezpiecza przed wykonywaniem na jednostce systemowej nieuprawnionych funkcji.

Uwaga: Dla niektórych modeli opcję blokady należy zamówić.

Ochrona fizyczna została opisana w Centrum informacyjnym (patrz sekcja “Informacje wstępne i pokrewne” na stronie xvi).

Ochrona za pomocą blokady

Blokada na panelu sterowania modelu 940x kontroluje dostęp do różnych funkcji panelu sterowania systemu. Pozycja blokady może być odczytana i zmieniona programowo za pomocą:

- funkcji API Retrieve IPL Attributes (QWCRIPLA),
- komendy Zmiana atrybutów IPL (Change IPL Attributes - CHGIPLA).

Umożliwia to zdalnemu użytkownikowi dostęp do dodatkowych funkcji dostępnych na panelu sterowania. Na przykład może zdalnie sterować tym, z jakiego obszaru zostanie wykonany IPL oraz do jakiego środowiska - OS/400 lub narzędzi DST (Dedicated Service Tools).

Wartość systemowa OS/400, QRMTSRVATR, kontroluje zdalny dostęp. Domyślnie jest ona wyłączona, co uniemożliwia przesłonięcie blokady. Wartość systemowa może być zmieniona, aby umożliwić zdalny dostęp, ale taka zmiana wymaga uprawnień specjalnych *SECADM i *ALLOBJ.

Poziom ochrony

Poziomy ochrony określa się za pomocą wartości systemowej QSECURITY. System oferuje pięć poziomów ochrony:

Poziom 10:
Poziom 10 nie jest już obsługiwany. Informacje dotyczące poziomów ochrony (10, 20, 30, 40 i 50) zawiera Rozdział 2, “Korzystanie z wartości systemowej Ochrona systemu (QSecurity)”, na stronie 7.

Poziom 20:
System wymaga do wpisania się identyfikatora użytkownika i hasła. Wszyscy użytkownicy mają dostęp do wszystkich obiektów.

Poziom 30:
System wymaga do wpisania się identyfikatora użytkownika i hasła. Narzucana jest ochrona zasobów.

Poziom 40:
System wymaga do wpisania się identyfikatora użytkownika i hasła. Narzucana jest ochrona zasobów. Narzucane są także dodatkowe opcje zabezpieczania integralności.

Poziom 50:
System wymaga do wpisania się identyfikatora użytkownika i hasła. Narzucana jest ochrona zasobów. Narzucane jest zabezpieczanie integralności z poziomu 40 oraz rozszerzone zabezpieczenie integralności. Poziom ochrony 50 jest przeznaczony dla systemów iSeries, którym stawia się duże wymagania w zakresie ochrony i został zaprojektowany w celu spełniania wymagań ochrony C2.

Poziomy ochrony systemu są opisane w sekcji Rozdział 2, “Korzystanie z wartości systemowej Ochrona systemu (QSecurity)”, na stronie 7.

Wartości systemowe

Wartości systemowe umożliwiają dostosowanie wielu charakterystyk systemu. Grupa wartości systemowych używana jest do definiowania ustawień ochrony dla systemu. Na przykład można podać:

- ile prób wpisania się jest dozwolonych dla urządzenia,
- czy system automatycznie wypisuje nieaktywną stację roboczą,
- jak często musi być zmieniane hasło,
- długość i strukturę haseł.

Wartości systemowe związane z ochroną opisano w sekcji Rozdział 3, “Wartości systemowe dotyczące ochrony”, na stronie 19.

Podpisywanie

Kluczowym komponentem ochrony jest integralność: możliwość ufania, że obiekty w systemie nie były modyfikowane. System operacyjny jest chroniony przy użyciu podpisów cyfrowych. Aby wzmocnić integralność systemu, wprowadzono możliwość podpisywania obiektów programowych. Więcej informacji dotyczących podpisywania w celu ochrony systemu znajduje się w temacie *Wskazówki i narzędzia dotyczące ochrony iSeries*. Jest to szczególnie ważne, jeśli obiekty przesyłane są przez sieć Internet lub przechowywane na nośnikach, które mogą być modyfikowane. Podpis cyfrowy może być użyty do wykrycia, czy obiekt został zmieniony.

Podpisy cyfrowe, oraz ich użycie do sprawdzania integralności oprogramowania, może być zarządzane zgodnie ze strategiami ochrony za pomocą wartości systemowej sprawdzania odtwarzania obiektu (Verify Object Restore - QVFYOBJRST), komendy Sprawdzenie integralności obiektu (Check Object Integrity - CHKOBJITG) i programu Menedżer certyfikatów cyfrowych (Digital Certificate Manager). Dodatkowo użytkownik może podpisywać własne programy (wszystkie programy licencjonowane dostarczane z systemem iSeries są podpisane). Program DCM opisany jest w Centrum informacyjnym (patrz sekcja “Informacje wstępne i pokrewne” na stronie xvi).

Nową funkcją w wersji V5R2 jest możliwość ograniczania dodawania podpisów cyfrowych do bazy certyfikatów cyfrowych za pomocą funkcji API Add Verifier oraz ograniczania resetowania haseł bazy certyfikatów cyfrowych. Narzędzia SST udostępniają nowe opcje menu Praca z ochroną systemu (Work with system security), gdzie można ograniczyć dodawanie certyfikatów cyfrowych.

Włączanie środowiska jednokrotnego wpisywania się

W dzisiejszych różnorodnych sieciach z serwerami partycjonowanymi i wieloma platformami, administratorzy muszą radzić sobie ze złożonością zarządzania identyfikacją i uwierzytelnianiem użytkowników sieci. Nowa infrastruktura firmy IBM i jej wykorzystywanie w systemie iSeries pomaga administratorom, użytkownikom i programistom aplikacji łatwiej i bardziej oszczędnie zarządzać identyfikacją i uwierzytelnianiem.

Aby włączyć środowisko jednokrotnego wpisywania się, IBM udostępnia dwie technologie, które współpracują ze sobą w celu umożliwienia użytkownikom wpisywania się za pomocą ich nazwy użytkownika oraz hasła w systemie Windows i uwierzytelnienia w systemach iSeries w sieci. Usługa uwierzytelniania sieciowego oraz oprogramowanie Enterprise Identity Mapping (EIM) to dwie technologie, które administrator musi skonfigurować, aby włączyć środowisko jednokrotnego wpisywania się. Systemy Windows 2000, XP, AIX i zSeries, do uwierzytelniania użytkowników w sieci, korzystają z protokołu Kerberos. Jednostki główne (użytkowników Kerberos) uwierzytelnia w sieci bezpieczny, centralny serwer nazywany centrum dystrybucji kluczy.

Usługa uwierzytelniania sieciowego umożliwia systemowi iSeries uczestnictwo w domenie Kerberos, natomiast technologia EIM udostępnia mechanizm łączący jednostkę główną protokołu Kerberos z pojedynczym identyfikatorem EIM, który reprezentuje użytkownika w całym przedsiębiorstwie. Inne identyfikatory użytkownika, takie jak nazwa użytkownika w OS/400 mogą być także powiązane z identyfikatorem EIM. Gdy użytkownik wpisuje się do sieci i uzyskuje dostęp do systemu iSeries, nie jest proszony o podanie swojego identyfikatora i hasła. Jeśli uwierzytelnianie Kerberos powiedzie się, aplikacje mogą sprawdzić powiązania z identyfikatorem EIM, aby odszukać nazwę użytkownika OS/400. Użytkownik nie potrzebuje już hasła do aplikacji i funkcji systemu iSeries, ponieważ został

uwierzytelniony przez protokół Kerberos. Administratorzy mogą centralnie zarządzać tożsamościami użytkownika za pomocą technologii EIM, natomiast użytkownicy sieci muszą zarządzać tylko jednym hasłem. Opcję jednokrotnego wpisywania się można włączyć konfigurując w systemie iSeries usługę uwierzytelniania sieciowego oraz program Enterprise Identity Mapping (EIM). Aby przejrzeć scenariusz opisujący sposób skonfigurowania środowiska pojedynczego logowania się, należy odwiedzić Centrum informacyjne i wyświetlić temat Scenariusz: włączanie pojedynczego logowania się. (**Ochrona —> Usługa uwierzytelnienia sieciowego —> Scenariusze usługi uwierzytelnienia sieciowego —> Scenariusz: włączanie pojedynczego logowania się**). Więcej informacji na temat sposobu dostępu do Centrum informacyjnego zawiera sekcja “Informacje wstępne i pokrewne” na stronie xvi.

Profile użytkowników

Każdy użytkownik systemu ma swój profil użytkownika. Na poziomie ochrony 10 system automatycznie tworzy profil, gdy użytkownik wpisuje się po raz pierwszy. Na wyższych poziomach ochrony najpierw należy taki profil utworzyć.

Profil użytkownika jest skutecznym i elastycznym narzędziem. Określa, co użytkownik może zrobić, a także definiuje sposób, w jaki widzi on system. Poniżej opisano kilka ważnych opcji ochrony związanych z profilem użytkownika:

Uprawnienia specjalne
: Uprawnienia specjalne określają, czy użytkownik może wykonywać pewne funkcje systemu, takie jak tworzenie profili użytkowników lub zmienianie zadań innych użytkowników.

Menu i program początkowy
: Menu i program początkowy określają, co użytkownik zobaczy po wpisaniu się do systemu. Użytkownika można ograniczyć do określonego zestawu zadań ograniczając menu początkowe.

Ograniczenie możliwości
: Pole Ograniczenie możliwości w profilu użytkownika określa, czy użytkownik może podawać komendy oraz zmieniać menu lub program początkowy podczas wpisywania się.

Profile użytkowników omówiono w Rozdział 4, “Profile użytkowników”, na stronie 57.

Profile grupowe

Profil grupowy jest szczególnym typem profilu użytkownika. Można go używać do definiowania uprawnień dla grupy użytkowników, zamiast przyznawania uprawnień każdemu użytkownikowi z osobna. Profil grupowy może być właścicielem obiektów. Profilu grupowego można także użyć jako wzorca do tworzenia pojedynczych profili użytkowników za pomocą funkcji kopiowania profilu.

Sekcja “Planowanie profili grupowych” na stronie 218 omawia korzystanie z uprawnień grupowych. Sekcja “Grupowe prawo własności do obiektów” na stronie 123 omawia, które obiekty powinny należeć do profili grupowych. Sekcja “Grupa podstawowa dla obiektu” na stronie 123 omawia korzystanie z grupy podstawowej oraz uprawnienia grupy podstawowej do obiektu. Sekcja “Kopiowanie profili użytkowników” na stronie 100 opisuje sposób kopiowania profilu grupowego w celu utworzenia pojedynczego profilu użytkownika.

Ochrona zasobów

Ochrona zasobów w systemie umożliwia definiowanie, kto może używać obiektów i w jaki sposób mogą one być używane. Możliwość dostępu do obiektu nazywa się **uprawnieniem**. Użytkownik może określić szczegółowe uprawnienia, takie jak dodawanie rekordów lub ich zmianę. Może także skorzystać z podzbiorów zdefiniowanych systemowo: *ALL, *CHANGE, *USE i *EXCLUDE.

Obiektami wymagającymi zabezpieczenia są zbiory, programy i biblioteki, ale użytkownik może określić uprawnienia dla każdego obiektu w systemie. Poniżej przedstawiono opisy funkcji ochrony zasobów:

Profile grupowe
: Grupa podobnych użytkowników może współużytkować te same uprawnienia do obiektów.

Listy autoryzacji
Obiekty z podobnymi wymaganiami ochrony mogą być zgrupowane na jednej liście; wtedy uprawnienia mogą być nadawane do takiej listy, a nie do pojedynczych obiektów.

Prawo własności do obiektu
Każdy obiekt w systemie ma właściciela. Właścicielem obiektu może być pojedynczy profil użytkownika lub profil grupowy. Poprawne przypisanie praw własności obiektów ułatwi zarządzanie aplikacjami i delegowanie odpowiedzialności za ochronę informacji.

Grupa podstawowa
Dla obiektu można określić grupę podstawową. Uprawnienia grupy podstawowej przechowywane są razem z obiektem. Korzystanie z grup podstawowych może uprościć zarządzanie uprawnieniami i zwiększyć wydajność sprawdzania uprawnień.

Uprawnienia do biblioteki
Zbiory i programy, które mają podobne wymagania ochrony, można umieścić w bibliotece i ograniczyć do niej dostęp. Często jest to łatwiejsze rozwiązanie, niż ograniczanie dostępu do każdego pojedynczego obiektu.

Uprawnienia do katalogu
Uprawnienia do katalogu można używać w ten sam sposób, jak uprawnienia do biblioteki. Obiekty można pogrupować w katalogi i zabezpieczać katalogi, a nie pojedyncze obiekty.

Uprawnienia do obiektu
W przypadkach, gdy dostęp do biblioteki lub katalogu nie jest wystarczająco ograniczony, istnieje możliwość ograniczenia uprawnień dostępu do pojedynczych obiektów.

Uprawnienia publiczne
Dla każdego obiektu można zdefiniować, jaki rodzaj dostępu ma użytkownik systemu, który nie ma żadnych innych uprawnień do obiektu. Uprawnienia publiczne to skuteczny sposób na zabezpieczanie informacji oraz zapewnienie dobrej wydajności systemu.

Uprawnienia adoptowane
Uprawnienia adoptowane dodają uprawnienia właściciela programu do uprawnień użytkownika uruchamiającego program. Uprawnienia adoptowane to przydatne narzędzie dla użytkownika wymagającego różnych uprawnień do obiektu, w zależności od sytuacji.

Magazyn uprawnień
Magazyn uprawnień przechowuje informacje o uprawnieniach dla zbioru bazy danych opisanego przez program. Informacje o uprawnieniach pozostają, nawet gdy zbiór jest usuwany. Magazyny uprawnień są powszechnie używane podczas konwertowania danych z systemu System/36, ponieważ aplikacje systemu System/36 często zbiory usuwają i tworzą je ponownie.

Uprawnienia na poziomie pola
Uprawnienia na poziomie pola nadawane są pojedynczym polom w zbiorze bazy danych. To uprawnienie zarządzane jest za pomocą instrukcji SQL.

Ochronę zasobów opisuje Rozdział 5, “Ochrona zasobów”, na stronie 113

Kronika kontroli ochrony

W systemie istnieje kilka funkcji, które pomagają kontrolować efektywność ochrony. W szczególności, system udostępnia możliwość protokołowania w kronice kontroli ochrony wybranych zdarzeń związanych z ochroną. Kontrolę nad tym, które zdarzenia mają być protokołowane, ma kilka wartości systemowych oraz wartości profilu użytkownika i obiektu.

Rozdział 9, “Kontrolowanie ochrony na systemie iSeries”, na stronie 233 udostępnia informacje dotyczące kontrolowania ochrony.

Ochrona C2

Korzystając z poziomu ochrony 50 oraz wykonując instrukcje z podręcznika *Security - Enabling for C2*, SC41-5303-00, użytkownik może doprowadzić system iSeries w wersji 4 wydaniu 4 do poziomu ochrony C2. Poziom C2 jest standardem ochrony zdefiniowanym przez rząd Stanów Zjednoczonych w dokumencie *Department of Defense Trusted System Evaluation Criteria* (DoD 5200.28.STD).

W październiku 1995 roku system iSeries formalnie otrzymał od departamentu obrony Stanów Zjednoczonych stopień ochrony C2. Stopień C2 dotyczy systemu OS/400 w wersji V2R3 oraz programów SEU, Query/400, SQL i Common Cryptographic Architecture Services/400. Stopień C2 został przyznany po rygorystycznej, trwającej wiele lat ocenie. System iSeries jest pierwszym systemem, który otrzymał stopień C2 dla systemu (sprzętu i systemu operacyjnego) ze zintegrowaną, w pełni funkcjonującą bazą danych.

W 1999 roku system iSeries otrzymał stopień C2 dla wersji 4 wydania 4 systemu operacyjnego OS/400 (opcja o kodzie 1920), programu SEU, Query/400, SQL, TCP/IP Utilities, Cryptographic Access Provider i Advanced Series Hardware. Do oceny włączono także ograniczony zestaw funkcji komunikacyjnych TCP/IP między systemami iSeries podłączonymi do sieci lokalnej.

Aby otrzymać stopień C2, system musi spełniać ścisłe kryteria w następujących obszarach:

- indywidualna kontrola dostępu,
- odpowiedzialność użytkownika,
- kontrola ochrony,
- izolowanie zasobów.

Niezależne pule dyskowe

Niezależne pule dyskowe udostępniają możliwość grupowania pamięci, która może być wyłączona lub włączona niezależnie od danych systemowych lub innych niezwiązanych danych. Terminy niezależna pula pamięci dyskowej (ASP) i niezależna pula dyskowa są synonimami. Niezależna pula dyskowa może być przełączalna między wieloma systemami w środowisku klastrowym lub podłączona prywatnie do pojedynczego systemu. W wersji V5R2 zmiany funkcjonalne dotyczące niezależnych pul dyskowych mają wpływ na ochronę systemu. Wykonując na przykład komendę CRTUSRPRF, nie można tworzyć profilu użytkownika (*USRPRF) w niezależnej puli dyskowej. Jednak jeśli użytkownik ma uprawnienia prywatne do obiektu na niezależnej puli dyskowej, jest właścicielem obiektu na niezależnej puli dyskowej lub jest w grupie podstawowej obiektu na niezależnej puli dyskowej, to nazwa profilu przechowywana jest na niezależnej puli dyskowej. Jeśli niezależna pula dyskowa przenoszona jest do innego systemu, uprawnienia prywatne, prawa własności do obiektu oraz pozycji grupy podstawowej będą dołączone w systemie docelowym do profilu o tej samej nazwie. Jeśli w systemie docelowym dany profil nie istnieje, to zostanie utworzony. Użytkownik nie będzie miał żadnych uprawnień specjalnych, a jego hasło będzie miało wartość *NONE.

Niezależne pule dyskowe zostały rozbudowane w celu zapewnienia obsługi obiektów opartych o biblioteki. W poprzednich wydaniach niezależne pule dyskowe obsługiwały jedynie systemy plików użytkownika (UDFS). Jednak niektóre obiekty nie mogą być przechowywane na niezależnych pulach dyskowych. Pełna lista obsługiwanych i nieobsługiwanych obiektów znajduje się w temacie Obsługiwane i nieobsługiwane typy obiektów systemu OS/400 w Centrum informacyjnym. (**Zarządzanie systemami —> Niezależne pule dyskowe —> Pojęcia —> Ograniczenia i uwagi —> Obsługiwane i nieobsługiwane typy obiektów systemu OS/400**)

Rozdział 2. Korzystanie z wartości systemowej Ochrona systemu (QSecurity)

Ten rozdział omawia wartość systemową poziom ochrony (QSECURITY) oraz związane z nią zagadnienia.

Przegląd:

Przeznaczenie:
Określa obowiązujący w systemie poziom ochrony.

Sposób używania:
WRKSYSVAL *SEC (komenda Praca z wartościami systemowymi - Work with System Values) lub menu SETUP, opcja 1 (Zmiana opcji systemu - Change System Options)

Uprawnienia:
*ALLOBJ i *SECADM

Pozycja kroniki:
SV

Uwaga:
Przed zmianą na system produkcyjny należy przeczytać odpowiednią sekcję dotyczącą migrowania z jednego poziomu ochrony na inny.

System oferuje pięć poziomów ochrony:

10 **Brak ochrony narzucanej przez system**

Uwaga: Użytkownik nie może ustawić wartości systemowej QSECURITY na poziom ochrony o wartości 10.

20 Ochrona przez wpisywanie się

30 Ochrona zasobów i przez wpisywanie się

40 Ochrona zasobów i przez wpisywanie się; zabezpieczenie integralności

50 Ochrona zasobów i przez wpisywanie się; zaawansowane zabezpieczenie integralności

Dostarczany system ma ustawiony poziom ochrony 40, co zapewnia ochronę zasobów i przez wpisywanie się oraz zabezpieczenie integralności. Więcej informacji na ten temat zawiera sekcja “Poziom ochrony 40” na stronie 11.

Poziom ochrony można zmienić za pomocą komendy Praca z wartościami systemowymi (Work with System Values - WRKSYSVAL). Minimalny zalecany poziom, jaki powinien być używany, to 30. Jednak zalecany jest poziom 40 lub wyższy. Zmiana zostanie uwzględniona podczas następnego ładowania programu początkowego (IPL). Tabela 1 zawiera porównanie poziomów ochrony w systemie:

Tabela 1. Poziomy ochrony: porównanie funkcji

Funkcja	Poziom 20	Poziom 30	Poziom 40	Poziom 50
Do wpisania się wymagana jest nazwa użytkownika.	Tak	Tak	Tak	Tak
Do wpisania się wymagane jest hasło.	Tak	Tak	Tak	Tak
Aktywne zabezpieczenie hasłem.	Tak	Tak	Tak	Tak
Aktywne zabezpieczenie menu i programem początkowym.	Tak[1]	Tak[1]	Tak[1]	Tak[1]
Aktywna obsługa ograniczenia możliwości.	Tak	Tak	Tak	Tak
Aktywna ochrona zasobów.	Nie	Tak	Tak	Tak
Dostęp do wszystkich obiektów.	Tak	Nie	Nie	Nie

Tabela 1. Poziomy ochrony: porównanie funkcji (kontynuacja)

Funkcja	Poziom 20	Poziom 30	Poziom 40	Poziom 50
Automatyczne tworzenie profilu użytkownika.	Nie	Nie	Nie	Nie
Dostępność możliwości kontroli ochrony.	Tak	Tak	Tak	Tak
Brak możliwości tworzenia lub ponownego kompilowania programów zawierających instrukcje zastrzeżone.	Tak	Tak	Tak	Tak
Ograniczenie uruchamiania programów, które korzystają z nieobsługiwanych interfejsów.	Nie	Nie	Tak	Tak
Obsługa zaawansowanej sprzętowej ochrony pamięci.	Nie	Nie	Tak	Tak
Biblioteka QTEMP jest obiektem tymczasowym.	Nie	Nie	Nie	Nie
Możliwość tworzenia obiektów *USRSPC, *USRIDX i *USRQ tylko w bibliotekach podanych w wartości systemowej QALWUSRDMN.	Tak	Tak	Tak	Tak
Sprawdzanie wskaźników używanych w parametrach dla programów domeny użytkownika uruchamianych w systemie.	Nie	Nie	Tak	Tak
Narzucanie reguł obsługi komunikatów między systemem a programami użytkownika.	Nie	Nie	Nie	Tak
Ograniczenie możliwości bezpośredniego modyfikowania przestrzeni związanej z programem.	Nie	Nie	Tak	Tak
Zabezpieczenie wewnętrznych bloków sterujących.	Nie	Nie	Tak	Tak[2]

[1] Gdy w profilu użytkownika podano parametr LMTCPB(*YES).

[2] Na poziomie 50 narzucona jest większa ochrona wewnętrznych bloków sterujących, niż na poziomie 40. Patrz “Zapobieganie modyfikowaniu wewnętrznych bloków sterujących” na stronie 17.

Poziom ochrony systemu określa dla każdej klasy użytkownika domyślne uprawnienia specjalne. Podczas tworzenia profilu użytkownika, w oparciu o klasę użytkownika, wybierane są uprawnienia specjalne. Uprawnienia specjalne są dodawane i usuwane także podczas zmiany poziomów ochrony.

Użytkownikowi można nadać następujące uprawnienia specjalne:

***ALLOBJ**
Uprawnienie specjalne do wszystkich obiektów daje użytkownikowi uprawnienie do wykonywania na obiektach wszystkich operacji.

***AUDIT**
Uprawnienie specjalne kontroli umożliwia użytkownikowi definiowanie charakterystyk kontroli systemu, obiektów i użytkowników systemu.

***IOSYSCFG**
Uprawnienie specjalne konfigurowania systemu umożliwia konfigurowanie urządzeń wejściowych i wyjściowych.

***JOBCTL**
Uprawnienie specjalne kontroli zadania umożliwia użytkownikowi sterowanie zadaniami wsadowymi oraz drukowanie.

***SAVSYS**
Uprawnienie specjalne składowania systemu umożliwia składowanie i odtwarzanie obiektów.

***SECADM**
Uprawnienie specjalne administratora ochroną umożliwia użytkownikowi pracę z profilami użytkowników.

***SERVICE**
Uprawnienie specjalne usługi umożliwia użytkownikowi wykonywanie funkcji usług oprogramowania.

***SPLCTL**
Uprawnienie specjalne sterowania buforami umożliwia nieograniczoną kontrolę nad zadaniami wsadowymi i kolejkami wyjściowymi.

Od wersji V5R2 istnieje także możliwość ograniczenia użytkownikom z uprawnieniami *SECADM i *ALLOBJ możliwości zmiany wartości systemowych związanych z ochroną za pomocą komendy CHGSYSVAL. To ograniczenie można określić z poziomu narzędzi SST, za pomocą opcji Praca z ochroną systemu (Work with system security).

Uwaga: To ograniczenie ma zastosowanie do kilku innych wartości systemowych.
Szczegółowe informacje dotyczące ograniczania zmian wartości systemowych oraz pełną listę tych wartości zawiera Rozdział 3: ″Wartości systemowe dotyczące ochrony″.

Tabela 2 zawiera domyślne uprawnienia specjalne dla każdej klasy użytkownika. Pozycje wskazują, że uprawnienie nadawane jest tylko na poziomach ochrony 10 i 20, na wszystkich poziomach ochrony lub wcale.

Tabela 2. Domyślne uprawnienia specjalne dla klas użytkowników według poziomu ochrony

Uprawnienie specjalne	Klasy użytkowników				
	***SECOFR**	***SECADM**	***PGMR**	***SYSOPR**	***USER**
*ALLOBJ	Wszystkie	10 lub 20	10 lub 20	10 lub 20	10 lub 20
*AUDIT	Wszystkie				
*IOSYSCFG	Wszystkie				
*JOBCTL	Wszystkie	10 lub 20	10 lub 20	Wszystkie	
*SAVSYS	Wszystkie	10 lub 20	10 lub 20	Wszystkie	10 lub 20
*SECADM	Wszystkie	Wszystkie			
*SERVICE	Wszystkie				
*SPLCTL	Wszystkie				

Uwaga: Informacje na temat klas użytkowników i uprawnień specjalnych zawierają tematy “Klasa użytkownika” na stronie 63 i “Uprawnienia specjalne” na stronie 68.

Zalecenia:

Zalecany jest poziom ochrony 30 lub wyższy, ponieważ wtedy system nie nadaje automatycznie użytkownikom dostępu do wszystkich zasobów. Na niższych poziomach ochrony wszyscy użytkownicy mają uprawnienia specjalne *ALLOBJ.

Na poziomie ochrony 30 (lub niższym) użytkownicy mają możliwość wywoływania interfejsów systemu, które przełączają ich na profil użytkownika QSECOFR lub umożliwiają dostęp do zasobów, do których normalnie dostęp powinien być niedozwolony. Na poziomie ochrony 40 użytkownicy nie mogą bezpośrednio wywoływać tych interfejsów i dlatego bardzo zalecany jest poziom ochrony 40 lub wyższy.

Poziom ochrony 40 udostępnia dodatkowe zabezpieczenie integralności bez wpływania na wydajność systemu. Aplikacje, które nie działają na poziomie ochrony 40, mają negatywny wpływ na wydajność na poziomie ochrony 30. Powoduje to, że system odpowiada na naruszenia domeny.

Poziom ochrony 50 przeznaczony jest dla systemów z bardzo wysokimi wymaganiami ochrony. Jeśli system działa na poziomie ochrony 50, jest możliwe pogorszenie wydajności spowodowane dodatkowym sprawdzaniem czynności wykonywanych przez system.

Nawet jeśli wszyscy użytkownicy mają mieć dostęp do wszystkich informacji, należy rozważyć korzystanie z poziomu ochrony 30. Do nadania dostępu do informacji można użyć uprawnień publicznych. Korzystanie z poziomu ochrony 30 od samego początku daje możliwość elastycznego zabezpieczania kilku zasobów krytycznych bez konieczności ponownego testowania wszystkich aplikacji.

Poziom ochrony 10

Na poziomie 10 nie ma żadnej ochrony i dlatego poziom 10 **nie jest zalecany** przez IBM. Począwszy od wersji 4 wydania 3 poziomu ochrony nie można ustawić na wartość 10. Jeśli jest ustawiony poziom ochrony 10, po zainstalowaniu wersji 4 wydania 3 system pozostanie na tym poziomie. Po zmianie poziomu ochrony na jakąkolwiek inną wartość nie będzie można go przywrócić.

Gdy wpisuje się nowy użytkownik, system tworzy profil użytkownika o nazwie takiej samej, jak identyfikator użytkownika podany na ekranie wpisywania się. Jeśli ten sam użytkownik wpisze się później z innym identyfikatorem, utworzony zostanie nowy profil użytkownika. Dodatek B zawiera domyślne wartości, które używane są podczas automatycznego tworzenia profilu użytkownika.

System przeprowadza sprawdzanie uprawnień na wszystkich poziomach ochrony. Ponieważ wszystkie profile użytkowników tworzone na poziomie ochrony 10 mają uprawnienia specjalne *ALLOBJ, użytkownicy pomyślnie przechodzą każdą kontrolę uprawnień i mają dostęp do wszystkich zasobów. Jeśli użytkownik chce przetestować efekt przejścia na wyższy poziom ochrony, może usunąć uprawnienia specjalne *ALLOBJ z profili użytkowników i nadać tym profilom uprawnienia do korzystania z określonych zasobów. Jednak nie da to żadnej ochrony. Każdy może wpisać się z nowym identyfikatorem użytkownika, dla którego utworzony zostanie nowy profil z uprawnieniami specjalnymi *ALLOBJ. Na poziomie ochrony 10 nie da się temu zapobiec.

Poziom ochrony 20

Poziom 20 udostępnia następujące funkcje ochrony:

- do wpisania się wymagany jest zarówno identyfikator użytkownika jak i hasło,
- profile użytkowników może tworzyć tylko szef ochrony lub osoba z uprawnieniami specjalnymi *SECADM,
- narzucana jest podana w profilu użytkownika wartość ograniczenia możliwości.

Domyślnie wszystkie profile tworzone na poziomie ochrony 20 mają uprawnienia specjalne *ALLOBJ. Dlatego poziom ochrony 20 **nie jest zalecany** przez IBM.

Zmienianie z poziomu 10 na poziom 20

Podczas zmiany z poziomu 10 na poziom 20, zachowywane są wszystkie profile użytkowników, które na poziomie 10 tworzone były automatycznie. Hasło dla każdego profilu użytkownika jest takie samo, jak nazwa tego profilu. Nie są wprowadzane żadne zmiany w uprawnieniach specjalnych tych profili.

Poniżej zaprezentowano listę zalecanych czynności, które należy wykonać, jeśli planowana jest zmiana poziomu ochrony z 10 na 20:

- za pomocą komendy Wyświetlenie uprawnionych użytkowników (Display Authorized User - DSPAUTUSR) należy utworzyć listę wszystkich profili użytkowników w systemie,
- należy utworzyć nowe profile użytkowników z zestandaryzowanymi nazwami lub skopiować istniejące profile i nadać im nowe, zestandaryzowane nazwy,
- dla każdego istniejącego hasła należy należy ustawić utratę jego ważności, narzucając w ten sposób konieczność przypisania przez użytkowników nowego hasła,
- aby zapobiec ustawieniu prostych haseł, należy ustawić wartość systemową dotyczącą budowy haseł,
- należy zapoznać się z wartościami domyślnymi, które zawiera Tabela 143, patrz Dodatek B, w celu dokonania zmian w profilach automatycznie utworzonych na poziomie ochrony 10.

Zmienianie na poziom 20 z wyższego

Podczas zmiany z wyższego poziomu ochrony na poziom 20, do profili użytkowników dodawane są uprawnienia specjalne. Po wprowadzeniu takiej zmiany użytkownik ma przynajmniej domyślne uprawnienia specjalne dla klasy użytkownika. Tabela 2 na stronie 9 opisuje różnice w uprawnieniach specjalnych miedzy poziomem 20 a wyższymi.

Uwaga: Podczas zmiany na poziom 20 z wyższego poziomu ochrony, system dodaje do każdego profilu użytkownika uprawnienia specjalne *ALLOBJ. Umożliwia to użytkownikom przeglądanie, zmienianie lub usunięcie dowolnego obiektu w systemie.

Poziom ochrony 30

Poziom 30 udostępnia następujące funkcje ochrony (oprócz tych udostępnianych przez poziom 20):

- użytkownicy muszą mieć nadawane uprawnienia do korzystania z zasobów w systemie,
- tylko użytkownik tworzony z klasą ochrony *SECOFR ma nadawane automatycznie uprawnienia specjalne *ALLOBJ.

Zmienianie na poziom 30 z niższych poziomów

Podczas zmiany na poziom ochrony 30 z niższego poziomu, podczas następnego IPL system zmienia wszystkie profile użytkowników. Uprawnienia specjalne, które użytkownik miał nadane na poziomie 10 lub 20, ale nie może ich mieć na poziomie 30 lub wyższym, są usuwane. Uprawnienia specjalne, które użytkownik miał nadane, ale które nie są związane z jego klasą użytkownika, nie są zmieniane. Na przykład uprawnienie specjalne *ALLOBJ zostanie usunięte ze wszystkich profili użytkowników z wyjątkiem tych, które mają klasę użytkownika *SECOFR. Tabela 2 na stronie 9 opisuje listę domyślnych uprawnień specjalnych oraz różnice między poziomami ochrony 10 lub 20 a wyższymi.

Jeśli w systemie aplikacje były uruchamiane na niższym poziomie ochrony, przed zmianą poziomu ochrony na 30 należy skonfigurować i przetestować ochronę zasobów. Poniżej przedstawiono listę zalecanych czynności:

- dla każdej aplikacji należy ustawić odpowiednie uprawnienia do obiektów aplikacji,
- korzystając z aktualnych profili użytkowników lub specjalnych profili testowych, należy przetestować aplikację:
  - z profilu używanego do testowania należy usunąć uprawnienia specjalne *ALLOBJ,
  - profilom użytkowników należy nadać odpowiednie uprawnienia do aplikacji,
  - za pomocą profili użytkowników należy uruchomić aplikację,
  - wyszukując komunikaty o błędach lub korzystając z kroniki kontroli ochrony, należy sprawdzić błędy uprawnień.
- gdy wszystkie aplikacje zostaną uruchomione pomyślnie, wszystkim produkcyjnym profilom użytkowników należy nadać odpowiednie uprawnienia do obiektów aplikacji,
- jeśli wartość systemowa QLMTSECOFR (ograniczanie dostępu dla szefa ochrony) ma wartość 1 (tak), użytkownicy z uprawnieniami specjalnymi *ALLOBJ lub *SERVICE muszą być autoryzowani do korzystania z urządzeń; tym użytkownikom należy nadać uprawnienia *CHANGE do wybranych urządzeń, użytkownikowi QSECOFR uprawnienia *CHANGE lub zmienić wartość systemową QLMTSECOFR na 0,
- w systemie należy zmienić poziom ochrony i wykonać ładowanie programu początkowego (IPL).

Jeśli użytkownik chce zmienić poziom ochrony na 30 bez konieczności definiowania pojedynczych uprawnień do obiektu, należy nadać odpowiednio wysokie uprawnienia publiczne do obiektów aplikacji, aby uruchamiać aplikację. Aby sprawdzić, czy nie pojawiają się błędy uprawnień, należy uruchomić testy aplikacji.

Uwaga: Więcej informacji na temat uprawnień do obiektu zawiera temat “Definiowanie sposobu dostępu do informacji” na stronie 114.

Poziom ochrony 40

Poziom ochrony 40 zapobiega potencjalnym zagrożeniom naruszenia integralności lub ochrony ze strony programów, które mogą obchodzić ochronę w szczególnych przypadkach. Poziom ochrony 50 udostępnia rozszerzone zabezpieczenie integralności dla instalacji ze ścisłymi wymaganiami ochrony. Tabela 3 na stronie 12 opisuje porównanie obsługi funkcji na poziomach 30, 40 i 50. Te funkcje zostały wyjaśnione szczegółowo w następnych sekcjach.

Tabela 3. Porównanie poziomów ochrony 30, 40 i 50

Opis scenariusza	Poziom 30	Poziom 40	Poziom 50
Program próbuje uzyskać dostęp do obiektów za pomocą interfejsów, które nie są obsługiwane.	Pozycja kroniki AF[1]	Pozycja kroniki AF[1]; operacja nie udaje się	Pozycja kroniki AF[1]; operacja nie udaje się
Program próbuje użyć zastrzeżonych instrukcji.	Pozycja kroniki AF[1]	Pozycja kroniki AF[1]; operacja nie udaje się	Pozycja kroniki AF[1]; operacja nie udaje się
Użytkownik wprowadzający zadanie nie ma uprawnień *USE do profilu użytkownika podanego w opisie zadania.	Pozycja kroniki AF[1]	Pozycja kroniki AF[1]; zadanie nie jest uruchamiane.	Pozycja kroniki AF[1]; zadanie nie jest uruchamiane.
Użytkownik próbuje domyślnego wpisania się bez podawania identyfikatora i hasła.	Pozycja kroniki AF[1]	Pozycja kroniki AF[1]; wpisywanie się nie udaje.	Pozycja kroniki AF[1]; wpisywanie się nie udaje.
Program użytkownika *USER próbuje zapisywać w obszarze systemu dysku zdefiniowanego jako tylko do odczytu lub bez dostępu.	Próba udaje się.	Pozycja kroniki AF [1,2]l operacja nie udaje się. [2]	Pozycja kroniki AF [1,2]l operacja nie udaje się. [2]
Przeprowadzona została próba odtworzenia programu, który nie ma wartości sprawdzania. [3]	Sprawdzanie nie jest przeprowadzane. Program musi być ponownie przekonwertowany przed użyciem.	Sprawdzanie nie jest przeprowadzane. Program musi być ponownie przekonwertowany przed użyciem.	Sprawdzanie nie jest przeprowadzane. Program musi być ponownie przekonwertowany przed użyciem.
Przeprowadzona została próba odtworzenia programu, który ma wartość sprawdzania.	Przeprowadzane jest sprawdzanie programu.	Przeprowadzane jest sprawdzanie programu.	Przeprowadzane jest sprawdzanie programu.
Wystąpiła próba zmiany przestrzeni przypisanej do programu.	Próba udaje się.	Pozycja kroniki AF;[1,2] operacja nie udaje się.[2]	Pozycja kroniki AF;[1,2] operacja nie udaje się.[2]
Wystąpiła próba zmiany przestrzeni adresowej zadania.	Próba udaje się.	Pozycja kroniki AF;[1,2] operacja nie udaje się.[2]	Pozycja kroniki AF;[1,2] operacja nie udaje się.[2]
Program użytkownika próbuje wywołać lub przenieść sterowanie do programu domeny systemu.	Próba udaje się.	Pozycja kroniki AF;[1,2] operacja nie udaje się.[2]	Pozycja kroniki AF;[1,2] operacja nie udaje się.[2]
Przeprowadzana jest próba utworzenia obiektu domeny użytkownika typu *USRSPC, *USRIDX lub *USRQ w bibliotece nie zawartej w wartości systemowej QALWUSRDMN.	Operacja nie udaje się.	Operacja nie udaje się.	Operacja nie udaje się.
Program użytkownika wysyła komunikat o wyjątku do programu systemowego, który nie znajduje się bezpośrednio powyżej niego na stosie programów.	Próba udaje się.	Próba udaje się.	Operacja nie udaje się.
Parametr jest przekazywany do programu domeny użytkownika działającego w systemie.	Próba udaje się.	Przeprowadzane jest sprawdzanie parametru.	Przeprowadzane jest sprawdzanie parametru.
Komenda IBM* jest zmieniana za pomocą komendy CHGCMD w celu uruchomienia innego programu. Komenda jest zmieniana ponownie, w celu uruchomienia oryginalnego programu IBM, który jest programem domeny systemu. Użytkownik próbuje uruchomić komendę.	Próba udaje się.	Pozycja kroniki AF;[1,2,4] operacja nie udaje się.[2,4]	Pozycja kroniki AF;[1,2,4] operacja nie udaje się.[2,4]

1 Jeśli funkcja kontroli jest aktywna, w kronice kontroli (QAUDJRN) zapisywana jest pozycja typu AF - błąd uprawnień (authority failure). Więcej informacji na temat funkcji kontroli zawiera Rozdział 9.

2 Jeśli procesor obsługuje zaawansowaną sprzętową ochronę pamięci.

3 Programy utworzone dla wersji wcześniejszych niż Wersja 1 Wydanie 3 nie mają wartości sprawdzania.

4 Jeśli komenda IBM zostanie zmieniona, nie może już wywoływać programu domeny systemu.

Jeśli funkcja kontroli używana jest na niższych poziomach ochrony, system protokołuje pozycje kroniki dla większości działań, które zawiera Tabela 3, z wyjątkiem tych wykrytych przez zaawansowaną funkcję sprzętowej ochrony

pamięci. Dla potencjalnych naruszeń integralności użytkownik otrzyma ostrzeżenia w postaci pozycji kroniki. Na poziomie 40 i wyższym naruszenia integralności powodują, że system nie wykonuje danych operacji.

Zapobieganie użyciu nieobsługiwanych interfejsów

Na poziomie ochrony 40 i wyższym system zapobiega próbom bezpośredniego wywoływania programów systemowych nieudokumentowanych jako interfejsy poziomu wywołania. Na przykład bezpośrednie wywołanie programu przetwarzania komendy dla programu SIGNOFF nie powiedzie się.

Do narzucenia tej ochrony system korzysta z atrybutu domeny obiektu oraz atrybutu stanu programu:

- **Domena:**

  Każdy obiekt należy do domeny *SYSTEM lub *USER. Dostęp do domeny obiektów *SYSTEM możliwy jest tylko przez programy systemowe (*SYSTEM) lub programy dziedziczące (*INHERIT), które są wywoływane przez programy systemowe (*SYSTEM).

  Domenę obiektu można wyświetlić za pomocą komendy Wyświetlenie opisu obiektu (Display Object Description - DSPOBJD) podając parametr DETAIL(*FULL). Można także użyć następujących komend:

  – Wyświetlenie programu (Display Program - DSPPGM) do wyświetlenia domeny programu,
  – Wyświetlenie programu usługowego (Display Service Program - DSPSRVPGM) do wyświetlenia domeny programu usługowego.

- **Stan:**

  Programy mają stan *SYSTEM, *INHERIT lub *USER. Programy użytkownika (*USER) mogą mieć dostęp tylko do obiektów domeny *USER. Dostęp do obiektów, które znajdują się w domenie *SYSTEM, możliwy jest za pomocą odpowiedniej komendy lub interfejsu API. Stany *SYSTEM i *INHERIT zarezerwowane są dla programów IBM.

  Stan programu można wyświetlić za pomocą komendy Wyświetlenie programu (Display Program - DSPPGM). Stan programu usługowego można wyświetlić za pomocą komendy Wyświetlenie programu usługowego (Display Service Program - DSPSRVPGM).

Tabela 4 opisuje reguły dostępu do domeny i stanu:

Tabela 4. Dostęp do domeny i stanu

	Domena obiektu	
Stan programu	***USER**	***SYSTEM**
*USER	TAK	NIE[1]
*SYSTEM	TAK	TAK

1 Naruszenie domeny lub stanu, na poziomie ochrony 40 lub wyższym powoduje, że wykonanie operacji kończy się niepowodzeniem. Na wszystkich poziomach ochrony, jeśli funkcja kontroli jest aktywna, w kronice kontroli zapisywana jest pozycja typu AF.

Pozycja kroniki:

Jeśli funkcja kontroli jest aktywna, a wartość systemowa QAUDLVL ma wartość *PGMFAIL, podczas próby użycia nieobsługiwanego interfejsu w kronice kontroli QAUDJRN zapisywana jest pozycja błędu uprawnień (AF), typ naruszenia D.

Ochrona opisów zadań

Jeśli jako wartość pola *Użytkownik*w opisie zadania używana jest nazwa profilu użytkownika, każde zadanie wprowadzone za pomocą opisu zadania może być uruchomione z atrybutami pobranymi z tego profilu użytkownika. Nieuprawniony użytkownik może użyć opisu zadania w celu naruszenia ochrony, wprowadzając zadanie tak, aby uruchomione zostało za pomocą profilu użytkownika podanego w opisie zadania.

Na poziomie ochrony 40 i wyższym użytkownik wprowadzający zadanie musi mieć uprawnienia *USE do opisu zadania oraz profilu użytkownika podanego w tym opisie, inaczej wykonanie zadania nie powiedzie się. Na poziomie ochrony 30 zadanie jest uruchamiane, jeśli osoba wprowadzająca ma uprawnienia *USE do opisu zadania.

Pozycja kroniki:

Jeśli funkcja kontroli jest aktywna, a wartość systemowa QAUDLVL ma wartość *AUTFAIL, podczas wprowadzania zadania przez użytkownika nieuprawnionego do profilu użytkownika w opisie zadania w kronice kontroli QAUDJRN zapisywana jest pozycja AF typ naruszenia J.

Wpisywanie się bez identyfikatora użytkownika i hasła

Na poziomie ochrony 30 i niższym z pewnymi opisami podsystemów możliwe jest wpisanie się przez naciśnięcie klawisza Enter bez podawania identyfikatora użytkownika i hasła. Na poziomie ochrony 40 i wyższym system zatrzymuje próbę wpisania się bez podania identyfikatora użytkownika i hasła. Więcej informacji na temat zagadnień dotyczących ochrony związanych z opisami podsystemów zawiera temat “Opisy podsystemów” na stronie 185.

Pozycja kroniki:

Gdy użytkownik usiłuje wpisać się bez podania identyfikatora użytkownika i hasła, a opis podsystemu zezwala na to, w kronice QAUDJRN zapisywana jest pozycja AF typ naruszenia S. (Na poziomie ochrony 40 i wyższym taka próba nie powiedzie się.)

Zaawansowana sprzętowa ochrona pamięci

Rozszerzona ochrona pamięci sprzętowej umożliwia definiowanie bloków informacji systemowych znajdujących się na dysku jako do odczytu i zapisu, tylko do odczytu lub bez dostępu. Na poziomie ochrony 40 i wyższym system steruje sposobem, w jaki programy użytkownika (*USER) uzyskują dostęp do tych zabezpieczonych bloków. Ta obsługa nie jest dostępna na poziomach ochrony niższych niż 40.

Zaawansowana sprzętowa ochrona pamięci jest dostępna na wszystkich modelach serwera iSeries, *z wyjątkiem* następujących:

- wszystkie modele B,
- wszystkie modele C,
- modele D: 9402 D04, 9402 D06, 9404 D10 i 9404 D20.

Pozycja kroniki:

Jeśli funkcja kontroli jest aktywna, a wartość systemowa QAUDLVL ma wartość *PGMFAIL, podczas próby zapisu przez program w obszarze dysku zabezpieczonego przez zaawansowaną sprzętową ochronę pamięci, w kronice QAUDJRN zapisywana jest pozycja AF typ naruszenia R. Ta obsługa dostępna jest tylko na poziomie ochrony 40 i wyższym.

Ochrona przestrzeni związanej z programem

Na poziomie ochrony 40 i wyższym program użytkownika nie może bezpośrednio zmieniać związanej przestrzeni obiektu programu.

Ochrona przestrzeni adresowej zadania

Na poziomie ochrony 50 program użytkownika nie może pobrać adresu dla innego zadania w systemie. Dlatego program użytkownika nie może bezpośrednio manipulować obiektami związanymi z innymi zadaniami.

Sprawdzanie parametrów

Interfejsy systemu operacyjnego to programy systemowe w domenie użytkownika. Innymi słowy są to programy, które nie mogą być wywoływane bezpośrednio przez użytkownika. Gdy parametry przekazywane są miedzy programami

użytkownika i systemowymi, to muszą być sprawdzane w celu zabezpieczenia przed zagrożeniem naruszenia integralności systemu operacyjnego przez nieoczekiwane wartości.

Gdy system uruchomiony jest z poziomem ochrony 40 lub 50, sprawdzane są wszystkie parametry przekazywane między programem użytkownika a programem systemowym w domenie użytkownika. Jest to wymagane przez system w celu oddzielenia domeny systemu i użytkownika i spełnienia wymagań poziomu ochrony C2. Dodatkowe sprawdzanie może nieznacznie pogorszyć wydajność.

Sprawdzanie odtwarzanych programów

Podczas tworzenia programu system iSeries oblicza wartość sprawdzania, która przechowywana jest w programie. Podczas odtwarzania programu ta wartość jest obliczana ponownie i porównywana z wartością sprawdzania przechowywaną w programie. Jeśli wartości sprawdzania nie są zgodne, działania podejmowane przez system są sterowane przez wartości systemowe QFRCCVNRST i QALWOBJRST.

Oprócz wartości sprawdzania, program może opcjonalnie mieć podpis cyfrowy weryfikowany podczas operacji odtwarzania. Wszystkie działania systemu związane z podpisami cyfrowymi są sterowane przez wartości systemowe QVFYOBJRST i QFRCCVNRST. Trzy wartości systemowe, sprawdzanie obiektu podczas odtwarzania (QVFYOBJRST), wymuszenie konwersji podczas odtwarzania (QFRCCVNRST) i umożliwienie odtwarzania obiektu (QALWOBJRST), działają jako serie filtrów służących do określenia, czy program będzie odtwarzany bez zmian, czy będzie ponownie tworzony (konwertowany) po odtworzeniu lub czy nie będzie odtworzony w systemie.

Pierwszym filtrem jest wartość systemowa QVFYOBJRST. Kontroluje operację odtwarzania niektórych obiektów, które zostały podpisane cyfrowo. Po pomyślnym sprawdzeniu obiektu i sprawdzeniu jego poprawności przez tę wartość systemową, obiekt przechodzi do drugiego filtru, do wartości systemowej QFRCCVNRST. Ta wartość systemowa umożliwia określenie, czy należy konwertować programy, programy serwisowe oraz obiekty modułów podczas odtwarzania. Ta wartość systemowa zapobiega także odtwarzaniu niektórych obiektów. Obiekty przechodzą do ostatniego filtru, wartości systemowej QALWOBJRST, tylko wtedy, gdy przejdą przez pierwsze dwa filtry. Ta wartość systemowa kontroluje, czy obiekty z atrybutami ochrony mogą być odtwarzane.

Programy tworzone dla systemu iSeries mogą zawierać informacje, które umożliwiają ponowne tworzenie programu podczas odtwarzania, bez konieczności dostarczenia kodu źródłowego programu. Programy utworzone dla systemu iSeries w wersji 5 wydania 1 i nowszych, zawierają informacje wymagane podczas ponownego tworzenia, nawet jeśli obserwowalność programu została usunięta. Programy utworzone dla wydań wcześniejszych niż Wersja 5, Wydanie 1 mogą być ponownie tworzone podczas operacji odtwarzania, jeśli informacje obserwowalne tych programów nie zostały usunięte.

Każda z tych wartości systemowych jest opisana w Rozdziale 3, ″Wartości systemowe dotyczące ochrony″ w sekcji zatytułowanej Wartości systemowe odtwarzania dotyczące ochrony.

Zmienianie poziomu ochrony na 40

Przed migracją do poziomu 40 należy upewnić się, że wszystkie aplikacje można pomyślnie uruchomić na poziomie 30. Poziom ochrony 30 daje możliwość przetestowania ochrony zasobów dla wszystkich aplikacji. Aby migrować od poziomu ochrony 40, należy skorzystać z następującej procedury:

1. Jeśli jeszcze tego nie zrobiono, należy aktywować funkcję kontroli ochrony. Temat “Konfigurowanie kontroli ochrony” na stronie 260 opisuje pełne instrukcje dotyczące konfigurowania funkcji kontroli.
2. Upewnij się, że wartość systemowa QAUDLVL zawiera wartości *AUTFAIL i *PGMFAIL. Wartość *PGMFAIL protokołuje pozycje kroniki dla wszystkich prób dostępu, które naruszają zabezpieczenie integralności na poziomie ochrony 40.
3. Podczas uruchamiania aplikacji na poziomie ochrony 30 monitoruj kronikę kontroli w poszukiwaniu pozycji *AUTFAIL i *PGMFAIL. Zwróć szczególną uwagę na następujące kody przyczyny w pozycjach typu AF:

   B Naruszenie ograniczonej (zablokowanej) instrukcji

   C Niepowodzenie sprawdzania obiektu

   D Naruszenie nieobsługiwanego interfejsu (domeny)

J Niepowodzenie autoryzowania opisu zadania i profilu użytkownika

R Próba dostępu do chronionego obszaru dysku (zaawansowana sprzętowa ochrona pamięci)

S Domyślna próba wpisania się

Te kody wskazują na obecność ryzyka naruszenia integralności w aplikacjach. Na poziomie ochrony 40 uruchomienie tych programów nie powiedzie się.

4. Jeśli istnieją programy utworzone dla wersji wcześniejszych niż wersja 1, wydanie 3, należy użyć komendy CHGPGM z parametrem FRCCRT w celu utworzenia wartości sprawdzania dla tych programów. Na poziomie ochrony 40 system konwertuje każdy program, który jest odtwarzany bez wartości sprawdzania. Podczas odtwarzania może to zająć sporo czasu. Więcej informacji na temat sprawdzania programów zawiera temat “Sprawdzanie odtwarzanych programów” na stronie 15.

   Uwaga: Jako część testowania aplikacji należy odtworzyć biblioteki programów. Należy sprawdzić kronikę kontroli w poszukiwaniu niepowodzenia sprawdzania.
5. W oparciu o pozycje w kronice kontroli, podejmij czynności umożliwiające poprawienie aplikacji i zapobiegające awariom programów.
6. Zmień wartość systemową QSECURITY na wartość 40 i wykonaj IPL.

Wyłączanie poziomu ochrony 40

Po zmianie na poziom ochrony 40 może zaistnieć potrzeba tymczasowego powrotu na poziom 30. Na przykład konieczne może być przetestowanie nowych aplikacji w celu odnalezienia błędów integralności. Użytkownik może również stwierdzić, że przed przejściem na poziom 40 nie przeprowadzono wystarczających testów.

Poziom ochrony można zmienić z 40 na 30 bez narażenia ochrony zasobów. Podczas przechodzenia z poziomu 40 na poziom 30 nie są dokonywane żadne zmiany w uprawnieniach specjalnych profili użytkowników. Po przetestowaniu aplikacji i usunięciu błędów z kroniki kontroli, można powrócić do poziomu 40.

Uwaga: W przypadku przechodzenia z poziomu 40 na poziom 20, do wszystkich profili użytkowników dodawane są niektóre uprawnienia specjalne. (Patrz Tabela 2 na stronie 9.) Powoduje to usunięcie zabezpieczenia ochrony zasobów.

Poziom ochrony 50

Poziom ochrony 50 został zaprojektowany w celu spełnienia wymagań zdefiniowanych przez departament obrony Stanów Zjednoczonych dla ochrony C2. Udostępnia zaawansowane zabezpieczenie integralności, bardziej restrykcyjne niż na poziomie ochrony 40. Uruchomienie systemu na poziomie ochrony 50 wymagane jest dla ochrony C2. Pozostałe wymagania ochrony C2 opisano w książce *Security - Enabling for C2*.

Te funkcje ochrony obejmuje poziom ochrony 50. Opisano je w następujących tematach:

- Ograniczanie typów obiektu domeny użytkownika (*USRSPC, *USRIDX i *USRQ)
- Ograniczanie obsługi komunikatów między programami użytkownika a systemowymi
- Zabezpieczenie przed modyfikowaniem wszystkich wewnętrznych bloków sterujących

Ograniczanie obiektów domeny użytkownika

Większość obiektów tworzonych jest w domenie systemu. Gdy system uruchamiany jest na poziomie ochrony 40 lub 50, dostęp do obiektów domeny systemu może odbywać się jedynie za pomocą udostępnionych komend i funkcji API.

Następujące typy obiektów mogą znajdować się w domenie systemu lub użytkownika:

- przestrzeń użytkownika (*USRSPC),
- indeks użytkownika (*USRIDX),
- kolejka użytkownika (*USRQ).

Obiektami typu *USRSPC, *USRIDX i *USRQ w domenie użytkownika można manipulować bezpośrednio, bez konieczności korzystania z udostępnianych przez system funkcji API oraz komend. Zapewnia to użytkownikowi dostęp do obiektu bez tworzenia rekordu kontroli.

Uwaga: Obiekty typu *PGM, *SRVPGM i *SQLPKG także mogą znajdować się w domenie użytkownika. Ich zawartością nie można manipulować bezpośrednio, a ograniczenia nie mają na nie wpływu.

Na poziomie ochrony 50 użytkownik nie może mieć uprawnień na przekazywanie informacji związanych z ochroną innemu użytkownikowi bez zdolności do wysłania rekordu kontroli. Aby to narzucić:

- na poziomie ochrony 50 żadne zadanie nie może pobrać adresowalności do biblioteki QTEMP dla innego zadania; dlatego jeśli obiekty domeny użytkownika przechowywane są w bibliotece QTEMP, to nie mogą być użyte do przekazania informacji do innego użytkownika,
- Aby zapewnić kompatybilność z istniejącymi aplikacjami, które korzystają z obiektów domeny użytkownika, w wartości systemowej QALWUSRDMN można określić dodatkowe biblioteki. Wartość systemowa QALWUSRDMN narzucana jest na wszystkich poziomach ochrony. Więcej informacji na ten temat zawiera sekcja “Udostępnienie obiektów domeny użytkownika (QALWUSRDMN)” na stronie 21.

Ograniczanie obsługiwania komunikatów

Komunikaty wysyłane między programami stanowią potencjalne ryzyko naruszające integralność. Na poziomie ochrony 50 do obsługi komunikatów mają zastosowanie następujące ograniczenia:

- dowolny program użytkownika może wysłać komunikat dowolnego typu do dowolnego programu innego użytkownika,
- dowolny program systemowy może wysłać komunikat dowolnego typu do dowolnego programu użytkownika lub systemowego,
- program użytkownika może wysłać komunikat inny niż wyjątek do dowolnego programu systemowego,
- program użytkownika może wysłać komunikat o wyjątku (status, powiadomienie lub wyjście) do programu systemowego, gdy spełniony jest jeden z poniższych warunkow:
  - program systemowy jest procesorem żądań,
  - program systemowy wywołał program użytkownika.

  Uwaga: Program użytkownika wysyłający komunikat o wyjątku nie musi być programem wywoływanym przez program systemowy. Na przykład w poniższym stosie programów komunikat o wyjątku może być wysłany do Programu A przez program B, C lub D:

Program A	Systemowy
Program B	Użytkownika
Program C	Użytkownika
Program D	Użytkownika

- Gdy program użytkownika odbiera komunikat z zewnętrznego źródła (*EXT), wszystkie wskaźniki w tekście zastępującym są usuwane.

Zapobieganie modyfikowaniu wewnętrznych bloków sterujących

Na poziomie ochrony 40 i wyższym niektóre wewnętrzne bloki sterujące, takie jak blok sterowania pracą, nie mogą być modyfikowane przez program użytkownika.

Na poziomie ochrony 50 żaden wewnętrzny blok sterujący nie może być modyfikowany. Dotyczy to ścieżki do otwartych danych (ODP), przestrzeni dla komend i programów CL oraz bloku sterującego zadania środowiska systemu S/36.

Zmienianie na poziom ochrony 50

Większość dodatkowych środków bezpieczeństwa, które narzucane są na poziomie ochrony 50, nie powoduje powstawania pozycji kroniki kontroli na niższych poziomach ochrony. Dlatego przed zmianą poziomu ochrony na 50 nie można przetestować aplikacji pod kątem wszystkich możliwych warunków błędów integralności.

Działania powodujące błędy na poziomie ochrony 50 nie są powszechne w normalnych aplikacjach. Większość oprogramowania, które jest pomyślnie uruchamiane na poziomie ochrony 40, uruchomi się także na poziomie 50.

Jeśli system aktualnie działa na poziomie ochrony 30, należy wykonać czynności opisane w sekcji “Zmienianie poziomu ochrony na 40” na stronie 15 w celu przygotowania systemu na zmianę poziomu ochrony.

Jeśli system aktualnie działa na poziomie ochrony 30 lub 40, należy wykonać następujące czynności:

- należy ocenić ustawienia wartości systemowej QALWUSRDMN; kontrolowanie obiektów domeny użytkownika jest ważne dla integralności systemu; patrz sekcja “Ograniczanie obiektów domeny użytkownika” na stronie 16,
- jeśli programy w języku COBOL były kompilowane za pomocą kompilatora starszego niż wersja V2R3, należy ponownie skompilować te, które przypisują urządzenie w warunku SELECT do WORKSTATION,
- należy ponownie skompilować programy w języku COBOL środowiska S/36, które były kompilowane za pomocą kompilatora starszego niż wersja V2R3,
- jeśli programy napisane w języku RPG/400* lub RPG* środowiska System/38 były kompilowane za pomocą kompilatora starszego niż wersja V2R2, a korzystają z wyświetlania zbiorów, należy je skompilować ponownie.

Z poziomu ochrony 30 można bezpośrednio przejść do poziomu 50. Wykorzystywanie poziomu ochrony 40 jako kroku pośredniego nie zapewnia wystarczających korzyści przy testowaniu.

Jeśli system aktualnie działa na poziomie ochrony 40 przejście na poziom 50 nie wymaga dodatkowego testowania. Poziom ochrony 50 nie może być wcześniej testowany. Dodatkowe zabezpieczenie integralności, które narzucane jest przez poziom ochrony 50, na niższych poziomach ochrony nie powoduje powstawania komunikatów o błędach lub pozycji kroniki.

Wyłączanie poziomu ochrony 50

Po zmianie na poziom ochrony 50 może zaistnieć potrzeba tymczasowego powrotu na poziom 30 lub 40. Na przykład konieczne może być przetestowanie nowych aplikacji w celu odnalezienia błędów integralności. Użytkownik może także wykryć problemy związane z integralnością, które nie pojawiają się na niższych poziomach ochrony.

Poziom ochrony można zmienić z 50 na 30 lub 40 bez narażenia ochrony zasobów. Podczas przechodzenia z poziomu 50 na poziom 30 lub 40 nie są dokonywane żadne zmiany w uprawnieniach specjalnych profili użytkowników. Po przetestowaniu aplikacji i usunięciu błędów z kroniki kontroli, można powrócić do poziomu 50.

Uwaga: W przypadku przechodzenia z poziomu 50 na poziom 20, do wszystkich profili użytkowników dodawane są niektóre uprawnienia specjalne. Powoduje to usunięcie zabezpieczenia ochrony zasobów. (Patrz Tabela 2 na stronie 9.)

Rozdział 3. Wartości systemowe dotyczące ochrony

Ten rozdział opisuje wartości systemowe, które sterują ochroną systemu. Wartości systemowe umożliwiają dostosowanie wielu charakterystyk systemu. Grupa wartości systemowych używana jest do definiowania ustawień ochrony dla systemu.

Istnieje możliwość ograniczenia użytkownikom możliwości zmieniania wartości systemowych związanych z ochroną. Narzędzia SST i DST udostępniają opcję blokowania tych wartości systemowych. Przez zablokowanie wartości systemowych można zapobiec zmianie wartości systemowych za pomocą komendy CHGSYSVAL, nawet przez użytkowników z uprawnieniami *SECADM i *ALLOBJ. Oprócz ograniczenia zmian tych wartości, można ograniczyć także dodawanie certyfikatów cyfrowych do bazy certyfikatów cyfrowych za pomocą funkcji API Add Verifier oraz ograniczyć resetowanie hasła bazy certyfikatów cyfrowych.

| **Uwaga:** Jeśli wartości systemowe związane z ochroną zostały zablokowane, to gdy podczas odzyskiwania systemu konieczne jest przeprowadzenie operacji odtwarzania, należy pamiętać o odblokowaniu tych wartości. Zapewnia to możliwość dowolnej zmiany wartości systemowych podczas przeprowadzania IPL.

Za pomocą opcji blokowania można ograniczyć dostęp do następujących wartości systemowych:

Tabela 5. Wartości systemowe, które można zablokować

QALWOBJRST	QAUTORMT	QINACTMSGQ	QPWDLMTREP	QRETSVRSEC
QALWUSRDMN	QAUTOVRT	QLMTDEVSSN	QPWDLVL	QRMTSIGN
QAUDCTL	QCRTAUT	QLMTSECOFR	QPWDMAXLEN	QRMTSRVATR
QAUDENACN	QCRTOBJAUD	QMAXSGNACN	QPWDMINLEN	QSECURITY
QAUDFRCLVL	QDEVRCYACN	QMAXSIGN	QPWDPOSDIF	QSHRMEMCTL
QAUDLVL	QDSPSGNINF	QPWDEXPITV	QPWDRQDDGT	QUSEADPAUT
QAUDLVL2	QDSCJOBITV	QPWDLMTAJC	QPWDRQDDIF	QVFYOBJRST
QAUTOCFG	QFRCCVNRST	QPWDLMTCHR	QPWDVLDPGM	QSCANFS
QSCANFSCTL				

Do blokowania i odblokowywania wartości systemowych związanych z ochroną można użyć narzędzi SST lub DST. Jednak w trybie odtwarzania można użyć tylko narzędzi DST, ponieważ narzędzia SST w tym trybie nie są dostępne. W innych przypadkach można używać także narzędzi SST.

Aby zablokować lub odblokować wartości systemowe związane z ochroną za pomocą komendy Uruchomienie SST (Start System Service Tools - STRSST), należy wykonać następujące czynności:

Uwaga: W celu blokowania lub odblokowywania wartości systemowych związanych z ochroną użytkownik musi mieć profil użytkownika narzędzi serwisowych oraz odpowiednie hasło.

1. Uruchom interfejs znakowy.
2. W wierszu komend wpisz STRSST.
3. Wpisz nazwę użytkownika i hasło dla narzędzi serwisowych.
4. Wybierz opcję 7 (Praca z ochroną systemu).
5. Dla parametru *Allow system value security changes* (Umożliwiaj zmiany wartości systemowych ochrony), aby odblokować wartości systemowe związane z ochroną wpisz 1 lub 2, aby je zablokować.

Aby podczas przeprowadzania nadzorowanego IPL w trakcie odzyskiwania systemu zablokować lub odblokować wartości systemowe związane z ochroną za pomocą narzędzi DST, należy wykonać następujące czynności:

1. Na ekranie IPL lub instalowanie systemu (IPL or Install the System) wybierz opcję 3 (Użyj narzędzi DST).

   Uwaga: W tym kroku przyjęto, że system jest w trybie odzyskiwania oraz wykonywane jest nadzorowane IPL.
2. Wpisz się za pomocą nazwy użytkownika i hasła dla narzędzi DST.
3. Wybierz opcję 13 (Praca z ochroną systemu).
4. Dla parametru *Allow system value security changes* (Umożliwiaj zmiany wartości systemowych ochrony), aby odblokować wartości systemowe związane z ochroną wpisz 1 lub 2, aby je zablokować.

Przedstawione poniżej sekcje omawiają wartości systemowe dotyczące ochrony. Informacje dotyczące wartości systemowych związanych z ochroną, które można zablokować, znajdują się w następujących sekcjach:

- Wartości systemowe ochrony ogólnej
- Wartości systemowe związane z ochroną
- Wartości systemowe odtwarzania związane z ochroną
- Wartości systemowe mające zastosowanie dla haseł
- Wartości systemowe sterowania kontrolą

Wartości systemowe ochrony ogólnej

Przegląd:

Przeznaczenie:
Wartości systemowe, które sterują ochroną systemu.

Sposób używania:
WRKSYSVAL *SEC (Komenda Praca z wartościami systemowymi (Work with System Values))

Uprawnienia:
*ALLOBJ i *SECADM

Pozycja kroniki:
SV

Uwaga:
Zmiany mają natychmiastowy efekt. Przeprowadzenie IPL wymagane jest jedynie podczas zmiany poziomu ochrony (wartość systemowa QSECURITY) lub poziomu hasła (wartość systemowa QPWDLVL).

Poniżej przedstawiono ogólne wartości systemowe, które sterują ochroną systemu:

QALWUSRDMN
Udostępnienie obiektów domeny użytkownika w bibliotekach

QCRTAUT
Tworzenie domyślnych uprawnień publicznych

QDSPSGNINF
Wyświetlenie informacji wpisania się

QFRCCVNRST
Wymuszenie konwersji podczas odtwarzania

QINACTITV
Interwał czasu nieaktywności zadania

QINACTMSGQ
Kolejka komunikatów nieaktywnego zadania

QLMTDEVSSN
Ograniczenie sesji urządzeń

QLMTSECOFR
Ograniczenie dostępu dla szefa ochrony

QMAXSIGN
Maksymalna liczba prób wpisania się

QMAXSGNACN
Działanie podejmowane po przekroczeniu maksymalnej liczby prób wpisania się

QRETSVRSEC
Zachowanie ochrony serwera

QRMTSIGN
Żądania zdalnego wpisania się

| **QSCANFS**
| Skanowanie systemów plików

| **QSCANFSCTL**
| Sterowanie skanowaniem systemów plików

QSECURITY
Poziom ochrony

QSHRMEMCTL
Sterowanie pamięcią współużytkowaną

QUSEADPAUT
Użycie uprawnień adoptowanych

QVFYOBJRST
Sprawdzenie obiektu podczas odtwarzania.

Poniżej znajdują się opisy tych wartości systemowych. Podano wszystkie możliwe opcje. Podkreślone opcje są wartościami domyślnymi. Dla większości wartości systemowych podano wartości zalecane.

Udostępnienie obiektów domeny użytkownika (QALWUSRDMN)

Wartość systemowa QALWUSRDMN określa, które biblioteki mogą przechowywać obiekty domeny użytkownika, takie jak *USRSPC, *USRIDX i *USRQ. Ograniczenie to nie ma zastosowania dla obiektów typu *PGM, *SRVPGM i *SQLPKG. W systemach z wysokimi wymaganiami ochrony konieczne jest ograniczenie dostępu dla obiektów użytkownika *USRSPC, *USRIDX i *USRQ. System nie może kontrolować przenoszenia informacji do i z obiektów domeny użytkownika.

| **Uwaga:** Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać
| zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych,
| należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 6. Możliwe wartości dla wartości systemowej QALWUSRDMN

***ALL**	Obiekty domeny użytkownika mogą znajdować się we wszystkich bibliotekach i katalogach systemu.
***DIR**	Obiekty domeny użytkownika mogą znajdować się we wszystkich katalogach systemu.
nazwa_biblioteki	Nazwy maksymalnie 50 bibliotek, które mogą przechowywać obiekty domeny użytkownika typu *USRSPC, *USRIDX i *USRQ. Jeśli wymieniane są pojedyncze biblioteki, to na liście *musi* znaleźć się biblioteka QTEMP.

Zalecana wartość: Dla większości systemów zalecana jest wartość *ALL. Jeśli system ma wysokie wymagania ochrony, obiekty domeny użytkownika powinny być ograniczone jedynie do biblioteki QTEMP. Na poziomie ochrony 50 biblioteka QTEMP jest obiektem tymczasowym i nie może być używana do przekazywania między użytkownikami poufnych danych.

W niektórych systemach znajdują się aplikacje opierające się na obiektach typu *USRSPC, *USRIDX lub *USRQ. Dla tych systemów lista bibliotek wartości systemowej QALWUSRDMN powinna obejmować biblioteki, które są używane przez dane aplikacje. Uprawnienia publiczne podane dla wartości QALWUSRDMN, z wyjątkiem biblioteki QTEMP, powinny być ustawione na wartość *EXCLUDE. Ogranicza to liczbę użytkowników, którzy mogą korzystać z interfejsu MI, który nie może być kontrolowany, do odczytu lub zmiany danych w obiektach domeny użytkownika znajdujących się w tych bibliotekach.

Uwaga: Podczas uruchamiania komendy Odzyskiwanie pamięci (Reclaim Storage - RCLSTG) może zaistnieć konieczność przenoszenia do i z biblioteki QRCL (odzyskiwania pamięci) obiektów domeny użytkownika. Aby pomyślnie uruchomić komendę RCLSTG, bibliotekę QRCL należy dodać do wartości systemowej QALWUSRDMN. Aby zabezpieczyć ochronę systemu, uprawnienia publiczne do biblioteki QRCL należy ustawić na *EXCLUDE. Po zakończeniu działania komendy RCLSTG, bibliotekę QRCL należy usunąć z listy wartości systemowej QALWUSRDMN.

Uprawnienia do nowych obiektów (QCRTAUT)

Wartość systemowa QCRTAUT używana jest do określania uprawnień publicznych do nowo tworzonych obiektów, jeśli spełnione są następujące warunki:

- wartość systemowa uprawnienia do tworzenia (CRTAUT) dla nowych obiektów ma wartość *SYSVAL,
- nowy obiekt tworzony jest z wykorzystaniem uprawnień publicznych (AUT) *LIBCRTAUT.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 7. Możliwe wartości dla wartości systemowej QCRTAUT

***CHANGE**	Użytkownicy mogą zmieniać nowo tworzone obiekty.
***USE**	Użytkownicy mogą przeglądać, ale nie mogą zmieniać nowo tworzonych obiektów.
***ALL**	Użytkownicy mogą wykonywać dowolne funkcje na nowych obiektach.
***EXCLUDE**	Użytkownicy nie mogą korzystać z nowych obiektów.

Zalecana wartość:
*CHANGE

Wartość systemowa QCRTAUT nie jest wykorzystywana dla obiektów tworzonych w katalogach w rozszerzonym systemie plików.

Uwaga: Kilka bibliotek IBM, w tym biblioteka QSYS, dla wartości systemowej CRTAUT ma ustawioną wartość *SYSVAL. Jeśli wartość systemowa QCRTAUT zostanie zmieniona na inną niż *CHANGE, mogą wystąpić problemy podczas wpisywania się na nowych lub automatycznie tworzonych urządzeniach. Aby uniknąć tych problemów, podczas zmiany wartości systemowej QCRTAUT na wartość inną niż *CHANGE należy upewnić się, że wszystkie opisy urządzeń oraz związane z nimi kolejki komunikatów mają uprawnienia publiczne *CHANGE. Jednym ze sposobów wykonania tego zadania jest zmiana wartości CRTAUT dla biblioteki QSYS z *SYSVAL na *CHANGE.

Wyświetlenie informacji wpisania się (QDSPSGNINF)

Wartość systemowa QDSPSGNINF określa, czy po wpisaniu się wyświetlany jest ekran Informacje wpisania się (Sign-on Information). Ekran Informacje wpisania się (Sign-on Information) zawiera:

- datę ostatniego wpisania się,
- niepoprawne próby wpisania się,
- liczbę dni do wygaśnięcia hasła (jeśli hasło ma wygasnąć za 7 dni lub mniej).

```
                    Informacje wpisania się
                     (Sign-on Information)

                                                          System:
Poprzednie wpisanie się  . . . . . . . . . :   10/30/91  14:15:00

Niepoprawne próby wpisania się . . . . . . :   3

Do wygaśnięcia hasła pozostało dni . . . . :   5
```

| **Uwaga:** Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać
| zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych,
| należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 8. Możliwe wartości dla wartości systemowej QDSPSGNINF

0	Ekran nie jest wyświetlany.
1	Ekran jest wyświetlany.

Zalecana wartość: 1 (ekran jest wyświetlany) jest zalecaną wartością, gdyż dzięki temu użytkownicy mogą monitorować próby użycia ich profili oraz wiedzą, kiedy muszą podać nowe hasło.

Uwaga: Wyświetlanie informacji wpisania się można podać także dla pojedynczych profili użytkowników.

Interwał czasu nieaktywności zadania (QINACTITV)

Wartość systemowa QINACTITV określa w minutach, jak długo system zezwala na pozostawienie nieaktywnego zadania, przed podjęciem działania. Stacja robocza uważana jest za nieaktywną jeśli, oczekuje z wyświetlonym menu lub ekranem lub jeśli oczekuje na komunikat bez ingerencji ze strony użytkownika. Przykład ingerencji użytkownika

- użycie klawisza Enter,
- użycie funkcji stronicowania,
- użycie klawiszy funkcyjnych,
- użycie klawisza pomocy.

Obejmuje to także sesje emulacji programu iSeries Access. Wykluczone są zadania lokalne, które wpisane zostały w systemie zdalnym. Wykluczone są także zadania połączone za pomocą protokołu FTP. W wersjach wcześniejszych niż Wersja 4, Wydanie 2, zadania telnet także były wykluczone. Aby sterować limitem czasu połączeń FTP, należy zmienić parametr INACTTIMO komendy Zmiana atrybutów FTP (Change FTP Attribute - CHGFTPA). Do kontrolowania limitu czasu sesji telnet w wersjach wcześniejszych niż V4R2 służy komenda Zmiana atrybutów TELNET (Change Telnet Attribute - CHGTELNA).

Poniżej przedstawiono przykłady pokazujące, w jaki sposób system określa, które zadania są nieaktywne:

- użytkownik korzysta z funkcji żądania systemowego do uruchomienia drugiego zadania interaktywnego; interakcja z systemem, taka jak naciśnięcie klawisza Enter, dla dowolnego zadania powoduje oznaczenie obu zadań jako aktywne,
- zadanie programu iSeries Access może być dla systemu nieaktywne, jeśli użytkownik wykonuje funkcje komputera PC, takie jak edytowanie dokumentu, które nie ma wpływu na system iSeries.

Wartość systemowa QINACTMSGQ określa jakie działania system podejmuje, gdy upłynie interwał czasu dla nieaktywnego zadania.

Podczas uruchamiania systemu, sprawdza on nieaktywne zadania dla interwału podanego dla wartości systemowej QINACTITV. Na przykład jeśli system został uruchomiony o 9:46 rano, a wartość systemowa QINACTITV jest ustawiona na 30 minut, to system sprawdza nieaktywne zadania o 10:16, 10:46, 11:16 i tak dalej. Jeśli znajdzie zadanie, które było nieaktywne przez 30 minut lub więcej, podejmuje działania określone w wartości systemowej

QINACTMSGQ. W tym przykładzie, jeśli zadanie staje się nieaktywne o godzinie 10:17, nie będzie używane do godziny 11:16. O 10:46 system sprawdzi, że zadanie było nieaktywne tylko przez 29 minut.

Wartości systemowe QINACTITV i QINACTMSGQ zapewniają ochronę przez zabezpieczanie stacji roboczych pozostawionych przez użytkowników. Nieaktywna stacja robocza może umożliwić niepowołanym osobom dostęp do systemu.

Tabela 9. Możliwe wartości dla wartości systemowej QINACTITV

***NONE:**	System nie sprawdza nieaktywnych zadań.
interwał_w_minutach	Należy podać wartość od 5 do 300. Gdy zadanie będzie nieaktywne przez podaną liczbę minut, system podejmie działania określone w wartości systemowej QINACTMSGQ.

Zalecana wartość: 60 minut.

Kolejka komunikatów nieaktywnego zadania (QINACTMSGQ)

Wartość systemowa QINACTMSGQ określa, jakie działanie podejmuje system, gdy interwał czasu nieaktywnego zadania dla zadania zostanie przekroczony.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 10. Możliwe wartości dla wartości systemowej QINACTMSGQ

***ENDJOB**	Zadanie nieaktywne jest zakańczane. Jeśli zadanie nieaktywne jest zadaniem grupowym[1], to wszystkie zadania związane z grupą również są zakańczane. Jeśli zadanie jest częścią zadania alternatywnego[1], zakańczane są oba zadania. Działanie podejmowane przez wartość *ENDJOB jest jednoznaczne z uruchomieniem komendy ENDJOB JOB(nazwa) OPTION (*IMMED) ADLINTJOBS(*ALL) dla zadania nieaktywnego.
***DSCJOB**	Nieaktywne zadanie jest odłączane, a z nim zadania alternatywne lub grupowe[1]. Wartość systemowa interwał czasu odłączonego zadania (QDSCJOBITV) steruje tym, czy system ma zakończyć odłączone zadania. Więcej informacji na ten temat zawiera sekcja “Interwał czasowy przed przerwaniem odłączonych zadań (QDSCJOBITV)” na stronie 33. **Uwaga:** System nie może odłączyć niektórych zadań, takich jak Organizator PC lub funkcja asystenta tekstowego (PCTA). Jeśli system nie może odłączyć nieaktywnego zadania, to kończy je.
nazwa_kolejki_komunikatów	Gdy interwał czasu nieaktywności zadania zostanie przekroczony, do określonej kolejki komunikatów wysyłany jest komunikat CPI1126. Ten komunikat oznacza, że: Zadanie &3/&2/&1; nie było aktywne. Przed podaniem dla wartości systemowej QINACTMSGQ kolejki komunikatów, należy ją utworzyć. Podczas przeprowadzania IPL zawartość tej kolejki jest automatycznie usuwana. Jeśli kolejka QINACTMSGQ zostanie podana jako kolejka komunikatów użytkownika, podczas przeprowadzania IPL wszystkie komunikaty z tej kolejki zostaną utracone.

[1] Zadania grupowe oraz alternatywne zostały opisane w podręczniku *Zarządzanie pracą w systemie AS/400*.

Zalecana wartość: *DSCJOB, chyba że użytkownicy uruchamiają zadania programu iSeries Access. Użycie opcji *DSCJOB, gdy uruchomione są zadania programu iSeries Access jest równoznaczne z ich zakończeniem. Może to powodować znaczną utratę informacji. W przypadku zainstalowanego programu licencjonowanego iSeries Access należy używać opcji *kolejka_komunikatów*. W książce *CL Programming* zaprezentowano przykład pisania programu obsługującego komunikaty.

Używanie kolejki komunikatów: Użytkownik lub program mogą monitorować kolejkę komunikatów i podjąć konieczne działania, takie jak kończenie zadania lub wysyłanie komunikatu ostrzegawczego do użytkownika. Używanie kolejki komunikatów umożliwia podejmowanie decyzji dotyczących poszczególnych urządzeń i profili

użytkowników, zamiast traktowania wszystkich nieaktywnych urządzeń w ten sam sposób. Ta metoda zalecana jest w przypadku używania programu licencjonowanego iSeries Access.

Jeśli nieaktywna jest stacja robocza z dwoma zadaniami alternatywnymi, do kolejki komunikatów wysyłane są dwa komunikaty (jeden dla każdego zadania alternatywnego). Użytkownik lub program może użyć komendy Zakończenie zadania (End Job - ENDJOB), aby zakończyć jedno lub oba takie zadania. Jeśli nieaktywne zadanie ma jedną lub więcej grup zadań, do kolejki komunikatów wysyłany jest pojedynczy komunikat. Komunikaty będą wysyłane do kolejki komunikatów dla każdego interwału, przez który zadanie jest nieaktywne.

Ograniczanie sesji urządzeń (QLMTDEVSSN)

Wartość systemowa QLMTDEVSSN określa, czy użytkownik może wpisać się do więcej niż jednego urządzenia w tym samym czasie. Ta wartość nie ogranicza menu System Request lub drugiego wpisywania się do tego samego urządzenia. Jeśli użytkownik ma odłączone zadanie, to może wpisać się do systemu za pomocą nowej sesji urządzenia.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 11. Możliwe wartości dla wartości systemowej QLMTDEVSSN

0	Liczba sesji wpisywania się nie jest ograniczona.
1	Użytkownicy ograniczeni są do jednej sesji urządzenia.

Zalecana wartość: 1 (tak) ponieważ ograniczenie użytkowników do pojedynczego urządzenia zmniejsza prawdopodobieństwo współużytkowania haseł lub pozostawiania nienadzorowanych stacji roboczych.

Uwaga: Ograniczanie sesji urządzeń można określić także dla pojedynczych profili użytkowników.

Ograniczanie dostępu dla szefa ochrony (QLMTSECOFR)

Wartość systemowa QLMTSECOFR steruje tym, czy użytkownik z uprawnieniami specjalnymi do wszystkich obiektów (*ALLOBJ) lub usługi (*SERVICE), może wpisać się do dowolnej stacji roboczej. Ograniczanie profili użytkowników z dużymi uprawnieniami tylko do dobrze kontrolowanych stacji roboczych zapewnia zabezpieczenie ochrony.

Wartość systemowa QLMTSECOFR narzucana jest tylko na poziomach ochrony 30 i wyższym. Więcej informacji na temat uprawnień wymaganych do wpisania się do stacji roboczej zawiera sekcja “Stacje robocze” na stronie 181.

Bez względu na wartość QLMTSECOFR użytkownik zawsze może się wpisać do konsoli, używając profilu QSECOFR, QSRV lub QSRVBAS.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 12. Możliwe wartości dla wartości systemowej QLMTSECOFR

1	Użytkownik z uprawnieniami specjalnymi *ALLOBJ lub *SERVICE może wpisać się na stacji graficznej tylko wtedy, gdy jest uprawniony (to znaczy ma uprawnienia *CHANGE) do tej stacji lub jeśli profil użytkownika QSECOFR jest uprawniony (ma nadane uprawnienia *CHANGE) do danej stacji graficznej. Te uprawnienia nie mogą pochodzić z uprawnień publicznych.
0	Użytkownicy z uprawnieniami specjalnymi *ALLOBJ lub *SERVICE mogą wpisywać się na dowolnej stacji graficznej, do której mają uprawnienia *CHANGE. Uprawnienia *CHANGE mogą otrzymywać z uprawnień publicznych lub prywatnych lub z uprawnień specjalnych *ALLOBJ.

Zalecana wartość: 1 (tak).

Maksymalna liczba prób wpisania się (QMAXSIGN)

Wartość systemowa QMAXSIGN kontroluje liczbę kolejnych prób wpisania się przez użytkowników lokalnych lub zdalnych, które nie były poprawne. Nieudane próby wpisania się spowodowane są podaniem niepoprawnego ID użytkownika, niepoprawnego hasła lub brakiem odpowiednich uprawnień do korzystania ze stacji roboczej.

Po wyczerpaniu limitu prób wpisania się, wartość systemowa QMAXSGNACN używana jest do określenia, jakie działania należy podjąć. Do kolejki komunikatów QSYSOPR wysyłany jest komunikat (oraz do kolejki QSYSMSG jeśli istnieje w bibliotece QSYS), powiadamiający szefa ochrony o możliwym włamaniu.

Jeśli kolejka komunikatów QSYSMSG została utworzona w bibliotece QSYS, komunikaty dotyczące krytycznych zdarzeń systemowych wysyłane są do niej oraz do kolejki QSYSOPR. Kolejka komunikatów QSYSMSG może być monitorowana oddzielnie przez program lub operatora systemu. Zapewnia to dodatkową ochronę zasobów systemu. Krytyczne komunikaty systemowe w kolejce QSYSOPR są czasem pomijane z powodu ilości komunikatów wysyłanych do tej kolejki.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 13. Możliwe wartości dla wartości systemowej QMAXSIGN

3	Użytkownik może próbować wpisać się maksymalnie 3 razy.
***NOMAX**	Liczba nieudanych prób wpisania się nie jest ograniczona. Taka sytuacja daje potencjalnemu intruzowi nieograniczoną liczbę szans odgadnięcia poprawnej kombinacji ID i hasła użytkownika.
ograniczenie	Należy podać wartość z zakresu od 1 do 25. Zalecaną liczbą prób wpisania się jest trzy. Taka liczba prób jest odpowiednia do poprawienia błędów w pisowni i jednocześnie zabezpiecza przed dostępem użytkowników bez uprawnień.

Zalecana wartość: 3.

Działanie podejmowane po przekroczeniu maksymalnej liczby prób wpisania się (QMAXSGNACN)

Wartość systemowa QMAXSGNACN określa, jakie działanie system podejmie, gdy maksymalna liczba prób wpisania się do danej stacji roboczej zostanie osiągnięta.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 14. Możliwe wartości dla wartości systemowej QMAXSGNACN

3	Wyłączenie profilu użytkownika i urządzenia.
1	Wyłączenie tylko urządzenia.
2	Wyłączenie tylko profilu użytkownika.

System wyłącza urządzenie blokując je. Urządzenie jest blokowane tylko wtedy, gdy nieudane próby wystąpiły jedna po drugiej na tym samym urządzeniu. Jedno poprawne wpisanie się użytkownika resetuje licznik nieudanych prób wpisania się do danego urządzenia.

System wyłącza profil użytkownika zmieniając parametr *Status* na wartość *DISABLED. Profil użytkownika jest wyłączany, gdy liczba niepoprawnych prób wpisania się przekroczy wartość określoną dla danego użytkownika w wartości systemowej QMAXSIGN, niezależnie od tego, czy nieprawidłowe próby wpisania się miały miejsce na tym samym czy różnych urządzeniach. Jedno poprawne wpisanie się resetuje licznik nieudanych prób wpisania się danego użytkownika.

Jeśli w bibliotece QSYS zostanie utworzona kolejka komunikatów QSYSMSG, to wysyłany komunikat (CPF1397) zawiera nazwę użytkownika i urządzenia. Dlatego możliwe jest kontrolowanie wyłączania urządzeń w oparciu o używane urządzenia.

Więcej informacji na temat kolejki komunikatów QSYSMSG zawiera sekcja “Maksymalna liczba prób wpisania się (QMAXSIGN)” na stronie 26.

Jeśli wyłączony zostanie profil QSECOFR, użytkownik może wpisać się za jego pomocą na konsoli, a następnie włączyć go. Jeśli konsola jest zablokowana, a żaden inny użytkownik nie może jej odblokować, w celu udostępnienia konsoli należy wykonać IPL.

Zalecana wartość: 3.

Zachowanie ochrony serwera (QRETSVRSEC)

Wartość systemowa QRETSVRSEC określa, czy możliwe do odszyfrowania informacje o uwierzytelnianiu związane z profilami użytkowników lub pozycjami listy sprawdzania (*VLDL) mogą być zachowane w systemie hosta. Nie obejmuje to hasła profilu użytkownika systemu iSeries.

Jeśli wartość 1 zmieniona zostanie na 0, system wyłączy dostęp do informacji o uwierzytelnianiu. Jeśli wartość zostanie zmieniona ponownie na 1, system umożliwi dostęp do informacji o uwierzytelnianiu.

Informacje o uwierzytelnianiu mogą być usunięte z systemu przez ustawienie wartości systemowej QRETSVRSEC na 0 i uruchomienie komendy CLRSVRSEC (Usuwanie danych ochrony serwera - Clear Server Security Data). Jeśli w systemie znajduje się duża liczba profili użytkowników lub list sprawdzania, komenda CLRSVRSEC może działać przez dłuższy czas.

Pole zaszyfrowanych danych pozycji listy sprawdzania zazwyczaj jest używane do przechowywania informacji o uwierzytelnianiu. Aplikacje określają, czy szyfrowane dane mają być przechowywane w postaci możliwej do odszyfrowania, czy też nie. Jeśli aplikacja nakazuje przechowywanie w postaci możliwej do odszyfrowania, wartość systemowa QRETSVRSEC zmieniana jest z 1 na 0, a zaszyfrowane informacje pola danych nie są dostępne z pozycji. Jeśli zaszyfrowane dane pola pozycji listy sprawdzania przechowywane są w postaci niemożliwej do odszyfrowania, nie ma to wpływu na wartość systemową QRETSVRSEC.

| **Uwaga:** Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 15. Możliwe wartości dla wartości systemowej QRETSVRSEC

0	Dane ochrony serwera nie są zachowywane.
1	Dane ochrony serwera są zachowywane.

Zalecana wartość: 0.

Kontrola zdalnego wpisywania się (QRMTSIGN)

Wartość systemowa QRMTSIGN określa obsługę przez system zdalnych żądań wpisania się do systemu. Przykładami zdalnego wpisania się jest tranzyt terminalu z innego systemu, funkcja stacji roboczej programu licencjonowanego iSeries Access i dostęp za pomocą usługi TELNET.

| **Uwaga:** Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 16. Możliwe wartości dla wartości systemowej QRMTSIGN

***FRCSIGNON**	Żądania zdalnego wpisania się będą podlegać zwykłej procedurze wpisywania się.

Tabela 16. Możliwe wartości dla wartości systemowej QRMTSIGN (kontynuacja)

***SAMEPRF**	Jeśli źródłowa i docelowa nazwa profilu użytkownika są takie same i zgłoszono automatyczne wpisanie się, można pominąć ekran wpisania. Przed użyciem programu tranzytowego system zażąda hasła. Jeśli podczas automatycznego wpisywania się użyte zostanie niepoprawne hasło, to sesja tranzytowa zostanie zakończona, a użytkownik otrzyma komunikat o błędzie. Jednak jeśli nazwy użytkownika nie pokrywają się, wartość *SAMEPRF wskazuje, że system ochrony zakończy sesję bez względu na poprawność hasła. Ekran wpisania się wyświetla się tylko wówczas, gdy nie jest wymagane automatyczne wpisanie się.
***VERIFY**	Opcja *VERIFY umożliwia ominięcie w systemie docelowym ekranu wpisania się, jeśli żądanie automatycznego wpisania się otrzymało poprawne dane dotyczące ochrony. Jeśli hasło profilu użytkownika docelowego nie jest poprawne, to system ochrony zakończy sesję. Jeśli system docelowy ma ustawioną wartość 10 dla QSECURITY, dozwolone są dowolne automatyczne żądania wpisania się. Ekran wpisania się wyświetla się tylko wówczas, gdy nie jest wymagane automatyczne wpisanie się.
***REJECT**	System nie zezwala na zdalne wpisywanie się. W przypadku usługi TELNET, dla opcji *REJECT nie jest podejmowane żadne działanie.
nazwa_programu nazwa_biblioteki	Podczas rozpoczęcia i zakończenia każdej sesji tranzytowej uruchamiany jest podany program.

Zalecana wartość: *REJECT jeśli nie ma być udostępniony tranzyt lub dostęp za pomocą programu iSeries Access. Jeśli tranzyt lub dostęp za pomocą programu iSeries Access ma być dozwolony, należy użyć opcji *FRCSIGNON lub *SAMEPRF.

Szczegółowe informacje na temat wartości systemowej QRMTSIGN zawiera książka *Remote Work Station Support*. Zawiera ona także wymagania dotyczące programu zdalnego wpisywania się oraz przykład.

Skanowanie systemów plików (QSCANFS)

Wartość systemowa skanowanie systemów plików (QSCANFS) umożliwia określenie zintegrowanego systemu plików, którego obiekty mają być przeskanowane. Na przykład można użyć tej opcji do skanowania w poszukiwaniu wirusa. Skanowanie zintegrowanego systemu plików jest włączane, gdy programy obsługi wyjścia rejestrowane są za pomocą punktów wyjścia związanych ze skanowaniem zintegrowanego systemu plików.

Wartość systemowa QSCANFS określa zintegrowane systemy plików, w których obiekty są skanowane, jeśli zarejestrowano programy obsługi wyjścia dla dowolnego z punktów wyjścia powiązanych ze skanowaniem w zintegrowanym systemie plików.

Punkty wyjścia związane ze skanowaniem zintegrowanego systemu plików to:

- QIBM_QP0L_SCAN_OPEN — skanowanie zintegrowanego systemu plików dla otwartego wyjścia,
- QIBM_QP0L_SCAN_CLOSE — skanowanie zintegrowanego systemu plików dla zamkniętego wyjścia.

Więcej informacji na temat zintegrowanych systemów plików znajduje się w temacie Zintegrowany system plików.

Tabela 17. Możliwe wartości dla wartości systemowej QSCANFS.

*NONE	Nie będą skanowane żadne obiekty zintegrowanego systemu plików.
***ROOTOPNUD**	Skanowane będą obiekty typu *STMF znajdujące się w katalogach typu *TYPE2 w systemach plików root(/), QOpenSys i zdefiniowanych przez użytkownika.

Zalecana wartość: Zalecaną wartością jest opcja *ROOTOPNUD, która określa, czy obiekty w systemach plików root(/), QOpenSys i użytkownika mają być skanowane, gdy rejestrowany jest program obsługi wyjścia z punktami wyjścia związanymi ze skanowaniem zintegrowanego systemu plików.

Informacje pokrewne dotyczące tego tematu zawiera sekcja “Sterowanie skanowaniem systemu plików (QSCANFSCTL)”.

Sterowanie skanowaniem systemu plików (QSCANFSCTL)

Wartość systemowa skanowania systemów plików (QSCANFSCTL) steruje skanowaniem zintegrowanego systemu plików, które jest włączane, gdy programy obsługi wyjścia są rejestrowane za pomocą dowolnego punktu wyjścia związanego ze skanowaniem zintegrowanego systemu plików.

Tabela 18. Możliwe wartości dla wartości systemowej QSCANFSCTL.

***NONE**	Nie określono żadnych elementów sterujących dla punktów wyjścia związanych ze skanowaniem zintegrowanego systemu plików.
*ERRFAIL	W razie wystąpienia błędów podczas wywoływania programu obsługi wyjścia (na przykład program nie został odnaleziony lub sygnalizuje błąd) system nie wykona żądania, które wyzwoliło wywołanie programu obsługi wyjścia. Jeśli nie określono żądania, system pominie program obsługi wyjścia i potraktuje to tak, jakby obiekt nie był skanowany.
*FSVRONLY	Skanowany będzie tylko ruch przez serwery plików. Na przykład skanowany będzie dostęp przez system Network File System, a także inne metody serwera plików. Jeśli nie podano tej opcji, skanowany będzie cały dostęp.
*NOFAILCLO	System pomyślnie wykona żądanie zamknięcia z zaznaczeniem niepowodzenia skanowania, nawet jeśli skanowanie obiektu nie powiedzie się, co miało miejsce jako część procesu zamykania. Również ta wartość zastąpi specyfikację *ERRFAIL dla przetwarzania zamykania, ale nie dla innych punktów wyjścia.
*NOPOSTRST	Po odtworzeniu obiekt nie będzie skanowany. Jeśli atrybut obiektu określa, że ″obiekt nie ma być skanowany″, obiekt nie będzie skanowany w żadnym momencie. Jeśli atrybut określa, że ″obiekt ma być skanowany tylko wtedy, gdy został zmodyfikowany od czasu poprzedniego skanowania″, będzie skanowany tylko gdy zostanie zmodyfikowany po odtworzeniu. Jeśli nie wybrano opcji *NOPOSTRST, obiekty będą skanowane przynajmniej raz, po odtworzeniu. Jeśli atrybut obiektu określa, że ″obiekt nie będzie skanowany″, obiekt zostanie przeskanowany raz, po odtworzeniu. Jeśli atrybut obiektu określa, że ″obiekt będzie skanowany tylko wtedy, gdy zostanie zmodyfikowany od czasu poprzedniego skanowania″, obiekt zostanie przeskanowany po odtworzeniu, ponieważ odtwarzanie traktowane jest jako modyfikowanie obiektu. Ogólnie mówiąc odtwarzanie obiektów bez skanowania ich przynajmniej raz może być niebezpieczne. Najlepiej użyć tej opcji tylko wtedy, gdy wiadomo, że obiekty były skanowane przed zeskładowaniem lub że pochodzą z zaufanego źródła.
*NOWRTUPG	System nie podejmie próby aktualizacji praw dostępu dla deskryptora skanowania przesyłanego do programu obsługi wyjścia, aby zawierał uprawnienia do zapisu. Jeśli nie podano inaczej, system podejmie próbę aktualizacji uprawnień do zapisu.
*USEOCOATR	System użyje specyfikacji atrybutu ″tylko zmiana obiektu″ do skanowania tylko obiektów, które zostały zmienione (także nie dlatego, że oprogramowanie skanowania wykazało aktualizację). Jeśli opcja ta nie została wybrana, atrybut ″tylko zmiana obiektu″ nie zostanie użyty, a obiekt zostanie przeskanowany po wprowadzeniu zmian i gdy oprogramowanie skanowania wykaże aktualizację.

Zalecana wartość: Jeśli dla skanowania zintegrowanego systemu plików wymagane są najbardziej restrykcyjne wartości, zalecane ustawienia to *ERRFAIL i *NOWRTUPG. Zapewni to, że wszystkie niepowodzenia programów wyjścia skanowania zabezpieczą związane z nimi operacje, a także nie nadadzą programowi obsługi wyjścia dodatkowych poziomów dostępu. Jednak dla większości użytkowników dobrą opcją jest wartość *NONE. Podczas instalowania kodu dostarczonego z zaufanego źródła, na czas trwania tej instalacji zalecane jest ustawienie wartości *NOPOSTRST.

| Informacje pokrewne dotyczące tego tematu, zawiera sekcja “Skanowanie systemów plików (QSCANFS)” na stronie
| 28.

Sterowanie pamięcią współużytkowaną (QSHRMEMCTL)

Wartość systemowa QSHRMEMCTL definiuje, którzy użytkownicy są uprawnieni do korzystania z pamięci współużytkowanej lub pamięci odwzorowanej, która ma możliwość zapisu. Aby zmienić daną wartość systemową, użytkownik musi mieć uprawnienia specjalne *ALLOBJ i *SECADM. Zmiana tej wartości odnosi natychmiastowy skutek.

| **Uwaga:** Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać
| zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych,
| należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 19. Możliwe wartości dla wartości systemowej QSHRMEMCTL.

0	Użytkownicy nie mogą korzystać z pamięci współużytkowanej lub pamięci odwzorowanej, która ma możliwość zapisu. Ta wartość oznacza, że użytkownicy nie mogą korzystać z funkcji API dla pamięci współużytkowanej (na przykład shmat() — Shared Memory Attach API) oraz nie mogą korzystać z obiektów pamięci odwzorowanej, które mają możliwość zapisu (na przykład taką funkcję udostępnia funkcja API mmap() — Memory Map a File). Tej wartości należy używać w środowiskach z wyższymi wymaganiami ochrony.
1	Użytkownicy mogą korzystać z pamięci współużytkowanej lub pamięci odwzorowanej, która ma możliwość zapisu. Ta wartość oznacza, że użytkownicy mogą korzystać z funkcji API dla pamięci współużytkowanej (na przykład shmat() — Shared Memory Attach API) oraz mogą korzystać z obiektów pamięci odwzorowanej, które mają możliwość zapisu (na przykład taką funkcję udostępnia funkcja API mmap() — Memory Map a File).

Zalecana wartość: 1.

Użycie uprawnień adoptowanych (QUSEADPAUT)

Wartość systemowa QUSEADPAUT definiuje, którzy użytkownicy mogą tworzyć programy, które korzystają z atrybutu uprawnień adoptowanych (*USEADPAUT(*YES)). Wszyscy użytkownicy, uprawnieni przez wartość systemową QUSEADPAUT, jeśli mają wymagane uprawnienia do programu lub programu usługowego, mogą tworzyć lub zmieniać programy oraz programy usługowe, w celu korzystania z uprawnień adoptowanych.

Wartość systemowa może zawierać nazwę listy autoryzacji. Uprawnienia użytkownika sprawdzane są z listą autoryzacji. Jeśli użytkownik ma przynajmniej uprawnienia *USE do używania podanej listy autoryzacji, może tworzyć, zmieniać lub aktualizować programy lub programy usługowe z atrybutem USEADPAUT(*YES). Uprawnienia do listy autoryzacji nie mogą pochodzić z uprawnień adoptowanych.

Jeśli lista autoryzacji wymieniona jest w wartości systemowej i nie istnieje, próba wywołania funkcji nie zostanie zakończona. Wysłany zostanie komunikat informujący o tym błędzie.

Jednak jeśli program tworzony jest za pomocą funkcji API QPRCRTPG, a w szablonie opcji podano wartość *NOADPAUT, program tworzony jest pomyślnie, nawet jeśli lista autoryzacji nie istnieje.

Jeśli w komendzie lub funkcji API wymagana jest więcej niż jedna funkcja, a lista autoryzacji nie istnieje, funkcja nie jest wykonywana. Jeśli uruchamianą komendą jest komenda Utworzenie programu w języku Pascal (Create Pascal Program - CRTPASPGM) lub Utworzenie programu w języku Basic (Create Basic Program - CRTBASPGM), wynikiem jej działania jest sprawdzenie funkcji.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 20. Możliwe wartości dla wartości systemowej QUSEADPAUT

nazwa listy autoryzacji	Komunikat diagnostyczny jest wysyłany, aby wskazać, że program tworzony jest z użyciem opcji USEADPAUT(*NO), jeśli spełnione są następujące warunki: • dla wartości systemowej QUSEADPAUT podano listę autoryzacji, • użytkownik nie ma uprawnień do wspomnianej powyżej listy autoryzacji, • podczas tworzenia programu lub programu usługowego nie wystąpiły inne błędy.
***NONE**	Wszyscy użytkownicy, jeśli mają wymagane uprawnienia do programu lub programu usługowego, mogą tworzyć lub zmieniać programy lub programy usługowe, w celu korzystania z uprawnień adoptowanych.

Zalecana wartość: Dla komputerów produkcyjnych, należy utworzyć listę autoryzacji z uprawnieniami *PUBLIC(*EXCLUDE). Należy ją podać w wartości systemowej QUSEADPAUT. Zapobiegnie to możliwości tworzenia programów, które korzystają z uprawnień adoptowanych.

Przed utworzeniem listy autoryzacji dla wartości systemowej QUSEADPAUT należy uważnie rozważyć projekt ochrony dla aplikacji. Jest to szczególnie ważne w środowiskach, w których tworzone są aplikacje.

Wartości systemowe związane z ochroną

Przegląd:

Przeznaczenie:
Wartości systemowe, które są związane z ochroną systemu.

Sposób używania:
WRKSYSVAL (Komenda Praca z wartościami systemowymi - Work with System Values)

Uprawnienia:
*ALLOBJ i *SECADM

Pozycja kroniki:
SV

Uwaga:
Zmiany mają natychmiastowy efekt. Przeprowadzenie IPL nie jest wymagane.

Poniżej przedstawiono opisy dodatkowych wartości systemowych, które związane są z ochroną systemu. Nie są one uwzględnione w grupie *SEC na ekranie Praca z wartościami systemowymi (Work with System Values).

QAUTOCFG
Automatyczne konfigurowanie urządzeń

QAUTOVRT
Automatyczne konfigurowanie urządzeń wirtualnych

QDEVRCYACN
Działanie odzyskiwania urządzenia

QDSCJOBITV
Interwał czasowy przed przerwaniem odłączonych zadań

Uwaga: Ta wartość systemowa została omówiona także w Centrum informacyjnym (więcej szczegółów zawiera sekcja “Informacje wstępne i pokrewne” na stronie xvi).

QRMTSRVATR
Atrybut zdalnej usługi

Poniżej znajdują się opisy tych wartości systemowych. Dla każdej z nich zaprezentowano możliwe opcje do wyboru. Podkreślone opcje są wartościami domyślnymi.

Automatyczne konfigurowanie urządzenia (QAUTOCFG)

Wartość systemowa QAUTOCFG automatycznie konfiguruje urządzenia podłączone lokalnie. Umożliwia automatyczne konfigurowanie urządzeń dodawanych do systemu.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 21. Możliwe wartości dla wartości systemowej QAUTOCFG

0	Automatyczne konfigurowanie jest wyłączone. Wszystkie nowe kontrolery lub urządzenia, które dodawane są do systemu, muszą być konfigurowane ręcznie.
1	Automatyczne konfigurowanie jest włączone. Nowe lokalne kontrolery lub urządzenia, które są dodawane do systemu, konfigurowane są automatycznie. Operator otrzymuje komunikat, który wskazuje zmiany w konfiguracji systemu.

Zaleca wartość: Przy inicjowaniu procesu konfigurowania systemu lub dodawaniu wielu nowych urządzeń, wartość systemowa powinna być ustawiona na 1. W pozostałych przypadkach wartość ta powinna być ustawiona na 0.

Automatyczne konfigurowanie urządzeń wirtualnych (QAUTOVRT)

Wartość systemowa QAUTOVRT określa, czy urządzenia wirtualne tranzytu oraz pełnoekranowe urządzenie wirtualne TELNET (jako przeciwieństwo urządzenia wirtualnego stacji roboczej) są konfigurowane automatycznie.

Urządzenie wirtualne to opis urządzenia, z którym nie jest skojarzony sprzęt fizyczny. Używa się go w celu nawiązania połączenia między użytkownikiem i fizyczną stacją roboczą w systemie zdalnym.

Zgoda na automatyczne konfigurowanie urządzeń wirtualnych ułatwia włamywanie się do systemu przy użyciu tranzytu lub usługi telnet. Jeśli automatyczne konfigurowanie nie jest aktywne, to użytkownik usiłujący się włamać ma ograniczoną liczbę prób dostępu do każdego urządzenia wirtualnego. Liczba ta definiowana jest przez szefa ochrony za pomocą wartości systemowej QMAXSIGN. Jeśli automatyczne konfigurowanie jest aktywne, liczba ta jest wyższa. Systemowa liczba prób wpisania się mnożona jest przez liczbę urządzeń wirtualnych, które mogą być utworzone przez obsługę automatycznego konfigurowania. Ta obsługa zdefiniowana jest przez wartość systemową QAUTOVRT.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 22. Możliwe wartości dla wartości systemowej QAUTOVRT

0	Urządzenia wirtualne nie są tworzone automatycznie.
liczba_urządzeń_ wirtualnych	Należy podać wartość od 1 do 9999. Jeśli do kontrolera wirtualnego dołączonych jest mniej urządzeń niż podana liczba i użytkownik nie ma dostępu do tranzytu lub pełnoekranowej usługi telnet, to system sam skonfiguruje nowe urządzenie.

Zalecana wartość: 0.

Więcej informacji na temat korzystania z terminalu tranzytu zawiera podręcznik *Remote Work Station Support*. Więcej informacji na temat usługi TELNET zawiera podręcznik *TCP/IP Configuration and Reference*.

Działanie odzyskiwania urządzenia (QDEVRCYACN)

Wartość QDEVRCYACN określa, jakie działanie ma zostać podjęte w przypadku wystąpienia błędu we/wy dla stacji roboczej pracującej interaktywnie.

| **Uwaga:** Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać
| zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych,
| należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 23. Możliwe wartości dla wartości systemowej QDEVRCYACN

***DSCMSG**	Zadanie zostanie odłączone. Kiedy użytkownik ponownie się wpisze, do aplikacji użytkownika wysłany zostanie komunikat o błędzie.
***MSG**	Wysyła komunikat o błędzie we/wy do aplikacji użytkownika. Program wykona odzyskiwanie po błędzie.
***DSCENDRQS**	Zadanie zostanie odłączone. Kiedy użytkownik ponownie się wpisze, nastąpi anulowanie żądania, w wyniku którego sterowanie zadaniem powróci do ostatniego poziomu żądania.
***ENDJOB**	Zadanie zostanie zakończone. Utworzony będzie protokół zadania. Do protokołu zadania i protokołu QHST jest wysyłany komunikat informujący, że zadanie zostało zakończone z powodu błędu urządzenia. Aby zminimalizować wpływ na wydajność kończonego zadania, jego priorytet jest obniżany do 10, wartość przedziału czasu jest ustawiana na 100 milisekund, a wartością atrybutu usuwania staje się YES.
***ENDJOBNOLIST**	Zadanie zostanie zakończone. Nie zostanie utworzony protokół zadania. Do protokołu QHST wysyłany jest komunikat informujący, że zadanie zostało zakończone z powodu wystąpienia błędu urządzenia.

Gdy wybrano opcję *MSG lub *DSCMSG, działanie odzyskiwania urządzenia wykonywane jest dopiero po następnej operacji we/wy wykonanej przez zadanie. W środowisku LAN/WAN umożliwia to odłączenie jednego urządzenia i podłączenie innego z użyciem tego samego adresu, zanim wystąpi kolejna operacja we/wy dla zadania. Zadanie może kontynuować pracę po wystąpieniu błędu we/wy i działać nadal z drugim urządzeniem. Aby tego uniknąć, należy podać parametr *DSCENDRQS, *ENDJOB lub *ENDJOBNOLIST. Działania te są wykonywane natychmiast po wystąpieniu błędu we/wy, takiego jak odłączenie zasilania.

Zalecana wartość:
*DSCMSG

Uwaga: Aby zmienić tę wartość, nie są wymagane uprawnienia specjalne *ALLOBJ i *SECADM.

W wersjach wcześniejszych niż wersja 3 wydanie 6 wartością domyślną była opcja *MSG. Pozostawienie opcji *MSG powoduje powstanie potencjalnego ryzyka naruszenia ochrony.

Interwał czasowy przed przerwaniem odłączonych zadań (QDSCJOBITV)

Wartość systemowa QDSCJOBITV określa, czy i kiedy system zakończy odłączone zadanie. Interwał podany jest w minutach.

Jeśli wartość systemowa QINACTMSGQ zostanie ustawiona tak, aby zadanie było odłączane (*DSCJOB), wartość QDSCJOBITV należy tak ustawić, aby ewentualnie odłączone zadanie było zakańczane. Odłączone zadanie korzysta z zasobów systemu, a także zachowuje blokady na obiektach.

| **Uwaga:** Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać
| zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych,
| należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 24. Możliwe wartości dla wartości systemowej QDSCJOBITV

240	System zakończy odłączone zadanie po 240 minutach.
***NONE**	System nie zakończy automatycznie odłączonego zadania.
czas_w_minutach	Należy podać wartość od 5 do 1440.

Zalecana wartość: 120.

Atrybut zdalnej usługi (QRMTSRVATR)

Wartość systemowa QRMTSRVATR steruje możliwością przeprowadzenia zdalnej analizy problemu, który wystąpił w systemie. Umożliwia zdalne analizowanie systemu.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Wartości dozwolone dla wartości systemowej QRMTSRVATR to:

Tabela 25. Możliwe wartości dla wartości systemowej QRMTSRVATR

0	Atrybut zdalnej usługi jest wyłączony.
1	Atrybut zdalnej usługi jest włączony.

Zalecana wartość: 0.

Więcej informacji na temat zdalnego dostępu oraz wartości systemowej QRMTSRVATR zawiera sekcja “Ochrona za pomocą blokady” na stronie 2.

Wartości systemowe odtwarzania związane z ochroną

Przegląd:

Przeznaczenie:
Steruje tym, jak i czy obiekty związane z ochroną odtwarzane są w systemie.

Sposób używania:
WRKSYSVAL*SEC (komenda Praca z wartościami systemowymi)

Uprawnienia:
*ALLOBJ i *SECADM

Pozycja kroniki:
SV

Uwaga:
Zmiany mają natychmiastowy efekt. Przeprowadzenie IPL nie jest wymagane.

Poniżej przedstawiono opisy wartości systemowych, które związane są z odtwarzaniem obiektów związanych z ochroną, które także należy wziąć pod uwagę podczas odtwarzania obiektów. Więcej informacji dotyczących wartości systemowej QSCANFSCTL *NOPOSTRST znajduje się w temacie Tabela 18 na stronie 29.

QVFYOBJRST
Sprawdzenie obiektu podczas odtwarzania.

QFRCCVNRST
Wymuszenie konwersji podczas odtwarzania

QALWOBJRST
Zezwolenie na odtwarzanie obiektów istotnych dla ochrony.

Poniżej znajdują się opisy tych wartości systemowych. Dla każdej z nich zaprezentowano możliwe opcje do wyboru. Podkreślone opcje są wartościami domyślnymi.

Sprawdzenie obiektu podczas odtwarzania (QVFYOBJRST)

Wartość systemowa QVFYOBJRST określa, czy obiekty muszą mieć podpisy cyfrowe, aby mogły zostać odtworzone w systemie. Istnieje możliwość zablokowania odtwarzania obiektu, chyba że ten obiekt ma poprawny podpis cyfrowy

od zaufanego dostawcy oprogramowania. Ta wartość ma zastosowanie dla obiektów typu: *PGM, *SRVPGM, *SQLPKG, *CMD i *MODULE. Stosowana jest także dla obiektów *STMF, które zawierają programy w języku Java.

Gdy podejmowana jest próba odtworzenia obiektu w systemie, trzy wartości systemowe współpracują ze sobą jako filtry w celu określenia, czy określony obiekt ma zostać odtworzony. Pierwszym filtrem jest wartość systemowa sprawdzająca podpisy obiektów podczas odtwarzania (QVFYOBJRST). Jest ona wykorzystywana do kontrolowania odtwarzania niektórych obiektów, które można podpisać cyfrowo. Drugim filtrem jest wartość systemowa narzucania konwersji podczas odtwarzania (QFRCCVNRST). Ta wartość systemowa umożliwia ustalenie, czy należy konwertować programy, programy serwisowe, pakiety SQL oraz moduły podczas odtwarzania. Może ona również uniemożliwić odtwarzanie niektórych obiektów. Jedynie obiekty pozytywnie zweryfikowane przez dwa pierwsze filtry są przetwarzane przez trzeci filtr. Trzecim filtrem jest wartość systemowa umożliwiająca odtwarzanie obiektu (QALWOBJRST). Określa ona, czy można odtworzyć obiekty z atrybutami zależnymi od ochrony.

Jeśli w systemie nie jest zainstalowany program DCM (opcja 34 OS/400), podczas określania wpływu wartości QVFYOBJRST na odtwarzanie, wszystkie obiekty, poza tymi podpisanymi przez zaufane źródło, traktowane są jako niepodpisane.

Zmiana tej wartości odnosi natychmiastowy skutek.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Uwaga

Nowy system dostarczany jest z wartością systemową QVFYOBJRST ustawianą na wartość 3. Po zmianie wartości QVFYOBJRST, przed zainstalowaniem nowego wydania systemu operacyjnego OS/400 ważne jest jej ponowne ustawienie na wartość 3 lub niższą.

Tabela 26. Możliwe wartości dla wartości systemowej QVFYOBJRST

1	Nie sprawdzaj podpisów podczas odtwarzania. Odtwarzaj wszystkie obiekty w zależności od ich podpisów. Wartości tej nie należy używać, chyba że odtwarzane mają być podpisane obiekty, dla których z jakichś przyczyn sprawdzanie podpisu nie powiedzie się.
2	Sprawdzaj obiekty podczas odtwarzania. Odtwarzaj niepodpisane komendy i obiekty użytkownika. Odtwarzaj podpisane komendy i obiekty użytkownika, nawet jeśli podpisy nie są poprawne. Ta wartość powinna być używana tylko wtedy, gdy istnieją specyficzne obiekty, które mają być odtwarzane, a które mają nieprawidłowe podpisy. Ogólnie mówiąc niebezpiecznie jest odtwarzać obiekty z nieprawidłowymi podpisami.
3	Sprawdzaj podpisy podczas odtwarzania. Odtwarzaj niepodpisane komendy i obiekty użytkownika. Odtwarzaj podpisane komendy i obiekty użytkownika tylko wówczas, gdy podpis jest poprawny. Tej wartości można użyć podczas normalnych operacji, jeśli część z ładowanych obiektów nie ma podpisu, ale użytkownik chce mieć pewność, że wszystkie podpisane obiekty mają poprawne podpisy. Komendy i programy utworzone lub zakupione zanim podpisy cyfrowe były dostępne, nie będą podpisane. Ta wartość umożliwia odtworzenie takich komend i programów. Jest to wartość domyślna.

Tabela 26. Możliwe wartości dla wartości systemowej QVFYOBJRST (kontynuacja)

4	Sprawdzaj podpisy podczas odtwarzania. Nie odtwarzaj niepodpisanych obiektów użytkownika. Odtwarzaj podpisane komendy i obiekty użytkownika, nawet jeśli podpisy nie są poprawne. Ta wartość powinna być używana tylko wtedy, gdy istnieją specyficzne obiekty z nieprawidłowymi podpisami, które użytkownik chce odtworzyć, ale nie chce odtwarzać obiektów, które mogą być niepodpisane. Ogólnie mówiąc niebezpiecznie jest odtwarzać obiekty z nieprawidłowymi podpisami.
5	Sprawdzaj podpisy podczas odtwarzania. Nie odtwarzaj niepodpisanych obiektów użytkownika. Odtwarzaj podpisane komendy i obiekty użytkownika tylko wówczas, gdy podpis jest poprawny. Ta wartość jest najbardziej restrykcyjna i powinna być używana, gdy odtwarzane są obiekty podpisane przez zaufane źródło.

Obiekty systemowe oraz dziedziczone muszą posiadać poprawne podpisy pochodzące z zaufanego źródła. Jedyną wartością, jaka umożliwia obiektom systemowym lub dziedziczonym odtwarzanie bez poprawnego podpisu, jest wartość 1. Uruchomienie takiej komendy lub programu stanowi zagrożenie dla integralności systemu. Jeśli zachodzi potrzeba zmiany wartości systemowej QVFYOBJRST na 1 w celu umożliwienia odtwarzania takiego obiektu w systemie, należy pamiętać, aby po zakończeniu odtwarzania obiektu przywrócić tej wartości poprzednie ustawienie.

Niektóre komendy używają podpisu, który nie obejmuje wszystkich części obiektu. Niektóre części komendy nie są podpisane, zaś inne są podpisane tylko wówczas gdy zawierają wartość inną niż wartość domyślna. Taki typ podpisu umożliwia wprowadzenie pewnych zmian w komendzie bez unieważniania jej podpisu. Przykłady zmian, które nie spowodują unieważnienia tych typów podpisu, są następujące:

- zmiana ustawień domyślnych komendy,
- dodawanie programu sprawdzania poprawności do komendy, która nie posiada jeszcze takiego programu,
- zmiana parametru ’Dozwolone środowisko wykonania’,
- zmiana parametru ’Zezwolenie na ograniczenie użytkowników’.

Istnieje możliwość dodania własnego podpisu do komend, które zawierają te elementy obiektu komendy.

Zalecana wartość: 3.

Wymuszenie konwersji podczas odtwarzania (QFRCCVNRST)

Ta wartość systemowa umożliwia ustalenie, czy należy konwertować poniższe typy obiektów podczas odtwarzania:

- program (*PGM),
- program usługowy (*SRVPGM),
- pakiet SQL (*SQLPKG),
- moduł (*MODULE).

Może ona również uniemożliwić odtwarzanie niektórych obiektów. Obiekt, dla którego w wartości systemowej określono konwertowanie, a który nie może być konwertowany, ponieważ nie zawiera wystarczającej ilości danych do tworzenia, nie zostanie odtworzony.

Wartość *SYSVAL dla parametru FRCOBJCVN komend odtwarzania (RST, RSTLIB, RSTOBJ, RSTLICPGM) korzysta z tej wartości systemowej. Dlatego zmieniając wartość QFRCCVNRST można włączyć lub wyłączyć konwertowanie dla całego systemu. Jednak w niektórych przypadkach parametr FRCOBJCVN przesłania wartość systemową. Podanie wartości *YES i *ALL dla parametru FRCOBJCVN spowoduje przesłonięcie wszystkich ustawień wartości systemowej. Podanie wartości *YES i *RQD dla parametru FRCOBJCVN ma takie samo znaczenie, jak podanie wartości ’2’ dla tej wartości systemowej, i powoduje przesłonięcie tej wartości, gdy ma ona wartość ’0’ lub ’1’.

Wartość systemowa QFRCCVNRST jest drugą z trzech wartości systemowych, które działają kolejno jako filtry określające, czy obiekt może być odtworzony lub czy ma być konwertowany podczas odtwarzania. Pierwszy filtr, wartość systemowa sprawdzania obiektu podczas odtwarzania (QVFYOBJRST), steruje odtwarzaniem niektórych obiektów, które mogą być podpisane cyfrowo. Jedynie obiekty pozytywnie zweryfikowane przez dwa pierwsze filtry są przetwarzane przez trzeci filtr, wartość systemową umożliwiającą odtwarzania obiektów (QALWOBJRST), która określa, czy obiekty z atrybutami istotnymi dla ochrony mogą być odtwarzane.

Wartością domyślną dla wartości systemowej QFRCCVNRST jest 1. Dla wszystkich wartości QFRCCVNRST, obiekt, który powinien być konwertowany, ale nie może być, nie zostanie odtworzony. Obiekty podpisane cyfrowo przez zaufane źródło systemu odtwarzane są bez konwertowania, bez względu na ustawienia tej wartości systemowej.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Przedstawiona poniżej tabela zawiera podsumowanie wartości dozwolonych dla QFRCCVNRST:

Tabela 27. Wartości możliwe wartości dla wartości systemowej QFRCCVNRST

0	Nie konwertuj niczego. Nie zapobiegaj odtwarzaniu.
1	Konwertowane będą obiekty z błędami sprawdzania.
2	Obiekty będą konwertowane, jeśli wymaga tego bieżący system operacyjny lub mają błędy sprawdzania.
3	Konwertowane będą obiekty, dla których istnieje podejrzenie, że były manipulowane, które zawierają błędy sprawdzania oraz obiekty, które wymagają konwertowania w celu używania ich w bieżącej wersji systemu operacyjnego.
4	Konwertowane będą obiekty, które zawierają wystarczającą ilość danych do tworzenia dla konwertowania i które nie mają poprawnych podpisów cyfrowych. Obiekty, które nie zawierają wystarczających danych do tworzenia, będą odtwarzane bez konwertowania. UWAGA: Konwertowane będą obiekty (podpisane i niepodpisane), dla których istnieje podejrzenie manipulacji ze względu na błędy sprawdzania lub wymagające konwersji w celu użycia w bieżącej wersji systemu operacyjnego; w przypadku niepowodzenia konwersji obiekty te nie zostaną odtworzone.
5	Konwertowane będą obiekty zawierające wystarczającą ilość danych do tworzenia. Obiekt, który nie zawiera wystarczającej ilości danych, zostanie odtworzony. UWAGA: Obiekty (podpisane i niepodpisane), dla których istnieje podejrzenie, że były zmieniane - ze względu na błędy sprawdzania - lub wymagające konwersji w celu użycia w bieżącej wersji systemu operacyjnego, a które nie mogą być konwertowane, nie zostaną odtworzone.
6	Konwertowane będą wszystkie obiekty, które nie mają poprawnego podpisu cyfrowego. UWAGA: Konwertowany będzie obiekt z poprawnym podpisem cyfrowym, który ma błędy sprawdzania lub istnieje podejrzenie manipulacji, a w przypadku braku możliwości jego konwertowania, nie zostanie on odtworzony.
7	Konwertowany będzie każdy obiekt.

Gdy obiekt jest konwertowany, jego podpis cyfrowy jest usuwany. Konwertowany obiekt jest obiektem użytkownika. Konwertowane obiekty będą miały dobrą wartość sprawdzania i nie będzie istniało dla nich podejrzenie manipulacji.

Zalecana wartość: 3 lub wyższa.

Zezwolenie na odtwarzanie obiektów istotnych dla ochrony (QALWOBJRST)

Wartość systemowa QALWOBJRST określa, czy w systemie mogą być odtwarzane obiekty, które są istotne dla ochrony. Można jej użyć, aby uniemożliwić każdemu użytkownikowi odtwarzanie obiektu systemowego lub obiektu adoptującego uprawnienia.

Gdy podejmowana jest próba odtworzenia obiektu w systemie, trzy wartości systemowe współpracują ze sobą jako filtry w celu określenia, czy określony obiekt ma zostać odtworzony lub czy poddany zostanie konwersji podczas

odtwarzania. Pierwszym filtrem jest wartość systemowa sprawdzająca podpisy obiektów podczas odtwarzania (QVFYOBJRST). Wykorzystywana ona jest do kontrolowania odtwarzania niektórych obiektów, które można podpisać cyfrowo. Drugim filtrem jest wartość systemowa narzucania konwersji podczas odtwarzania (QFRCCVNRST). Ta wartość systemowa umożliwia ustalenie, czy należy konwertować programy, programy serwisowe, pakiety SQL oraz moduły podczas odtwarzania. Może ona również uniemożliwić odtwarzanie niektórych obiektów. Jedynie obiekty pozytywnie zweryfikowane przez dwa pierwsze filtry są przetwarzane przez trzeci filtr. Trzecim filtrem jest wartość systemowa umożliwiająca odtwarzanie obiektu (QALWOBJRST). Określa ona, czy można odtworzyć obiekty z atrybutami zależnymi od ochrony.

W nowym systemie wartość systemowa QALWOBJRST ustawiona jest na *ALL. Jest ona wymagana, aby pomyślnie zainstalować system.

UWAGA: Przed przeprowadzeniem wymienionych poniżej czynności, ważne jest, aby wartość systemową QALWOBJRST ustawić na *ALL:

- instalowanie nowego wydania programu licencjonowanego OS/400,
- instalowanie nowych programów licencjonowanych,
- odtwarzanie systemu.

Jeśli wartość QALWOBJRST nie jest ustawiona na *ALL, te czynności mogą się nie powieść. Aby zapewnić ochronę systemu, po zakończeniu czynności systemowych wartość QALWOBJRST należy ustawić do normalnego poziomu.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Dla wartości systemowej QALWOBJRST można podać kilka wartości, chyba że podano wartość *ALL lub *NONE.

Tabela 28. Możliwe wartości dla wartości systemowej QALWOBJRST.

***ALL**	Użytkownik z odpowiednimi uprawnieniami może odtworzyć na systemie dowolny obiekt.
***NONE**	Obiekty istotne dla ochrony, takie jak programy systemowe lub programy adoptujące uprawnienia, nie mogą być odtwarzane.
***ALWSYSSTT**	Mogą być odtwarzane obiekty typu system-state i inherit-state.
***ALWPGMADP**	Mogą być odtwarzane obiekty, które adoptują uprawnienia.
***ALWPTF**	Podczas instalowania poprawki PTF mogą być odtwarzane obiekty typu system-state i inherit-state, obiekty adoptujące uprawnienia, obiekty mające włączony atrybut S_ISUID(ustaw_ID_użytkownika) oraz atrybut S_ISGID (ustaw_ID_grupy).
***ALWSETUID**	Umożliwia odtwarzanie zbiorów z włączonym atrybutem S_ISUID (ustaw_ID_użytkownika).
***ALWSETGID**	Umożliwia odtwarzanie zbiorów z włączonym atrybutem S_ISGID (ustaw_ID_grupy).
***ALWVLDERR**	Umożliwia odtwarzanie obiektów, które nie przeszły testów sprawdzania obiektu. Jeśli ustawienie wartości systemowej QFRCCVNRST powoduje konwertowanie obiektu, jego błędy sprawdzania zostaną poprawione.

Zalecana wartość: Wartość systemowa QALWOBJRST zapewnia metodę zabezpieczania systemu przed programami, które mogą powodować poważne problemy. Dla normalnych operacji należy rozważyć ustawienie *NONE. Zawsze należy pamiętać o zmianie na *ALL przed wykonywaniem czynności wymienionych powyżej. Jeśli w systemie programy i aplikacje odtwarzane są regularnie, wartość systemową QALWOBJRST należy ustawić na *ALWPGMADP.

Wartości systemowe dotyczące haseł

Przegląd:

Przeznaczenie:
Wartości systemowe służące do ustawienia wymagań dotyczących haseł użytkowników.

Sposób używania:
WRKSYSVAL *SEC (Komenda Praca z wartościami systemowymi (Work with System Values))

Uprawnienia:
*ALLOBJ i *SECADM

Pozycja kroniki:
SV

Uwaga:
Zmiany mają natychmiastowy efekt. Przeprowadzenie IPL nie jest wymagane.

Poniżej zaprezentowano wartości systemowe, które sterują hasłami. Za pomocą tych wartości można wymuszać regularne zmienianie haseł użytkowników i uniemożliwić wybieranie haseł trywialnych, łatwych do odgadnięcia. Zapewniają także, że hasła będą spełniać wymagania sieci komunikacyjnej:

QPWDEXPITV [1]
Okres ważności

QPWDLVL
Poziom hasła

QPWDMINLEN [1]
Długość minimalna

QPWDMAXLEN [1]
Długość maksymalna

QPWDRQDDIF [1]
Wymagana różnica

QPWDLMTCHR
Znaki zastrzeżone

QPWDLMTAJC
Ograniczenie znaków przylegających

QPWDLMTREP
Ograniczenie powtarzania znaków

QPWDPOSDIF
Różnica w położeniu znaku

QPWDRQDDGT
Wymaganie znaków numerycznych

QPWDVLDPGM
Program sprawdzający poprawność hasła

Wartości systemowe budowy hasła narzucane są jedynie wtedy, gdy hasło zmieniane jest za pomocą komendy CHGPWD, opcji menu ASSIST do zmiany hasła lub za pomocą funkcji API QSYCHGPW. Nie są narzucane, gdy hasło ustawiane jest za pomocą komendy CRTUSRPRF lub CHGUSRPRF.

Jeśli wartość systemowa minimalnej długości hasła (QPWDMINLEN) ma wartość inną niż 1 lub wartość systemowa maksymalnej długości hasła (QPWDMAXLEN) ma wartość inną niż 10 lub użytkownik zmienił inne wartości systemowe sterowania hasłem, system zapobiega ustawieniu przez użytkownika - za pomocą komendy CHGPWD, menu ASSIST lub funkcji API QSYCHGPW - hasła równego nazwie profilu użytkownika.

---

1. Te wartości systemowe zostały omówione także w Centrum informacyjnym (patrz sekcja “Informacje wstępne i pokrewne” na stronie xvi).

Jeśli hasło zostało zapomniane, szef ochrony może użyć komendy Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF), aby ustawić hasło równe nazwie profilu lub innej wartości. Pole *Ustawienie hasła jako wygasłe* w profilu użytkownika może być użyte do żądania zmiany hasła podczas następnego wpisywania się.

Okres ważności hasła (QPWDEXPITV)

Wartość systemowa QPWDEXPITV kontroluje liczbę dni, po ilu hasło powinno być zmienione. Jeśli użytkownik próbuje wpisać się po wygaśnięciu hasła, system wyświetli ekran żądający zmiany hasła przed wpisaniem się.

```
                    Informacje wpisania się
                     (Sign-on Information)
                                                          System:
Hasło wygasło. Aby wpisać się do systemu musisz zmienić
hasło.

Poprzednie wpisanie się  . . . . . :   10/30/91  14:15:00

Niepoprawne próby wpisania się . . . . . :   3
```

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 29. Możliwe wartości dla wartości systemowej QPWDEXPITV

***NOMAX**	Użytkownicy nie muszą zmieniać swoich haseł.
limit_w_dniach	Należy podać wartość 1 do 366.

Zalecana wartość: od 30 do 90.

Uwaga: Okres ważności hasła może być określony także dla pojedynczych profili użytkowników.

Poziom hasła (QPWDLVL)

Poziom hasła w systemie może być ustawiony tak, aby dozwolone były hasła profilu użytkownika od 1 do 10 znaków lub aby dozwolone były hasła profilu użytkownika od 1 do 128 znaków.

Można ustawić poziom hasła, aby zezwolić na używanie długich haseł. Terminu ″długie hasło″ (ang. passphrase) używa się w opisach systemów komputerowych na określenie hasła, które może składać się z bardzo wielu znaków i dla którego nie są ograniczone rodzaje znaków, jakie mogą występować w haśle (lub ograniczenia takie są minimalne). Dozwolone jest używanie spacji między znakami hasła, co pozwala na tworzenie haseł będących zdaniami lub fragmentami zdań. Jedynym ograniczeniem długiego hasła jest to, że hasło nie może rozpoczynać się od znaku gwiazdki (’*’), a występujące na końcu hasła znaki spacji są usuwane. Przed zmianą poziomu hasła systemu należy zapoznać się z informacjami w sekcji “Planowanie zmian poziomu haseł” na stronie 200.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 30. Możliwe wartości dla wartości systemowej QPWDLVL.

0	System obsługuje profile użytkowników z hasłami o długości od 1 do 10 znaków. Dozwolonymi znakami są znaki A-Z, 0-9 oraz $, @, # i podkreślenie. Wartość 0 dla QPWDLVL powinna być używana, jeśli system komunikuje się z innymi systemami iSeries połączonymi w sieć, a w tych systemach wartość systemowa QPWDLVL też jest ustawiona na 0 lub systemy operacyjne są w wersji niższej niż V5R1M0. Wartości tej należy użyć, jeśli system komunikuje się z jakimkolwiek innym systemem, w którym długość hasła jest ograniczona do zakresu od 1 do 10 znaków. Wartość QPWDLVL 0 musi być stosowana, jeśli system komunikuje się z produktemWindows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer), a z innymi systemami przy użyciu haseł składających się z od 1 do 10 znaków. Jeśli wartość QPWDLVL jest ustawiona na 0, system operacyjny utworzy szyfrowane hasło do użycia dla wartości QPWDLVL 2 i 3. Hasło, które może być użyte dla wartości QPWDLVL 2 i 3, będzie takim samym hasłem, jakie było używane dla wartości QPWDLVL 0 lub 1.
1	Wartość QPWDLVL 1 jest odpowiednikiem wartości QPWDLVL 0 z następującym wyjątkiem: hasła produktu iSeries NetServer dla klientów systemu Windows 95/98/ME zostaną usunięte z systemu. Wybierając obsługę klienta dla produktu iSeries NetServer, nie można używać wartości QPWDLVL 1. Wartość QPWDLVL 1 zwiększa ochronę systemu iSeries, usuwając z systemu wszystkie hasła produktu iSeries NetServer.
2	System obsługuje hasła profili użytkowników o długości od 1 do 128 znaków. Dozwolone jest użycie wielkich i małych liter. Hasło może zawierać dowolne znaki, a wielkie i małe litery są rozróżniane. Poziom ten jest udostępniony dla zapewnienia zgodności. Ten poziom umożliwia przywrócenie wartości QPWDLVL 0 lub 1 pod warunkiem, że hasło utworzone dla wartości QPWDLVL 2 lub 3 spełnia wymagania długości i składni hasła poprawnego dla wartości QPWDLVL 0 lub 1. Wartość QPWDLVL 2 może być używana, jeśli system komunikuje się z produktem Windows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer) pod warunkiem, że hasło składa się z od 1 do 14 znaków. Wartość 2 dla QPWDLVL nie może być używana, jeśli system komunikuje się z innymi systemami iSeries połączonymi w sieć, a w tych systemach wartość systemowa QPWDLVL ustawiona jest na 0 lub 1 lub systemy operacyjne są w wersji niższej niż V5R1M0. Wartości tej nie można używać, jeśli system komunikuje się z jakimkolwiek innym systemem, w którym długość hasła jest ograniczona do zakresu od 1 do 10 znaków. Gdy wartość systemowa QPWDLVL jest zmieniana na wartość 2, nie są usuwane żadne zaszyfrowane hasła.
3	System obsługuje hasła profili użytkowników o długości od 1 do 128 znaków. Dozwolone jest użycie wielkich i małych liter. Hasło może zawierać dowolne znaki, a wielkie i małe litery są rozróżniane. Wartość 3 dla QPWDLVL nie może być używana, jeśli system komunikuje się z innymi systemami iSeries połączonymi w sieć, a w tych systemach wartość systemowa QPWDLVL ustawiona jest na 0 lub 1 lub systemy operacyjne są w wersji niższej niż V5R1M0. Wartości tej nie można używać, jeśli system komunikuje się z jakimkolwiek innym systemem, w którym długość hasła jest ograniczona do zakresu od 1 do 10 znaków. Wartość QPWDLVL 3 nie może być używana, jeśli system komunikuje się z produktem Windows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer). Wszystkie hasła profili użytkowników używane na poziomie 0 i 1 są usuwane. Zmiana z poziomu QPWDLVL 3 do poziomu 0 lub 1 najpierw wymaga zmiany na poziom 2. Poziom QPWDLVL 2 umożliwia tworzenie haseł profili użytkowników, które mogą być używane na poziomie QPWDLVL 0 lub 1, jeśli spełniają wymagania składni dla haseł poziomu QPWDLVL 0 lub 1.

Zmiana poziomu hasła w systemie z hasła zawierającego od 1 do 10 znaków na hasła zawierające od 1 do 128 znaków powinna być przeprowadzona ze szczególną uwagą. Jeśli system komunikuje się z innymi systemami w sieci, wszystkie systemy muszą obsługiwać dłuższe hasła.

Zmiana tej wartości systemowej będzie miała miejsce podczas następnego IPL. Aby zobaczyć bieżące i oczekujące wartości poziomu hasła, należy użyć komendy CL DSPSECA (Wyświetlenie atrybutów ochrony - Display Security Attributes).

Minimalna długość hasła (QPWDMINLEN)

Wartość systemowa QPWDMINLEN okresla minimalną liczbę znaków hasła.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 31. Możliwe wartości dla wartości systemowej QPWDMINLEN

6	Wymaganych jest minimum sześć znaków.
minimalna_liczba_znaków	Gdy wartość systemowa poziomu hasła (QPWDLVL) ustawiona jest na 0 lub 1, należy podać wartość z zakresu od 1 do 10. Gdy wartość systemowa QPWDLVL ma wartość 2 lub 3, należy podać liczbę z zakresu od 1 do 128.

Zalecana wartość: 6, aby zapobiec podawaniu hasła, które łatwo odgadnąć, takich jak inicjały lub pojedyncze znaki.

Maksymalna długość hasła (QPWDMAXLEN)

Wartość systemowa QPWDMAXLEN określa maksymalną liczbę znaków hasła. Ta wartość zapewnia dodatkową ochronę, uniemożliwiając podawanie zbyt długich haseł, które użytkownicy muszą gdzieś zapisywać, ponieważ z powodu dużej długości nie mogą ich zapamiętać.

Niektóre sieci komunikacyjne wymagają haseł o długości do 8 znaków lub mniej. Ta wartość systemowa zapewni zgodność z wymaganiami danej sieci.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 32. Możliwe wartości dla wartości systemowej QPWDMAXLEN

8	Dozwolonych jest maksymalnie osiem znaków.
maksymalna_liczba_znaków	Gdy wartość systemowa poziomu hasła (QPWDLVL) ustawiona jest na 0 lub 1, należy podać wartość z zakresu od 1 do 10. Gdy wartość systemowa QPWDLVL ma wartość 2 lub 3, należy podać liczbę z zakresu od 1 do 128.

Zalecana wartość: 8.

Wymagana różnica haseł (QPWDRQDDIF)

Wartość systemowa QPWDRQDDIF określa, czy nowe hasło musi różnić się od poprzedniego. Zapobiega to podawaniu przez użytkowników poprzednio używanych haseł. Uniemożliwia także użytkownikowi, którego hasło wygasło, zmianę hasła na nowe, a następnie ponownego przywrócenia starego hasła.

Uwaga: Wartość QPWDRQDDIF określa, ile poprzednich haseł jest sprawdzanych w poszukiwaniu zduplikowanego hasła.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 33. Możliwe wartości dla wartości systemowej QPWDRQDDIF

wartość	*Liczba poprzednich haseł sprawdzanych pod kątem powtórzeń*
0	Dozwolonych jest 0 powtarzających się haseł.
1	32
2	24
3	18
4	12
5	10
6	8
7	6
8	4

Zalecana wartość: Aby uniemożliwić ponowne użycie hasła, należy wybrać wartość 5 lub więcej. Aby zapobiec ponownemu użyciu hasła przez 6 miesięcy, należy użyć kombinacji wartości systemowej QPWDRQDDIF i QPWDEXPITV (okres ważności hasła). Na przykład wartość systemową QPWDEXPITV można ustawić na 30 (dni), a wartość QPWDRQDDIF na 5 (10 unikalnych haseł). Przy takich ustawieniach przeciętny użytkownik, zmieniający hasło po ostrzeżeniu systemowym, nie będzie mógł powtórzyć hasła przez około 9 miesięcy.

Znaki zastrzeżone w hasłach (QPWDLMTCHR)

Wartość systemowa QPWDLMTCHR ogranicza użycie niektórych znaków w haśle. Zapewnia ona dodatkową ochronę, zapobiegając użyciu przez użytkowników pewnych znaków, takich jak samogłoski. Wykluczenie samogłosek uniemożliwia podanie w haśle rzeczywistych słów.

Wartość systemowa QPWDLMTCHR nie jest narzucana, gdy wartość systemowa poziomu hasła (QPWDLVL) ustawiona jest na 2 lub 3. Wartość systemowa QPWDLMTCHR może być zmieniona, jeśli poziomem hasła jest 2 lub 3, ale jej ustawienie będzie wykorzystane dopiero po zmianie poziomu hasła na 0 lub 1.

| **Uwaga:** Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać
| zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych,
| należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 34. Możliwe wartości dla wartości systemowej QPWDLMTCHR

***NONE**	Brak znaków zastrzeżonych dla haseł.
znaki_zastrzeżone	Należy podać do 10 znaków zastrzeżonych. Dozwolonymi znakami są litery od A do Z, cyfry od 0 do 9 oraz znaki specjalne: funt (#), dolar ($), znak at (@) i podkreślenie (_).

Zalecana wartość: A, E, I, O i U. W celu zapewnienia kompatybilności z innymi systemami, można także zastrzec znaki specjalne (#, $ i @).

Ograniczenie kolejnych cyfr w hasłach (QPWDLMTAJC)

Wartość systemowa QPWDLMTAJC ogranicza użycie w hasłach następujących po sobie znaków numerycznych (przylegających). Ta wartość zwiększa bezpieczeństwo systemu poprzez uniemożliwienie użytkownikom tworzenia haseł będących datami urodzin, numerami telefonu lub innymi sekwencjami cyfr.

| **Uwaga:** Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać
| zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych,
| należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 35. Możliwe wartości dla wartości systemowej QPWDLMTAJC

0	Podawanie w hasłach następujących po sobie znaków numerycznych jest dozwolone.
1	Podawanie w hasłach następujących po sobie znaków numerycznych jest niedozwolone.

Ograniczenie powtarzania znaków w hasłach (QPWDLMTREP)

Wartość systemowa QPWDLMTREP ogranicza użycie w hasłach powtórzonych znaków. Ta wartość zapewnia dodatkową ochronę, ponieważ uniemożliwia podanie hasła łatwego do odgadnięcia, na przykład składającego się z kilku takich samych znaków.

Kiedy poziomem hasła jest 2 lub 3, test powtarzających się znaków jest przeprowadzany z rozróżnianiem wielkości liter. Oznacza to, że mała litera ″a″ jest traktowana jako znak inny niż wielka litera ″A″.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 36. Możliwe wartości dla wartości systemowej QPWDLMTREP

0	Opcja ta umożliwia wielokrotne użycie jednego znaku w haśle.
1	Opcja ta zabrania wielokrotnego użycia jednego znaku w haśle.
2	Opcja ta zabrania wielokrotnego użycia jednego znaku w haśle.

Tabela 37 opisuje przykłady, jakie hasła są dozwolone w zależności od wartości systemowej QPWDLMTREP.

Tabela 37. Hasła z powtórzonymi znakami dla wartości QPWDLVL 0 lub 1

Przykład hasła	QPWDLMTREP wartość 0	QPWDLMTREP wartość 1	QPWDLMTREP wartość 2
A11111	Dozwolone	Niedozwolone	Niedozwolone
BOBBY	Dozwolone	Niedozwolone	Niedozwolone
SAMOLOT	Dozwolone	Niedozwolone	Dozwolone
N707PL	Dozwolone	Niedozwolone	Dozwolone

Tabela 38. Hasła z powtórzonymi znakami dla wartości QPWDLVL 2 lub 3

Przykład hasła	QPWDLMTREP wartość 0	QPWDLMTREP wartość 1	QPWDLMTREP wartość 2
j222222	Dozwolone	Niedozwolone	Niedozwolone
BardzoSzybko	Dozwolone	Niedozwolone	Niedozwolone
CiastoA'laDomowe	Dozwolone	Niedozwolone	Dozwolone
AaBbCcDdEe	Dozwolone	Dozwolone	Dozwolone

Różnica pozycji znaków w hasłach (QPWDPOSDIF)

Wartość systemowa QPWDPOSDIF kontroluje każdą pozycję nowego hasła. Zapewnia to dodatkową ochronę zapobiegając używaniu przez użytkowników takich samych znaków (alfabetycznych lub numerycznych) na pozycji odpowiadającej tej samej pozycji w poprzednim haśle.

Kiedy wartość systemowa poziomu hasła (QPWDLVL) ma wartość 2 lub 3, test takich samych znaków przeprowadzany jest z rozróżnianiem wielkości liter. Oznacza to, że mała litera ″a″ jest traktowana jako znak inny niż wielka litera ″A″.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 39. Możliwe wartości dla wartości systemowej QPWDPOSDIF

0	Na pozycji odpowiadającej pozycji w poprzednim haśle mogą być takie same znaki.
1	Na pozycji odpowiadającej pozycji w poprzednim haśle nie mogą być takie same znaki.

Wymaganie znaków numerycznych w haśle (QPWDRQDDGT)

Wartość systemowa QPWDRQDDGT określa, czy w nowym haśle wymagany jest znak numeryczny. Ta wartość udostępnia dodatkową ochronę zapobiegając używaniu przez użytkowników tylko znaków alfabetu.

| **Uwaga:** Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 40. Możliwe wartości dla wartości systemowej QPWDRQDDGT

0	W nowych hasłach nie są wymagane znaki numeryczne.
1	W nowych hasłach wymagany jest jeden lub więcej znaków numerycznych.

Zalecana wartość: 1.

Program zatwierdzający hasło (QPWDVLDPGM)

Jeśli dla wartości systemowej QPWDVLDPGM podano parametr *REGFAC lub nazwę programu, po zatwierdzeniu hasła przez testy sprawdzania określone w wartościach systemowych sterowania hasłem, system uruchamia jeden lub więcej programów. Programy te można wykorzystać do dodatkowego sprawdzenia haseł użytkowników, zanim zostaną zaakceptowane przez system.

W temacie “Używanie programu zatwierdzającego hasło” omówione zostały wymagania dotyczące programu zatwierdzania haseł oraz przedstawione przykłady.

Program zatwierdzania hasła musi znajdować się w puli pamięci dyskowej (ASP) lub podstawowej puli ASP użytkownika.

| **Uwaga:** Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 41. Możliwe wartości dla wartości systemowej QPWDVLDPGM

***NONE**	Nie jest używany żaden program napisany przez użytkownika. Obejmuje to programy zatwierdzania hasła zarejestrowane w narzędziu do rejestracji wyjścia.
**REGFAC*	Program sprawdzający wczytywany jest z narzędzia do rejestracji, punktu wyjścia QIBM_QSY_VLD_PASSWRD. W narzędziu do rejestracji można podać więcej niż jeden program sprawdzający. Wywołany zostanie każdy program, do czasu aż jeden nie wskaże, że hasło powinno zostać odrzucone lub wszystkie wskażą, że hasło jest poprawne.
nazwa_programu	Należy podać nazwę programu sprawdzania napisanego przez użytkownika, którego nazwa ma od 1 do 10 znaków. Nazwy nie można podawać, gdy bieżąca lub oczekująca wartość dla wartości systemowej poziomu hasła (QPWDLVL) jest równa 2 lub 3.
nazwa_biblioteki	Należy podać nazwę biblioteki, w której znajduje się program napisany przez użytkownika. Jeśli nie podano nazwy biblioteki, w poszukiwaniu programu używana jest lista bibliotek (*LIBL) użytkownika zmieniającego wartość systemową. Zalecaną biblioteką jest biblioteka QSYS.

Używanie programu zatwierdzającego hasło

Jeśli dla wartości systemowej QPWDVLDPGM podano wartość *REGFAC lub nazwę programu, komenda Zmiana hasła (Change Password - CHGPWD) lub funkcja API Change Password (QSYCHGPW) wywołuje jeden lub więcej programów. Programy wywoływane są tylko wtedy, gdy wprowadzane przez użytkownika nowe hasło przeszło wszystkie testy podane w wartościach systemowych sterowania hasłem.

W przypadku, gdy konieczne jest odtwarzanie systemu po awarii dysku, program zatwierdzania hasła należy umieścić w bibliotece QSYS. W ten sposób program ten zostanie załadowany podczas odtwarzania biblioteki QSYS.

Jeśli dla wartości systemowej QPWDVLDPGM podano nazwę programu, system przekazuje do niego następujące parametry:

Tabela 42. Parametry dla programu zatwierdzania hasła

Pozycja	Typ	Długość	Opis
1	*CHAR	10	Podane przez użytkownika nowe hasło.
2	*CHAR	10	Poprzednie hasło użytkownika.
3	*CHAR	1	Kod powrotu: 0 dla poprawnego hasła; inny niż 0 dla niepoprawnego hasła.
4 [1]	*CHAR	10	Nazwa użytkownika.

1 Pozycja 4 jest opcjonalna.

Jeśli dla wartości systemowej QPWDVLDPGM określono parametr *REGFAC, należy zapoznać się sekcją dotyczącą programu obsługi wyjścia ochrony w podręczniku opisującym API systemu, aby poznać informacje na temat parametrów przekazywanych do programu sprawdzającego.

Jeśli program użytkownika określa, że nowe hasło nie jest poprawne, można wysłać albo komunikat wyjątku (za pomocą komendy SNDPGMMSG) lub ustawić kod powrotu na wartość inną niż 0 i umożliwić systemowi wyświetlenie komunikatu o błędzie. Komunikaty wyjątku sygnalizowane przez program muszą być tworzone z użyciem opcji DMPLST(*NONE) komendy Dodanie opisu komunikatu (Add Message Description - ADDMSGD).

Nowe hasło akceptowane jest tylko wtedy, gdy program napisany przez użytkownika zakończy działanie bez komunikatu o przedwczesnym zakończeniu i z kodem powrotu 0. Ponieważ kod powrotu początkowo ustawiany jest dla haseł, które nie są poprawne (jest inny niż zero), program zatwierdzający musi ustawić kod powrotu na 0.

Uwaga: Bieżące i nowe hasła przekazywane są do programu sprawdzającego bez szyfrowania. Program sprawdzający może przechowywać hasła w zbiorze bazy danych i wpływać na poziom ochrony systemu. Należy upewnić się, że funkcje programu sprawdzającego zostały zatwierdzone przez szefa ochrony, a zmiany w programie są ściśle kontrolowane.

Zaprezentowany poniżej program CL jest przykładem programu zatwierdzania hasła, którego nazwa została podana w wartości systemowej QPWDVLDLVL. Ten przykład sprawdza, czy hasło nie jest zmieniane więcej niż raz na dzień. Do programu można dodać dodatkowe kalkulacje, aby sprawdzał inne kryteria dla haseł:

```
/************************************************/
/* NAZWA:    PWDVALID - Sprawdzanie hasła       */
/*                                              */
/* FUNKCJA: Ograniczenie zmiany hasła do jednej   */
/*          na dzień, chyba że hasło wygasło.   */
/************************************************/
   PGM (&NEW &OLD &RTNCD &USER)
   DCL VAR(&NEW)       TYPE(*CHAR) LEN(10)
   DCL VAR(&OLD)       TYPE(*CHAR) LEN(10)
   DCL VAR(&RTNCD)     TYPE(*CHAR) LEN(1)
   DCL VAR(&USER)      TYPE(*CHAR) LEN(10)
   DCL VAR(&JOBDATE)   TYPE(*CHAR) LEN(6)
   DCL VAR(&PWDCHGDAT) TYPE(*CHAR) LEN(6)
   DCL VAR(&PWDEXP)    TYPE(*CHAR) LEN(4)
/* Pobranie bieżącej daty w celu przekonwertowania*/
/* do formatu RMD                               */
   RTVJOBA    DATE(&JOBDATE)
   CVTDAT     DATE(&JOBDATE) TOVAR(&JOBDATE) +
              TOFMT(*YMD)    TOSEP(*NONE)
/* Pobranie daty ostatniej zmiany hasła i czy     */
/* dla tego profilu użytkownika hasło wygasło     */
   RTVUSRPRF  USRPRF(&USER)  PWDCHGDAT(&PWDCHGDAT)+
     PWDEXP(&PWDEXP)
/* Porównanie dwóch dat                         */
/*   jeśli są równe i hasło nie wygasło         */
```

```
/*   wysyłany jest komunikat *ESCAPE, aby zapobiec*/
/*   zmianie, lub ustawiany jest kod powrotu,     */
/*   aby umożliwić zmianę                         */
   IF (&JOBDATE=&PWDCHGDAT *AND &PWDEXP='*NO ') +
       SNDPGMMSG  MSGID(CPF9898) MSGF(QCPFMSG) +
       MSGDTA('Hasło można zmieniać tylko +
               raz dziennie') +
             MSGTYPE(*ESCAPE)
   ELSE  CHGVAR &RTNCD '0'
   ENDPGM
```

Zaprezentowany poniżej program CL jest przykładem programu zatwierdzania hasła, gdy dla wartości systemowej QPWDVLDLVL podano wartość *REGFAC.

Ten przykład sprawdza, czy nowe hasło używa zestawu znaków CCSID 37 (lub jeśli używa CCSID 13488, konwertuje je do CCSID 37), czy nie kończy się znakiem numerycznym i czy nie zawiera nazwy profilu użytkownika. W przykładzie przyjęto, że zbiór komunikatów (PWDERRORS) został utworzony, a opisy komunikatów (PWD0001 i PWD0002) zostały dodane do zbioru komunikatów. Do programu można dodać dodatkowe kalkulacje, aby sprawdzał inne kryteria dla haseł:

```
| /*********************************************************/
| /*                                                       */
| /*  NAZWA:   PWDEXITPGM1 - Program sprawdzania hasła 1    */
| /*                                                       */
| /*  Sprawdza hasła, gdy dla QPWDVLDPGM podano parametr    */
| /*  *REGFAC. Program rejestrowany jest za pomocą komendy  */
| /*  ADDEXITPGM dla punktu wyjścia QIBM_QSY_VLD_PASSWRD. */
| /*                                                       */
| /*                                                       */
| /*  ZAŁOŻENIA: Jeśli używana jest komenda CHGPWD, użyty   */
| /*  będzie domyślny dla zadania CCSID (CCSID 37).       */
| /*  Jeśli użyto funkcji API QSYCHGPW, CCSID hasła będzie  */
| /*  UNICODE CCSID 13488.                                */
| /*********************************************************/
|
| DCL &EXINPUT    *CHAR 1000
| DCL &RTN        *CHAR 1
|
| DCL   &UNAME    *CHAR  10DCL &NEWPW      *CHAR 256
| DCL &NPOFF      *DEC 5 0
| DCL &NPLEN      *DEC 5 0
| DCL &INDX       *DEC 5 0
| DCL &INDX2      *DEC 5 0
| DCL &INDX3      *DEC 5 0
| DCL &UNLEN      *DEC 5 0
|
| DCL &XLTCHR2    *CHAR 2 VALUE(X'0000')
| DCL &XLTCHR     *DEC 5 0
| DCL &XLATEU     *CHAR 255 VALUE('............................. +
|                                !"#$%&''()*+,-./0123456789:;<=>?+
|                                @ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_+
|                                `ABCDEFGHIJKLMNOPQRSTUVWXYZ{|}~.+
|                                ................................+
|                                ................................+
|                                ................................+
|                                .............................')
|
| DCL &XLATEC     *CHAR 255 VALUE('................................+
|                                ................................+
|                                ................................+
|                                ................................+
|                                .ABCDEFGHI.......JKLMNOPQR......+
|                                ..STUVWXYZ......................+
|                                ................................+
|                                .................................')
|
```

```
|  /*****************************************************************/
|  /* FORMAT DANYCH WEJŚCIOWYCH:                                    */
|
|  /* POZYCJA    OPIS                                               */
|  /* 001 - 020  NAZWA PUNKTU WYJŚCIA                               */
|  /* 021 - 028  NAZWA FORMATU PUNKTU WYJŚCIA                       */
|  /* 029 - 032  POZIOM HASŁA (binarnie)                            */
|  /* 033 - 042  NAZWA PROFILU UŻYTKOWNIKA                          */
|  /* 043 - 044  ZAREZERWOWANE                                      */
|  /* 045 - 048  POZYCJA DLA POPRZEDNIEGO HASŁA (binarnie)          */
|  /* 049 - 052  DŁUGOŚĆ POPRZEDNIEGO HASŁA (binarnie)              */
|  /* 053 - 056  CCSID POPRZEDNIEGO HASŁA (binarnie)                */
|  /* 057 - 060  POZYCJA NOWEGO HASŁA (binarnie)                    */
|  /* 061 - 064  DŁUGOŚĆ NOWEGO HASŁA (binarnie)                    */
|  /* 065 - 068  CCSID NOWEGO HASŁA  (binarnie)                     */
|  /* ??? - ???  POPRZEDNIE HASŁO                                   */
|  /* ??? - ???  NOWE HASŁO                                         */
|  /*                                                               */
|  /*****************************************************************/
|
|
|  /*****************************************************************/
|  /*  Uruchomienie ogólnego monitora dla programu.                 */
|  /*****************************************************************/
|
|               MONMSG     CPF0000
|  /* Przyjęcie, że nowe hasło jest poprawne */
|  CHGVAR &RTN  VALUE('0') /* zaakceptowanie */
|  /* Pobranie długości nowego hasła, pozycji i wartości. Także pobranie nazwy użytkownika */
|  CHGVAR &NPLEN VALUE(%BIN(&EXINPUT 61 4))
|  CHGVAR &NPOFF VALUE(%BIN(&EXINPUT 57 4) + 1)
|  CHGVAR &UNAME VALUE(%SST(&EXINPUT 33 10))
|  CHGVAR &NEWPW VALUE(%SST(&EXINPUT &NPOFF &NPLEN))
|  /* Jeśli CCSID to 13488, prawdopodobnie użyto funkcji API QSYCHGPW, która konwertuje */
|  /* hasła do formatu UNICODE CCSID 13488. Przekonwertuj do formatu CCSID 37, jeśli to */
|  /* możliwe, w przeciwnym przypadku zwróć błąd */
|  IF COND(%BIN(&EXINPUT 65 4) = 13488) THEN(DO)
|      CHGVAR &INDX2 VALUE(1)
|      CHGVAR &INDX3 VALUE(1)
|     CVT1:
|      CHGVAR &XLTCHR VALUE(%BIN(&NEWPW &INDX2 2))
|      IF COND( (&XLTCHR *LT 1) *OR (&XLTCHR *GT 255) ) THEN(DO)
|    CHGVAR &RTN  VALUE('3') /* odrzucenie */
|         SNDPGMMSG MSG('HASŁO ZAWIERA NIEPOPRAWNY ZNAK')
|         GOTO DONE
|  ENDDO    CHGVAR %SST(&NEWPW &INDX3 1) VALUE(%SST(&XLATEU &XLTCHR 1))
|      CHGVAR &INDX2  VALUE(&INDX2 + 2)
|      CHGVAR &INDX3  VALUE(&INDX3 + 1)
|      IF COND(&INDX2 > &NPLEN) THEN(GOTO ECVT1)
|      GOTO CVT1
|     ECVT1:
|      CHGVAR &NPLEN VALUE(&INDX3 - 1)
|      CHGVAR %SST(&EXINPUT 65 4) VALUE(X'00000025')
|  ENDDO
|   /* Sprawdzenie CCSID wartości nowego hasła - musi mieć format 37     */
|   IF COND(%BIN(&EXINPUT 65 4) *NE 37) THEN(DO)
|    CHGVAR &RTN  VALUE('3') /* odrzucenie */
|     SNDPGMMSG MSG('IDENTYFIKATOR CCSID NOWEGO HASŁA MUSI MIEĆ WARTOŚĆ 37')
|     GOTO DONE
|  ENDDO
|   /* ZMIANA WARTOŚCI HASŁA NA WIELKIE LITERY                       */
|   CHGVAR &INDX2 VALUE(1)
|   CHGVAR &INDX3 VALUE(1)
|   CVT4:
|     CHGVAR %SST(&XLTCHR2 2 1) VALUE(%SST(&NEWPW &INDX2 1))
|     CHGVAR &XLTCHR VALUE(%BIN(&XLTCHR2 1 2))
|     IF COND( (&XLTCHR *LT 1) *OR (&XLTCHR *GT 255) ) THEN(DO)
```

```
|    CHGVAR &RTN  VALUE('3') /* odrzucenie */
|         SNDPGMMSG MSG('HASŁO ZAWIERA NIEPOPRAWNY ZNAK')
|       GOTO DONE
|  ENDDO   IF COND(%SST(&XLATEC &XLTCHR 1) *NE '.') +
|     THEN(CHGVAR %SST(&NEWPW &INDX3 1) VALUE(%SST(&XLATEC &XLTCHR 1)))
|     CHGVAR &INDX2  VALUE(&INDX2 + 1)
|     CHGVAR &INDX3  VALUE(&INDX3 + 1)
|     IF COND(&INDX2 > &NPLEN) THEN(GOTO ECVT4)
|     GOTO CVT4
|    ECVT4:
|
|    /* SPRAWDZENIE, CZY OSTATNIA POZYCJA W NOWYM HAŚLE JEST NUMERYCZNA */
|    IF COND(%SST(&NEWPW &NPLEN 1) = '0') THEN(GOTO ERROR1)
|    IF COND(%SST(&NEWPW &NPLEN 1) = '1') THEN(GOTO ERROR1)
|    IF COND(%SST(&NEWPW &NPLEN 1) = '2') THEN(GOTO ERROR1)
|    IF COND(%SST(&NEWPW &NPLEN 1) = '3') THEN(GOTO ERROR1)
|    IF COND(%SST(&NEWPW &NPLEN 1) = '4') THEN(GOTO ERROR1)
|    IF COND(%SST(&NEWPW &NPLEN 1) = '5') THEN(GOTO ERROR1)
|    IF COND(%SST(&NEWPW &NPLEN 1) = '6') THEN(GOTO ERROR1)
|    IF COND(%SST(&NEWPW &NPLEN 1) = '7') THEN(GOTO ERROR1)
|    IF COND(%SST(&NEWPW &NPLEN 1) = '8') THEN(GOTO ERROR1)
|    IF COND(%SST(&NEWPW &NPLEN 1) = '9') THEN(GOTO ERROR1)
|
|    /* SPRAWDZENIE, CZY HASŁO ZAWIERA NAZWĘ PROFILU UŻYTKOWNIKA        */
|    CHGVAR &UNLEN VALUE(1)
|    LOOP2:      /* ODSZUKAJ DŁUGOŚĆ NAZWY UŻYTKOWNIKA */
|     IF COND(%SST(&UNAME &UNLEN 1) *NE ' ') THEN(DO)
|       CHGVAR &UNLEN VALUE(&UNLEN + 1)
|       IF COND(&UNLEN = 11) THEN(GOTO ELOOP2)
|       GOTO LOOP2
|  ENDDO ELOOP2:
|    CHGVAR &UNLEN VALUE(&UNLEN - 1)
|
|
|    /* SPRAWDZENIE NOWEGO HASŁA POD KĄTEM NAZWY UŻYTKOWNIKA      */
|    IF COND(&UNLEN *GT &NPLEN) THEN(GOTO ELOOP3)
|    CHGVAR &INDX VALUE(1)
|    LOOP3:
|      IF COND(%SST(&NEWPW &INDX &UNLEN) = %SST(&UNAME 1 &UNLEN))+
|         THEN(GOTO ERROR2)
|      IF COND((&INDX + &UNLEN + 1) *LT 128) THEN(DO)
|         CHGVAR &INDX VALUE(&INDX + 1)
|         GOTO LOOP3
|  ENDDO ELOOP3:
|
|    /* Nowe hasło jest poprawne                        */
|    GOTO DONE
|
|    ERROR1:  /* NOWE HASŁO KOŃCZY SIĘ ZNAKIEM NUMERYCZNYM */
|     CHGVAR &RTN  VALUE('3') /* odrzucenie */
|     SNDPGMMSG TOPGMQ(*PRV) MSGTYPE(*ESCAPE) MSGID(PWD0001) MSGF(QSYS/PWDERRORS)
|     GOTO DONE
|
|    ERROR2:  /* NOWE HASŁO ZAWIERA NAZWĘ UŻYTKOWNIKA */
|     CHGVAR &RTN  VALUE('3') /* odrzucenie */
|     SNDPGMMSG TOPGMQ(*PRV) MSGTYPE(*ESCAPE) MSGID(PWD0002) MSGF(QSYS/PWDERRORS)
|     GOTO DONE
|
|    DONE:
|    ENDPGM
|
|
```

Wartości systemowe, które sterują kontrolą

Przegląd:

Przeznaczenie:
Wartości systemowe, które sterują kontrolą ochrony systemu.

Sposób używania:
WRKSYSVAL *SEC (Komenda Praca z wartościami systemowymi (Work with System Values))

Uprawnienia:
*AUDIT

Pozycja kroniki:
SV

Uwaga:
Zmiany mają natychmiastowy efekt. Przeprowadzenie IPL nie jest wymagane.

| Poniższe wartości systemowe sterują kontrolą systemu:

| **QAUDCTL**
| Sterowanie kontrolą

| **QAUDENDACN**
| Działanie zakończenia kontroli

| **QAUDFRCLVL**
| Poziom narzucenia kontroli

| **QAUDLVL**
| Poziom kontroli

| **QAUDLVL2**
| Rozszerzenie poziomu kontroli

| **QCRTOBJAUD**
| Tworzenie domyślnej kontroli

Poniżej znajdują się opisy tych wartości systemowych. Podano wszystkie możliwe opcje. Podkreślone opcje są wartościami domyślnymi. Dla większości wartości systemowych podano wartości zalecane.

Sterowanie kontrolą (QAUDCTL)

Wartość systemowa QAUDCTL określa, czy przeprowadzana jest kontrola. Działa jak przełącznik dla:

| • wartości systemowych QAUDLVL i QAUDLVL2,
• kontroli zdefiniowanej dla obiektów za pomocą komend Zmiana kontroli obiektu (Change Object Auditing - CHGOBJAUD) i Zmiana kontroli DLO (Change DLO Auditing - CHGDLOAUD),
• kontroli zdefiniowanej dla użytkowników za pomocą komendy Zmiana kontroli użytkownika (Change User Audit - CHGUSRAUD).

| **Uwaga:** Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać
| zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych,
| należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Dla wartości systemowej QAUDCTL można podać więcej niż jedną wartość, chyba że jest to wartość *NONE.

Tabela 43. Możliwe wartości dla wartości systemowej QAUDCTL

***NONE**	Nie jest przeprowadzana żadna kontrola działania użytkownika i obiektów.
***OBJAUD**	Kontrola przeprowadzana jest dla obiektów, które zostały wybrane za pomocą komend CHGOBJAUD, CHGDLOAUD lub CHGAUD.
***AUDLVL**	Kontrola przeprowadzana jest dla funkcji wybranych dla wartości systemowych QAUDLVL i QAUDLVL2 oraz parametru AUDLVL pojedynczych profili użytkowników. Poziom kontroli dla użytkownika podany jest za pomocą komendy Zmiana kontroli użytkownika (Change User Audit - CHGUSRAUD).
***NOQTEMP**	Jeśli obiekt znajduje się w bibliotece QTEMP, dla większości działań kontrola nie jest przeprowadzana. Więcej szczegółów zawiera sekcja Rozdział 9, “Kontrolowanie ochrony na systemie iSeries”, na stronie 233. Ta wartość musi być podana razem z wartością *OBJAUD lub *AUDLVL. Pełen opis procesu sterowania kontrolą w systemie zawiera sekcja “Planowanie kontroli ochrony” na stronie 238.

Działanie zakończenia kontroli (QAUDENDACN)

Wartość systemowa QAUDENDACN określa, jakie działanie podejmuje system, jeśli kontrola jest aktywna, a system nie może zapisać pozycji w kronice kontroli.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 44. Możliwe wartości dla wartości systemowej QAUDENDACN

***NOTIFY**	Co godzinę, do czasu pomyślnego zrestartowania kontroli, do kolejki komunikatów QSYSOPR i kolejki QSYSMSG (jeśli istnieje) wysyłany jest komunikat CPI2283. Wartość systemowa QAUDCTL ustawiana jest na *NONE, aby zapobiec próbom zapisania dodatkowych pozycji kroniki kontroli przez system. Przetwarzanie w systemie jest kontynuowane. Jeśli IPL zostanie przeprowadzone przed zrestartowaniem kontroli, podczas IPL do kolejek komunikatów QSYSOPR i QSYSMSG wysyłany jest komunikat CPI2284.
***PWRDWNSYS**	Jeśli system nie może zapisać pozycji kroniki kontroli, natychmiast jest wyłączany. Jednostka systemowa wyświetla kod SRC B900 3D10. Gdy system zostanie włączony ponownie, będzie w stanie zastrzeżonym. Oznacza to, że podsystem sterujący znajduje się w stanie zastrzeżonym, żadne inne podsystemy nie są aktywne, a wpisywanie się dozwolone jest jedynie z poziomu konsoli. Wartość systemowa QAUDCTL ustawiona jest na *NONE. Użytkownik wpisujący się na konsoli w celu dokończenia IPL musi mieć uprawnienia specjalne *ALLOBJ i *AUDIT.

Zalecana wartość: Dla większości instalacji zalecaną wartością jest *NOTIFY. Jeśli strategia ochrony wymaga, aby bez kontroli nie było wykonywane żadne przetwarzanie, wtedy należy wybrać opcję *PWRDWNSYS.

Brak możliwości zapisu pozycji kroniki kontroli powodują jedynie bardzo niezwykłe okoliczności. Jednak jeśli to się zdarzy, a wartość systemowa QAUDENDACN będzie ustawiona na *PWRDWNSYS, system nieprawidłowo zakończy swoje działanie. Może to spowodować przedłużone ładowanie programu początkowego (IPL) przy ponownym włączeniu systemu.

Poziom narzucenia kontroli (QAUDFRCLVL)

Wartość systemowa QAUDFRCLVL określa, jak często narzucane są nowe pozycje kroniki kontroli z pamięci do pamięci dyskowej. Ta wartość systemowa steruje także ilością danych kontroli, które mogą być utracone, jeśli system nieprawidłowo zakończy działanie.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 45. Możliwe wartości dla wartości systemowej QAUDFRCLVL

***SYS**	System określa, w oparciu o wewnętrzną wydajność systemu, kiedy w pamięci dyskowej zapisywane są pozycje kontroli.
liczba_rekordów	Należy podać liczbę z przedziału od 1 do 100, aby określić, ile pozycji kontroli ma być przechowywanych w pamięci przed zapisaniem ich w pamięci dyskowej. Im mniejsza liczba, tym większy wpływ na wydajność systemu.

Zalecana wartość: Wartość *SYS zapewnia najlepszą wydajność kontroli. Jednak jeśli instalacja użytkownika wymaga, aby żadna pozycja kontroli nie została utracona, gdy system nieprawidłowo zakończy działanie, należy podać wartość 1. Podanie 1 może zmniejszyć wydajność.

Poziom kontroli (QAUDLVL)

Wartość systemowa QAUDLVL łącznie z wartością QAUDLVL2 określa, czy dla wszystkich użytkowników systemu w kronice kontroli ochrony (QAUDJRN) protokołowane są zdarzenia związane z ochroną systemu. Dla wartości systemowej QAUDLVL można podać więcej niż jedną wartość, chyba że jest to wartość *NONE.

Aby wartość systemowa QAUDLVL mogła działać, wartość systemowa QAUDCTL musi zawierać wartość *AUDLVL.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 46. Możliwe wartości dla wartości systemowej QAUDLVL

***NONE**	Nie będą protokołowane żadne zdarzenia kontrolowane przez wartości systemowe QAUDLVL lub QAUDLVL2. Zdarzenia protokołowane są dla pojedynczych użytkowników w oparciu o wartości AUDLVL dla profili użytkowników.
***AUDLVL2**	W celu określenia kontrolowanych działań ochrony będą użyte wartości systemowe QAUDLVL i QAUDLVL2.
***AUTFAIL**	Protokołowane są zdarzenia błędu uprawnień.
***CREATE**	Protokołowane są operacje tworzenia obiektu.
***DELETE**	Protokołowane są operacje usunięcia obiektu.
***JOBDTA**	Protokołowane są działania wpływające na zadanie.
***NETBAS**	Kontrolowane są podstawowe funkcje sieciowe.
***NETCLU**	Kontrolowane są operacje klastra i grupy zasobów klastra.
***NETCMN**	Kontrolowane są funkcje sieci i komunikacji. Parametr *NETCMN składa się z kilku wartości umożliwiających lepsze dostosowanie kontroli. Na parametr *NETCMN składają się następujące wartości: *NETBAS, *NETCLU, *NETFAIL, *NETSCK.
***NETFAIL**	Kontrolowane są awarie sieci.
***NETSCK**	Kontrolowane są zadania gniazd.
***OBJMGT**	Protokołowane są operacje przenoszenia i zmiany nazwy obiektu.
***OFCSRV**	Protokołowane są zmiany katalogu dystrybucyjnego systemu oraz działania poczty.
***OPTICAL**	Protokołowane jest użycie woluminów optycznych.
***PGMADP**	Protokołowane jest uzyskiwanie uprawnień z programów, które adoptują uprawnienia.
***PGMFAIL**	Protokołowane są naruszenia integralności systemu.

Tabela 46. Możliwe wartości dla wartości systemowej QAUDLVL (kontynuacja)

***PRTDTA**	Protokołowane jest drukowanie zbiorów buforowych, bezpośrednie wysyłanie wydruków do drukarki oraz wysyłanie wydruków do zdalnej drukarki.
***SAVRST**	Protokołowane są operacje odtwarzania.
***SECCFG**	Kontrolowane jest konfigurowanie ochrony.
***SECDIRSRV**	Kontrolowane są zmiany lub aktualizacje podczas wykonywania funkcji usług katalogowych.
***SECIPC**	Kontrolowane są zmiany w komunikacji międzyprocesorowej.
***SECNAS**	Kontrolowane są działania usługi uwierzytelniania sieciowego.
***SECRUN**	Kontrolowane są funkcje uruchamiania ochrony.
***SECSCKD**	Kontrolowane są opisy gniazda.
***SECURITY**	Protokołowane są funkcje związane z ochroną. Parametr *SECURITY składa się z kilku wartości umożliwiających lepsze dostosowanie kontroli. Na parametr *SECURITY składają się następujące wartości: *SECCFG, *SECDIRSRV, *SECIPC, *SECNAS, *SECRUN, *SECSCKD, *SECVFY, *SECVLDL.
***SECVFY**	Kontrolowane jest użycie funkcji sprawdzania.
***SECVLDL**	Kontrolowane są zmiany obiektów listy sprawdzania.
***SERVICE**	Protokołowane jest użycie narzędzi serwisowych.
***SPLFDTA**	Protokołowane są działania wykonywane na zbiorach buforowych.
***SYSMGT**	Użycie funkcji zarządzania systemem jest protokołowane.

Pełną listę typów pozycji kroniki oraz możliwe wartości QAUDLVL zawiera sekcja “Planowanie kontroli działania” na stronie 238.

Rozszerzenie poziomu kontroli (QAUDLVL2)

Wartość systemowa QAUDLVL2 jest wymagana, gdy potrzebnych jest więcej niż szesnaście wartości kontroli. Podanie wartości *AUDLVL2 jako jednej z wartości dla wartości systemowej QAUDLVL spowoduje, że system sprawdzi także wartości kontroli podane dla QAUDLVL2. Dla wartości systemowej QAUDLVL2 można podać więcej niż jedną wartość, chyba że jest to wartość *NONE. Aby wartość systemowa QAUDLVL2 mogła działać, wartość systemowa QAUDCTL musi zawierać wartość *AUDLVL, a wartość QAUDLVL musi zawierać *AUDLVL2.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 47. Możliwe wartości dla wartości systemowej QAUDLVL2

***NONE**	W tej wartości systemowej nie są zawarte żadne wartości kontroli.
***AUTFAIL**	Protokołowane są zdarzenia błędu uprawnień.
***CREATE**	Protokołowane są operacje tworzenia obiektu.
***DELETE**	Protokołowane są operacje usunięcia obiektu.
***JOBDTA**	Protokołowane są działania wpływające na zadanie.
***NETBAS**	Kontrolowane są podstawowe funkcje sieciowe.
***NETCLU**	Kontrolowane są operacje klastra i grupy zasobów klastra.

| *Tabela 47. Możliwe wartości dla wartości systemowej QAUDLVL2 (kontynuacja)*

***NETCMN**	Kontrolowane są funkcje sieci i komunikacji. Parametr *NETCMN składa się z kilku wartości umożliwiających lepsze dostosowanie kontroli. Na parametr *NETCMN składają się następujące wartości: *NETBAS, *NETCLU, *NETFAIL, *NETSCK.
***NETFAIL**	Kontrolowane są awarie sieci.
***NETSCK**	Kontrolowane są zadania gniazd.
***OBJMGT**	Protokołowane są operacje przenoszenia i zmiany nazwy obiektu.
***OFCSRV**	Protokołowane są zmiany katalogu dystrybucyjnego systemu oraz działania poczty.
***OPTICAL**	Protokołowane jest użycie woluminów optycznych.
***PGMADP**	Protokołowane jest uzyskiwanie uprawnień z programów, które adoptują uprawnienia.
***PGMFAIL**	Protokołowane są naruszenia integralności systemu.
***PRTDTA**	Protokołowane jest drukowanie zbiorów buforowych, bezpośrednie wysyłanie wydruków do drukarki oraz wysyłanie wydruków do zdalnej drukarki.
***SAVRST**	Protokołowane są operacje odtwarzania.
***SECCFG**	Kontrolowane jest konfigurowanie ochrony.
***SECDIRSRV**	Kontrolowane są zmiany lub aktualizacje podczas wykonywania funkcji usług katalogowych.
***SECIPC**	Kontrolowane są zmiany w komunikacji międzyprocesorowej.
***SECNAS**	Kontrolowane są działania usługi uwierzytelniania sieciowego.
***SECRUN**	Kontrolowane są funkcje uruchamiania ochrony.
***SECSCKD**	Kontrolowane są opisy gniazda.
***SECURITY**	Protokołowane są funkcje związane z ochroną. Parametr *SECURITY składa się z kilku wartości umożliwiających lepsze dostosowanie kontroli. Na parametr *SECURITY składają się następujące wartości: *SECCFG, *SECDIRSRV, *SECIPC, *SECNAS, *SECRUN, *SECSCKD, *SECVFY, *SECVLDL.
***SECVFY**	Kontrolowane jest użycie funkcji sprawdzania.
***SECVLDL**	Kontrolowane są zmiany obiektów listy sprawdzania.
***SERVICE**	Protokołowane jest użycie narzędzi serwisowych.
***SPLFDTA**	Protokołowane są działania wykonywane na zbiorach buforowych.
***SYSMGT**	Użycie funkcji zarządzania systemem jest protokołowane.

| Pełną listę typów pozycji kroniki oraz możliwe wartości QAUDLVL2 zawiera sekcja “Planowanie kontroli działania” na stronie 238.

Kontrola nowych obiektów (QCRTOBJAUD)

Wartość systemowa QCRTOBJAUD używana jest w celu określenia wartości kontroli dla nowych obiektów, jeśli domyślna kontrola dla biblioteki nowego obiektu ustawiona jest na *SYSVAL. Wartość systemowa QCRTOBJAUD jest także domyślną wartością kontroli obiektu dla dokumentów znajdujących się poza folderami.

Na przykład wartość CRTOBJAUD dla biblioteki CUSTLIB to *SYSVAL. Wartość QCRTOBJAUD to *CHANGE. Jeśli w bibliotece CUSTLIB tworzony jest nowy obiekt, jego wartość kontroli automatycznie będzie ustawiona na *CHANGE. Wartość kontroli obiektu można zmienić za pomocą komendy CHGOBJAUD.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Aby uzyskać informacje o tym, w jaki sposób ograniczać zmiany wartości systemowych ochrony oraz zapoznać się z pełną listą ograniczonych wartości systemowych, należy przejść do Rozdziału 3: ″Wartości systemowe ochrony″.

Tabela 48. Możliwe wartości dla wartości systemowej QCRTOBJAUD

***NONE**	Brak kontroli obiektu.
***USRPRF**	Kontrolowanie obiektu przeprowadzane jest w oparciu o wartość w profilu użytkownika uzyskującego dostęp do obiektu.
***CHANGE**	Rekord kontroli zapisywany jest podczas każdej zmiany obiektu.
***ALL**	Rekord kontroli zapisywany jest dla każdego działania wpływającego na zawartość obiektu. Rekord kontroli zapisywany jest także gdy zmieni się zawartość obiektu.

Zalecana wartość: wybrana wartość zależy od wymagań kontroli dla danej instalacji. Sekcja “Planowanie kontroli dostępu do obiektu” na stronie 256 udostępnia informacje dotyczące metod konfigurowania kontroli obiektu w systemie. Wartością kontroli można sterować także z poziomu biblioteki za pomocą parametru CRTOBJAUD komendy CRTLIB i CHGLIB.

Rozdział 4. Profile użytkowników

Ten rozdział opisuje profile użytkowników: ich przeznaczenie, opcje oraz sposób ich projektowania. Profile użytkowników to elastyczne narzędzie o dużych możliwościach. Ich dobre zaprojektowanie może pomóc zabezpieczać system oraz dostosować go do potrzeb użytkowników.

Przegląd:

Przeznaczenie:
Tworzenie i obsługa profili użytkowników oraz profili grupowych w systemie.

Sposób używania:
Praca z profilami użytkowników (Work with User Profiles - WRKUSRPRF), komenda

Komenda Zmiana kontroli użytkownika (Change User Audit - CHGUSRAUD).

Uprawnienia:
Uprawnienie specjalne *SECADM.

Uprawnienie specjalne *AUDIT do zmiany kontroli użytkownika.

Pozycja kroniki:
CP dla zmian profili użytkowników.

AD dla zmian kontroli użytkownika.

ZC dla zmian profilu użytkownika, które nie są związane z ochroną.

Role profilu użytkownika

Profil użytkownika w systemie ma kilka ról:

- przechowuje informacje związane z ochroną, które sterują sposobem, w jaki użytkownik wpisuje się do systemu, a także określają, co może zrobić po wpisaniu się i jak kontrolowane są wykonywane przez niego działania,
- przechowuje informacje, które dostosowują system i dopasowują go do użytkownika,
- jest to narzędzie do zarządzania i odzyskiwania używane przez system operacyjny; profil użytkownika przechowuje informacje na temat obiektów posiadanych przez użytkownika oraz wszystkich uprawnień prywatnych do tych obiektów,
- nazwa profilu użytkownika identyfikuje jego zadania oraz zbiory wydruku.

Jeśli w systemie ustawiono wartość systemową poziomu ochrony (QSECURITY) na 10, podczas wpisywania się za pomocą identyfikatora użytkownika, automatycznie tworzony jest profil tego użytkownika, jeśli jeszcze nie istnieje w systemie. Tabela 143, Dodatek B, zawiera wartości przypisywane podczas tworzenia profilu użytkownika przez system.

Jeśli wartość systemowa QSECURITY ma wartość 20 lub wyższą, zanim użytkownik będzie mógł się wpisać, jego profil musi istnieć.

Profile grupowe

Profil grupowy jest szczególnym typem profilu użytkownika. W systemie pełni podwójną rolę:

Narzędzie ochrony
Profil grupowy udostępnia metodę organizowania uprawnień w systemie oraz współużytkowania ich przez użytkowników. Zamiast dla każdego pojedynczego profilu użytkownika, uprawnienia do obiektu lub uprawnienia specjalne można zdefiniować dla profilu grupowego. Użytkownik może być członkiem do 16 profili grupowych.

Narzędzie dostosowujące

Profil grupowy może być wykorzystany jako wzorzec do tworzenia pojedynczych profili użytkowników. Większość osób należących do tej samej grupy ma takie same potrzeby konfiguracyjne, takie jak menu początkowe oraz domyślna drukarka. Te elementy można zdefiniować w profilu grupowym, a następnie skopiować je w celu utworzenia pojedynczych profili użytkowników.

Profile grupowe tworzy się w taki sam sposób, jak pojedyncze profile użytkowników. System rozpoznaje profil grupowy po dodaniu do niego pierwszego członka. Od tego momentu system ustawia informacje w profilu wskazujące, że jest to profil grupowy. System generuje także dla takiego profilu numer identyfikacyjny grupy (group identification number - gid). Użytkownik może także wskazać, że profil będzie profilem grupowym, podając wartość dla parametru GID podczas tworzenia profilu. Sekcja “Planowanie profili grupowych” na stronie 218 opisuje przykład konfigurowania profilu grupowego.

Pola parametrów profilu użytkownika

Profile użytkowników mogą być tworzone w następujący sposób:

- za pomocą programu iSeries Navigator,
- za pomocą Centrum Zarządzania,
- za pomocą interfejsu znakowego.

Podczas tworzenia profilu użytkownika, nadaje on sam sobie następujące uprawnienia: *OBJMGT, *CHANGE. Te uprawnienia są wymagane dla funkcji systemowych i nie powinny być usuwane.

Poniżej zaprezentowano wyjaśnienia wszystkich pól w profilu użytkownika. Pola opisane są według kolejności ich pojawiania się na ekranie Tworzenie profilu użytkownika (Create User Profile).

Wiele ekranów systemu ma różne wersje nazywane **poziomami asysty**, tak aby spełnić wymagania różnych użytkowników:

- podstawowy poziom asysty, który zawiera mniej informacji i nie korzysta z terminologii technicznej,
- średni poziom asysty, który zawiera więcej informacji i korzysta z terminów technicznych,
- zaawansowany poziom asysty, który korzysta z terminów technicznych i pokazuje maksymalną ilość danych, ale nie zawsze wyświetla klawisze funkcyjne oraz informacje o opcjach.

Przedstawione poniżej sekcje prezentują informacje o nazwach pól profilu użytkownika na ekranach z podstawowym i średnim poziomem asysty. Użyto następującego formatu:

Tytuł pola

Tytuł sekcji zawiera nazwę pola pojawiającą się na ekranie Tworzenie profilu użytkownika (Create User Profile), który jest wyświetlany podczas tworzenia profilu użytkownika z pośredni poziom asysty lub za pomocą komendy Tworzenie profilu użytkownika (Create User Profile - CRTUSRPRF).

Podpowiedź ekranu Dodanie użytkownika:

Pokazuje nazwę pola pojawiającą się na ekranie Dodanie użytkownika (ADD User) oraz pozostałych ekranach profilu użytkownika, które wykorzystują podstawowy poziom asysty. Ekrany z podstawowym poziomem asysty prezentują podzbiór pól profilu użytkownika. *Nie prezentowane* oznacza pole, które nie pojawia się na ekranie z podstawowym poziomem asysty. Podczas tworzenia profilu użytkownika za pomocą ekranu Dodanie użytkownika (Add User), we wszystkich pokazanych polach wstawione są wartości domyślne.

Parametr CL:

Nazwa parametru CL dla pola używana jest w programach CL lub gdy komenda profilu użytkownika wprowadzana jest bez podpowiedzi.

Długość:

Jeśli w programie CL używana jest komenda Odtworzenie profilu użytkownika (Retrieve User Profile - RTVUSRPRF), jest to długość, jaka powinna być użyta do zdefiniowania parametru związanego z polem.

Uprawnienia:

Jeśli pole odnosi się do oddzielnego obiektu, takiego jak biblioteka lub program, przedstawione zostaną wymagania dotyczące uprawnień do tego obiektu. Aby podczas tworzenia lub zmiany profilu użytkownika podać obiekt, wymagane są wymienione w tym miejscu uprawnienia. Aby wpisać się za pomocą danego profilu, użytkownik musi mieć wymienione uprawnienia. Na przykład jeśli tworzony jest profil użytkownika UŻYTKOWNIK_A z opisem zadania ZADANIE_1, to użytkownik musi mieć uprawnienia *USE do ZADANIA_1. Aby pomyślnie wpisać się za pomocą utworzonego profilu, UŻYTKOWNIK_A musi mieć uprawnienia *USE do ZADANIA_1.

Dodatkowo każda sekcja opisuje możliwe oraz zalecane wartości dla poszczególnych pól.

Nazwa profilu użytkownika

Podpowiedź ekranu Dodanie użytkownika:
Użytkownik

Parametr CL:
USRPRF

Długość:
10

Nazwa profilu użytkownika identyfikuje użytkownika w systemie. Ta nazwa profilu użytkownika znana jest także jako identyfikator użytkownika. Jest to nazwa, którą użytkownik wpisuje w polu *Użytkownik* ekranu Wpisanie się (Sing On).

Nazwa profilu użytkownika może mieć maksymalnie 10 znaków. Tymi znakami mogą być:

- dowolne litery (od A do Z),
- dowolne cyfry (od 0 do 9),
- znaki specjalne: funt (#), dolar ($), podkreślenie (_) i znak at (@).

Uwaga: Ekran Dodanie użytkownika (Add User) zezwala na podanie tylko ośmioznakowej nazwy użytkownika.

Nazwa profilu użytkownika nie może rozpoczynać się od cyfry.

Uwaga: Możliwe jest takie utworzenie profilu użytkownika, aby podczas wpisywania się mógł podawać wyłącznie liczby. Aby utworzyć taki profil, jako pierwszy znak należy podać literę Q, na przykład Q12345. Użytkownik może wtedy wpisywać się podając w polu *Użytkownik* na ekranie Wpisanie się (Sign On), 12345 lub Q12345.

Więcej informacji dotyczących podawania nazw w systemie zawiera podręcznik *CL Programming*.

Zalecenia dotyczące nazywania profili użytkowników: Podczas decydowania, jak nazwać profile użytkowników, należy rozważyć następujące kwestie:

- nazwa profilu użytkownika może mieć do 10 znaków; niektóre metody komunikacji ograniczają ją do ośmiu znaków; ekran Dodanie użytkownika (Add User) także ogranicza nazwę profilu użytkownika do ośmiu znaków,
- należy używać schematu nazewnictwa, który ułatwi zapamiętywanie identyfikatorów użytkowników,
- system nie rozróżnia wielkich i małych liter w nazwie profilu użytkownika, w przypadku wpisania małych liter alfabetu w stacji roboczej, system zamienia je na wielkie litery,
- ekrany i listy wykorzystywane do zarządzania profilami użytkowników prezentują je w porządku alfabetycznym, według nazwy,
- należy unikać stosowania znaków specjalnych; znaki specjalne mogą powodować problemy z odwzorowaniem klawiatury na niektórych stacjach roboczych lub związanych z wersjami w języku narodowym programu licencjonowanego OS/400.

Jedną z technik nadawania nazwy profilowi użytkownika jest użycie pierwszych siedmiu znaków nazwiska, z następującym po nich pierwszym znakiem imienia. Na przykład:

Nazwa użytkownika	Nazwa profilu użytkownika
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Harrisburg, Keith	HARRISBK
Jones, Sharon	JONESS
Jones, Keith	JONESK

Zalecenia dotyczące nazywania profili grupowych: Jeśli profile grupowe mają być łatwe do zidentyfikowania na listach lub ekranach, należy użyć konwencji nazewnictwa. Wszystkie nazwy profili grupowych powinny rozpoczynać się od tych samych znaków, na przykład GRP (od grupa) lub WYD (od wydziału).

Hasło

Podpowiedź ekranu Dodanie użytkownika:
Hasło

Parametr CL:
PASSWORD

Długość:
128

Hasło wykorzystywane jest do sprawdzania uprawnienia użytkownika do wpisywania się do systemu. Aby wpisać się, gdy aktywna jest ochrona przy użyciu hasła (wartość systemowa QSECURITY ustawiona jest na wartość 20 lub wyższą), wymagane jest podanie identyfikatora użytkownika oraz hasła.

Gdy wartość systemowa QPWDLVL ustawiona jest na 0 lub 1, hasło może mieć maksymalnie 10 znaków. Natomiast gdy wartość QPWDLVL jest ustawiona na 2 lub 3, hasło może mieć 128 znaków.

Gdy wartość systemowa poziomu hasła (QPWDLVL) ustawiona jest na 0 lub 1, reguły dotyczące podawania haseł są takie same, jak reguły dla nazw profilu użytkownika. Jeśli pierwszym znakiem hasła jest litera Q, a następnym znakiem jest cyfra, wtedy podczas wpisywania hasła na ekranie Wpisanie się (Sign On), litera Q może zostać pominięta. Jeśli na ekranie Zmiana hasła (Change Password) użytkownik podał hasło Q12345, to na ekranie Wpisanie się (Sing On) może podać albo 12345, albo Q12345. Gdy wartość systemowa QPWDLVL ustawiona jest na 2 lub 3, na ekranie wpisywania się użytkownik musi podać hasło Q12345, jeśli takie hasło zostało podane podczas tworzenia profilu użytkownika. Hasła numeryczne dozwolone są na poziomie 2 lub 3 wartości QPWDLVL, ale hasło profilu użytkownika musi być utworzone jako tylko numeryczne.

Gdy wartość systemowa poziomu hasła (QPWDLVL) ustawiona jest na 2 lub 3, w haśle rozróżniana jest wielkość liter, a hasło może zawierać dowolny znak, również odstępy. Jednak hasło nie może rozpoczynać się od znaku gwiazdki (’*’), a puste znaki końcowe są usuwane.

Uwaga: Hasła mogą być tworzone za pomocą znaków dwubajtowych. Jednak hasło zawierające znaki dwubajtowe nie może posłużyć do wpisywania się za pomocą ekranu wpisania. Hasła zawierające znaki dwubajtowe mogą być utworzone za pomocą komend CRTUSRPRF i CHGUSRPRF, a przekazane do systemu za pomocą funkcji API, które obsługują parametr hasła.

Szyfrowanie jednokierunkowe wykorzystywane jest do przechowywania hasła w systemie. Jeśli hasło zostanie zapomniane, szef ochrony może użyć komendy Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF), aby przypisać hasło tymczasowe i ustawić je jako wygasłe, wymagając w ten sposób, aby użytkownik podał nowe hasło podczas następnego wpisania się.

Wartości systemowe można wykorzystać do kontrolowania haseł, których używają użytkownicy. Wartości systemowe komponowania hasła mają zastosowanie jedynie wtedy, gdy użytkownik zmienia hasło za pomocą komendy Zmiana hasła (Change Password - CHGPWD) opcji Zmiana hasła z menu ASSIST lub za pomocą funkcji API QSYCHGPW. Jeśli wartość systemowa minimalnej długości hasła (QPWDMINLEN) ma wartość inną niż 1 lub wartość systemowa maksymalnej długości hasła (QPWDMAXLEN) ma wartość inną niż 10 lub inne dowolne wartości systemowe kompozycji hasła mają zmienione wartości domyślne, użytkownik nie może podać hasła równego nazwie swojego profilu korzystając z komendy CHGPWD, menu ASSIST lub funkcji API QSYCHGPW.

Więcej informacji na temat ustawiania wartości systemowych kompozycji hasła zawiera temat “Wartości systemowe dotyczące haseł” na stronie 38.

Tabela 49. Możliwe wartości parametru PASSWORD:

***USRPRF**	Hasło dla tego użytkownika jest takie samo, jak jego nazwa profilu. Gdy wartość systemowa poziomu hasła (QPWDLVL) ustawiona jest na 2 lub 3, hasło będzie miało nazwę profilu użytkownika, ale pisane wielkimi literami. Dla profilu JOHNDOE, hasło będzie miało wartość JOHNDOE, a nie johndoe.
***NONE**	Dla tego profilu użytkownika nie przypisano hasła. Za pomocą takiego profilu użytkownika nie można się wpisywać. Jeśli użytkownik ma odpowiednie uprawnienia do profilu użytkownika, może wprowadzić zadanie wsadowe przy użyciu profilu użytkownika z hasłem o wartości *NONE.
hasło- użytkownika	Łańcuch znaków (128 znaków lub mniej).

Zalecenia dotyczące haseł:

- Dla profilu grupowego hasło powinno mieć wartość *NONE. Zapobiegnie to wpisywaniu się za pomocą profilu grupowego.
- Podczas tworzenia pojedynczego profilu użytkownika hasło należy ustawić na wartość początkową, a następnie żądać podania nowego hasła podczas wpisywania się użytkownika (wartość parametru wygasłego hasła należy ustawić na *YES). Domyślne hasło podczas tworzenia profilu użytkownika jest takie samo, jak nazwa profilu.
- Jeśli podczas tworzenia nowego profilu użytkownika wybierane jest proste lub domyślne hasło, należy upewnić się, że użytkownik zamierza natychmiast wpisać się do systemu. Jeśli oczekiwane jest opóźnienie przed wpisaniem się użytkownika, status profilu użytkownika należy ustawić na *DISABLED. Gdy użytkownik będzie gotowy do wpisania się, status należy zmienić na *ENABLED. Zapobiegnie to użyciu nowego profilu użytkownika przez kogoś, kto nie jest do tego upoważniony.
- Aby zapobiec ustawianiu prostych haseł, należy użyć wartości systemowych kompozycji haseł.
- Niektóre metody komunikacji wysyłają hasła między systemami oraz ograniczają długość hasła i znaki, które może zawierać. Jeśli system komunikuje się z innymi systemami, należy użyć wartości systemowej QPWDMAXLEN, która ogranicza długość hasła. Na poziomach haseł 0 i 1, wartość systemowa QPWDLMTCHR może być użyta do podania znaków, które nie mogą być używane w hasłach.

Ustawienie hasła jako wygasłe

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
PWDEXP

Długość:
4

Pole *Ustawienie hasła jako wygasłe* umożliwia administratorowi ochrony wskazanie w profilu użytkownika, że jego hasło wygasło i musi być zmienione podczas następnego wpisywania się. Po zmianie hasła ta wartość jest resetowana do wartości *NO. Hasło można zmienić za pomocą komendy CHGPWD lub CHGUSRPRF, funkcji API QSYCHGPW lub jako część procesu następnego wpisywania się.

To pole może być użyte, gdy użytkownik nie może przypomnieć sobie hasła, a administrator ochrony musi przypisać mu nowe. Wymaganie zmiany hasła przez użytkownika zapobiega poznaniu przez administratora ochrony nowego hasła oraz wpisaniu się za użytkownika.

Gdy hasło użytkownika wygaśnie, na ekranie wpisywania się otrzyma on komunikat (patrz Rys. 1). Użytkownik może nacisnąć klawisz Enter, aby podać nowe hasło lub klawisz F3 (Wyjście), aby anulować próbę wpisywania się bez podawania nowego hasła. Jeśli użytkownik wybierze zmianę hasła, prezentowany jest ekran Zmiana hasła (Change Password), a dla nowego hasła przeprowadzane jest sprawdzanie.

```
                    Informacje wpisania się
                     (Sign-on Information)
                                                          System:
Hasło wygasło. Aby wpisać się do systemu musisz zmienić
hasło.

Poprzednie wpisanie się  . . . . . :   10/30/91  14:15:00
```

Rysunek 1. Komunikat o wygaśnięciu hasła

Tabela 50. Możliwe wartości parametru PWDEXP:

***NO:**	Hasło nie jest ustawione jako wygasłe.
***YES:**	Hasło jest ustawione jako wygasłe.

Zalecenia: Ustawienie hasła jako wygasłe należy stosować podczas tworzenia nowego profilu użytkownika lub przypisywania tymczasowego hasła.

Status

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
STATUS

Długość:
10

Wartość pola *Status* wskazuje, czy profil jest poprawny i umożliwia wpisywanie się. Jeśli status profilu ma wartość włączony, to profil jest poprawny do wpisywania się. Jeśli status profilu ma wartość wyłączony, uprawniony użytkownik musi ponownie włączyć profil, tak aby był poprawny do wpisywania się.

Aby włączyć profil, można użyć komendy CHGUSRPRF. Aby zmienić status profilu, użytkownik musi mieć uprawnienia specjalne *SECADM oraz uprawnienia *OBJMGT i *USE do danego profilu. Temat “Włączanie profilu użytkownika” na stronie 105 zawiera przykład programu adoptującego uprawnienia, który umożliwia operatorowi systemu włączanie profilu.

W zależności od ustawień wartości systemowych QMAXSIGN i QMAXSGNACN system może wyłączyć profil po pewnej liczbie nieprawidłowych prób wpisania się za pomocą danego profilu.

Za pomocą profilu QSECOFR (szef ochrony) zawsze można wpisać się z poziomu konsoli, nawet jeśli profil QSECOFR ma status *DISABLED. Jeśli profil użytkownika QSECOFR zostanie wyłączony, należy wpisać się z poziomu konsoli jako użytkownik QSECOFR i wpisać komendę CHGUSRPRF QSECOFR STATUS(*ENABLED).

Tabela 51. Możliwe wartości parametru STATUS:

***ENABLED**	Profil jest poprawny do wpisywania się.
***DISABLED**	Profil nie jest poprawny do wpisywania się, do czasu aż autoryzowany użytkownik nie włączy go ponownie.

Zalecenia: Statusu *DISABLED należy używać, jeśli operator chce zapobiec wpisywaniu się za pomocą danego profilu użytkownika. Na przykład można wyłączyć profil użytkownika, który przez dłuższy czas będzie nieobecny.

Klasa użytkownika

Podpowiedź ekranu Dodanie użytkownika:
Rodzaj użytkownika

Parametr CL:
USRCLS

Długość:
10

Klasa użytkownika używana jest do sterowania tym, jakie opcje menu użytkownik widzi w menu systemu OS/400. To niekoniecznie ogranicza użycie komend. To pole *Ograniczenie możliwości* okresla, czy użytkownik może wprowadzać komendy. Klasa użytkownika może nie wpływać na to, jakie opcje wyświetlane są w menu udostępnianych przez inne programy licencjonowane.

Jeśli podczas tworzenia profilu użytkownika nie podano uprawnień specjalnych, do określania uprawnień specjalnych danego użytkownika wykorzystywana jest klasa użytkownika oraz wartość systemowa poziomu ochrony (QSECURITY).

Możliwe wartości dla parametru USRCLS: Tabela 52 opisuje możliwe klasy użytkowników oraz domyślne uprawnienia specjalne dla każdej z klas. Pozycje wskazują, że uprawnienia nadawane jest tylko na poziomach ochrony 10 i 20, na wszystkich poziomach ochrony lub wcale.

Domyślną wartością dla klasy użytkownika jest wartość ***USER**.

Tabela 52. Domyślne uprawnienia specjalne według klasy użytkownika

Uprawnienie specjalne	**Klasy użytkowników**				
	***SECOFR**	***SECADM**	***PGMR**	***SYSOPR**	***USER**
*ALLOBJ	Wszystkie	10 lub 20	10 lub 20	10 lub 20	10 lub 20
*SECADM	Wszystkie	Wszystkie			
*JOBCTL	Wszystkie	10 lub 20	10 lub 20	Wszystkie	
*SPLCTL	Wszystkie				
*SAVSYS	Wszystkie	10 lub 20	10 lub 20	Wszystkie	10 lub 20
*SERVICE	Wszystkie				
*AUDIT	Wszystkie				
*IOSYSCFG	Wszystkie				

Zalecenia: Większość użytkowników nie musi wykonywać funkcji systemowych. Klasę użytkownika należy ustawić na wartość *USER, chyba że użytkownik potrzebuje korzystać z funkcji systemowych.

Poziom asysty

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
ASTLVL

Długość:
10

Dla każdego użytkownika system śledzi ostatni poziom asysty, który został użyty dla każdego ekranu systemowego, który ma więcej niż jeden poziom asysty. Ten poziom używany jest podczas następnego żądania ekranu przez użytkownika. Podczas aktywnego zadania użytkownik może zmienić poziom asysty dla ekranu lub grupy pokrewnych ekranów, naciskając klawisz F21 (Wybór poziomu asysty). Nowy poziom asysty dla tego ekranu przechowywany jest razem z informacjami o użytkowniku.

Podanie parametru poziomu asysty (ASTLVL) w komendzie nie zmienia poziomu asysty, który przechowywany jest w informacjach użytkownika dla związanego z nią ekranu.

Pole *Poziom asysty* w profilu użytkownika używane jest do określania domyślnego poziomu asysty dla użytkownika. Jeśli poziom asysty zostanie zmieniony za pomocą komendy CHGUSRPRF lub komendy Zmiana profilu (Change Profile - CHGPRF), poziomy asysty przechowywane dla wszystkich ekranów danego użytkownika zostaną zresetowane do nowej wartości.

Na przykład profil użytkownika dla UŻYTKOWNIKA_A tworzony jest z domyślnym poziomem asysty (podstawowym). Tabela 53 pokazuje, czy UŻYTKOWNIK_A widzie ekran Praca z profilami użytkowników (Work with User Profiles) czy ekran Praca z rejestrowaniem użytkowników (Work with User Enrollment) podczas używania różnych opcji. Tabela pokazuje także, czy system zmienia wersję ekranu, która jest przechowywana razem z profilem UŻYTKOWNIKA_A.

Tabela 53. W jaki sposób poziomy asysty są przechowywane i zmieniane

Podejmowane działanie	Wersja wyświetlanego ekranu	Wersja zapamiętywanego ekranu
Użycie komendy WRKUSRPRF	Ekran Praca z rejestrowaniem użytkowników	Brak zmian (podstawowy poziom asysty)
Naciśnięcie na ekranie Praca z rejestrowaniem użytkowników klawisza F21 i wybranie pośredni poziom asysty.	Ekran Praca z profilami użytkowników	Zmiana na pośredni poziom asysty
Użycie komendy WRKUSRPRF	Ekran Praca z profilami użytkowników	Brak zmian (średni poziom asysty)
Wybranie opcji Praca z rejestrowaniem użytkowników z menu SETUP.	Ekran Praca z profilami użytkowników	Brak zmian (średni poziom asysty)
Wpisanie komendy CHGUSRPRF USERA ASTLVL(*BASIC)		Zmiana na podstawowy poziom asysty
Użycie komendy WRKUSRPRF	Ekran Praca z rejestrowaniem użytkowników	Brak zmian (podstawowy poziom asysty)
Wpisanie komendy WRKUSRPRF ASTLVL(*INTERMED)	Ekran Praca z profilami użytkowników	Brak zmian (podstawowy poziom asysty)

Uwaga: Pole *Opcje użytkownika* w profilu użytkownika także wpływają na sposób wyświetlania ekranów systemowych. To pole zostało opisane na stronie 91.

Tabela 54. Możliwe wartości parametru ASTLVL:

***SYSVAL**	Użyty zostanie poziom asysty podany dla wartości systemowej QASTLVL.
***BASIC**	Użyty zostanie interfejs użytkownika Asysty Operacyjnej.
***INTERMED**	Użyty zostanie interfejs systemu.
***ADVANCED**	Użyty zostanie interfejs systemu typu ekspert. Aby umożliwić wyświetlenie większej liczby pozycji, numery opcji i klawisze funkcyjne nie zawsze są wyświetlane. Jeśli komenda nie ma zaawansowanego poziomu (*ADVANCED), użyty zostanie poziom średni (*INTERMED).

Biblioteka bieżąca

Podpowiedź ekranu Dodanie użytkownika:
Biblioteka domyślna

Parametr CL:
CURLIB

Długość:
10

Uprawnienia
*USE

Dla dowolnych obiektów typu *LIBL, przed bibliotekami z części użytkownika listy bibliotek, przeszukiwana jest biblioteka bieżąca. Jeśli użytkownik tworzy obiekty i podaje parametr *CURLIB, obiekty umieszczane są w bibliotece bieżącej.

Podczas wpisywania się użytkownika, biblioteka bieżąca automatycznie jest dodawana do listy bibliotek użytkownika. Nie musi być dołączana do początkowej listy bibliotek w opisie zadania użytkownika.

Jeśli pole *Ograniczenie możliwości* w profilu użytkownika ma wartość *YES lub *PARTIAL, użytkownik nie może mienić biblioteki bieżącej.

Temat “Listy bibliotek” na stronie 187 udostępnia więcej informacji dotyczących używania listy bibliotek oraz biblioteki bieżącej.

Tabela 55. Możliwe wartości parametru CURLIB:

***CRTDFT**	Ten użytkownik nie ma biblioteki bieżącej. Jeśli obiekty tworzone są z użyciem parametru *CURLIB, jako domyślna biblioteka bieżąca używana jest biblioteka QGPL.
nazwa_biblioteki_bieżącej	Nazwa biblioteki.

Zalecenia: Pola *Biblioteka bieżąca* należy używać do kontrolowania, gdzie użytkownicy mogą umieszczać nowe obiekty, takie jak programy Query. Pola *Ograniczenie możliwości* można użyć do zapobiegania zmienianiu przez użytkowników swoich bibliotek bieżących.

Program początkowy

Podpowiedź ekranu Dodanie użytkownika:
Program wpisywania się

Parametr CL:
INLPGM

Długość:
10 (nazwa programu) 10 (nazwa biblioteki)

Uprawnienia:
*USE do programu, *EXECUTE do biblioteki

Istnieje możliwość podania nazwy programu, który będzie wywoływany podczas wpisywania się użytkownika. Taki program uruchamia się przed wyświetleniem menu początkowego, jeśli takie istnieje. Jeśli pole *Ograniczenie możliwości* profilu użytkownika ma wartość *YES lub *PARTIAL, użytkownik nie może podać programu początkowego na ekranie wpisania się.

Program początkowy wywoływany jest tylko wtedy, gdy program routingu użytkownika to QCMD lub QCL. Więcej informacji na temat przetwarzania sekwencji wpisywania się użytkownika zawiera sekcja “Uruchamianie zadania interaktywnego” na stronie 179.

Programy początkowe używane są w dwóch głównych celach:

- do ograniczenia użytkownika do określonego zestawu funkcji,
- do przeprowadzenia przetwarzania początkowego, takiego jak otwieranie zbiorów lub ustanawianie listy bibliotek, podczas pierwszego wpisywania się użytkownika.

Do programu początkowego nie można przekazywać parametrów. Jeśli wykonanie programu początkowego nie powiedzie się, użytkownik nie będzie mógł się wpisać.

Tabela 56. Możliwe wartości parametru INLPGM:

***NONE**	Podczas wpisywania się użytkownika nie jest wywoływany żaden program. Jeśli dla parametru menu początkowego (INLMNU) podano nazwę menu, wyświetlane jest to menu.
nazwa_programu	Nazwa programu, który jest wywoływany podczas wpisywania się użytkownika.

Tabela 57. Możliwe wartości dla biblioteki INLPGM:

***LIBL**	Do odnalezienia programu używana jest lista bibliotek. Jeśli opis zadania dla profilu użytkownika ma listę bibliotek, używana jest ta lista. Jeśli opis zadania dla początkowej listy bibliotek ma wartość *SYSVAL, używana jest wartość systemowa QUSRLIBL.
***CURLIB**	Do odszukania programu używana jest biblioteka bieżąca podana w profilu użytkownika. Jeśli nie podano biblioteki bieżącej, używana jest biblioteka QGPL.
nazwa-biblioteki	Biblioteka, w której znajduje się program.

Menu początkowe

Podpowiedź ekranu Dodanie użytkownika:
Pierwsze menu

Parametr CL:
INLMNU

Długość:
10 (nazwa menu) 10 (nazwa biblioteki)

Uprawnienia
*USE do menu, *EXECUTE do biblioteki

Istnieje możliwość podania nazwy menu, które zostanie wyświetlone po wpisaniu się użytkownika. Menu początkowe wyświetlane jest po uruchomieniu programu początkowego użytkownika. Menu początkowe wywoływane jest tylko wtedy, gdy program routingu użytkownika to QCMD lub QCL.

Jeśli dla użytkownika ma być uruchomiony jedynie program początkowy, dla menu początkowego można podać wartość *SIGNOFF.

Jeśli pole *Ograniczenie możliwości* profilu użytkownika ma wartość *YES, użytkownik nie może podać innego menu początkowego na ekranie wpisania się. Jeśli użytkownik może podać menu początkowe na ekranie Wpisanie Się (Sing On), podane menu przesłania menu podane w profilu użytkownika.

Tabela 58. Możliwe wartości parametru MENU:

MAIN	Prezentowane jest Menu Główne systemu iSeries.
***SIGNOFF**	System wypisuje użytkownika po zakończeniu działania programu początkowego. Tego parametru można użyć w celu ograniczenia użytkowników do uruchamiania pojedynczego programu.
nazwa_menu	Nazwa menu, które wywoływane jest po wpisaniu się użytkownika.

Tabela 59. Możliwe wartości dla biblioteki MENU:

***LIBL**	Do odnalezienia menu używana jest lista bibliotek. Jeśli program początkowy dodaje pozycje do listy bibliotek, te pozycje także uwzględniane są podczas przeszukiwania, ponieważ menu wywoływane jest po wykonaniu programu początkowego.
***CURLIB**	Do odnalezienia menu wykorzystywana jest bieżąca biblioteka zadania. Jeśli na liście bibliotek nie znajduje się biblioteka bieżąca, używana jest biblioteka QGPL.
nazwa-biblioteki	Biblioteka, w której znajduje się menu.

Ograniczenie możliwości

Podpowiedź ekranu Dodanie użytkownika:
Ograniczenie użycia wiersza komend

Parametr CL:
LMTCPB

Długość:
10

Pole *Ograniczenie możliwości* można wykorzystać do ograniczenia użytkownikowi możliwości wprowadzania komend oraz do przesłonięcia programu początkowego, menu początkowego, biblioteki bieżącej oraz programu obsługi klawisza ATTN podanych w profilu użytkownika. To pole jest jednym z narzędzi zabezpieczających przed eksperymentowaniem przez użytkowników w systemie.

Użytkownik z parametrem LMTCPB(*YES) może uruchomić tylko te komendy, które zdefiniowano w parametrze dozwolone dla użytkownika z ograniczonymi możliwościami (ALWLMTUSR) z wartością *YES. Te komendy dostarczane są przez IBM z parametrem ALWLMTUSR(*YES):

Wpisanie się (Sign off - SIGNOFF),

Wysłanie komunikatu (Send message - SNDMSG),

Wyświetlenie komunikatów (Display messages - DSPMSG),

Wyświetlenie zadania (Display job - DSPJOB),

Wyświetlenie protokołu zadania (Display job log - DSPJOBLOG),

Uruchomienie PC Organizer (Start PC Organizer - STRPCO),

Praca z komunikatami (Work with Messages - WRKMSG).

Pole *Ograniczenie możliwości* w profilu użytkownika oraz parametr ALWLMTUSR komend mają zastosowanie tylko do tych komend, które uruchamiane są z wiersza komend, ekranu Wprowadzanie komendy (Command Entry) lub opcji menu grupowania komend. Użytkownicy nie są ograniczeni podczas wykonywania następujących czynności:

- uruchamianie komend w programach CL, które uruchamiają komendy jako wynik wyboru opcji z menu,
- uruchamianie zdalnych komend za pomocą aplikacji.

Istnieje możliwość zezwolenia użytkownikowi z ograniczonymi możliwościami na uruchamianie dodatkowych komend lub usuwanie niektórych komend z listy, przez zmianę parametru ALWLMTUSR dla danej komendy. W tym celu należy użyć komendy Zmiana komendy (Change Command - CHGCMD). Jeśli użytkownik tworzy własne komendy, parametr ALWLMTUSR może podać w komendzie Tworzenie komendy (Create Command - CRTCMD).

Możliwe wartości: Tabela 60 opisuje możliwe wartości pola *Ograniczenie możliwości* oraz funkcje dozwolone dla każdej wartości.

Tabela 60. Funkcje dozwolone dla wartości pola Ograniczenie możliwości

Funkcja	*YES	*PARTIAL	*NO
Zmiana programu początkowego	Nie	Nie	Tak
Zmiana menu początkowego	Nie	Tak	Tak

Tabela 60. Funkcje dozwolone dla wartości pola Ograniczenie możliwości (kontynuacja)

Funkcja	*YES	*PARTIAL	*NO
Zmiana biblioteki bieżącej	Nie	Nie	Tak
Zmiana programu klawisza ATTN	Nie	Nie	Tak
Wprowadzanie komend	Częściowo[1]	Tak	Tak

[1] Dozwolone są komendy: SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPJOBLOG, STRPCO, WRKMSG. Użytkownik nie może używać klawisza F9 do wyświetlania wiersza komend z dowolnego menu lub ekranu.

Zalecenia: Używanie menu początkowego, ograniczanie użycia wiersza komend oraz udostępnianie dostępu do menu umożliwia skonfigurowanie środowiska dla użytkowników, którzy nie potrzebują lub nie chcą mieć dostępu do funkcji systemowych. Więcej informacji na temat tego typu środowiska zawiera temat “Planowanie menu” na stronie 207.

Tekst

Podpowiedź ekranu Dodanie użytkownika:
Opis użytkownika

Parametr CL:
TEXT

Długość:
50

Tekst w profilu użytkownika służy do opisu danego profilu użytkownika oraz jego przeznaczenia. Dla profili użytkowników tekst powinien zawierać informacje identyfikacyjne, takie jak nazwę użytkownika oraz wydział. Dla profili grupowych tekst powinien identyfikować grupę, na przykład jakie wydziały obejmuje dana grupa.

Tabela 61. Możliwe wartości parametru text:

***BLANK:**	Nie podano tekstu.
opis	Należy podać nie więcej niż 50 znaków.

Zalecenia: Pole *Tekst* na wielu ekranach systemowych jest obcinane. Dlatego najważniejsze informacje identyfikacyjne należy umieścić na początku pola.

Uprawnienia specjalne

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
SPCAUT

Długość:
100 (10 znaków na każde uprawnienie specjalne)

Uprawnienia:
Aby nadać uprawnienie specjalne profilowi użytkownika, użytkownik musi mieć to uprawnienie specjalne.

Uprawnienia specjalne używane są do określanie rodzajów działania, które użytkownik może wykonać na zasobach systemu. Użytkownik może mieć nadane jedno lub więcej uprawnień specjalnych.

Tabela 62. Możliwe wartości parametru SPCAUT:

***USRCLS**	Uprawnienia specjalne są nadawane temu użytkownikowi w oparciu o pole klasy użytkownika (USRCLS) w profilu użytkownika oraz wartości systemowej poziomu ochrony (QSECURITY). Jeśli podana jest wartość *USRCLS, dla tego użytkownika nie można podać żadnych dodatkowych uprawnień specjalnych. Jeśli wartość *USRCLS zostanie podana podczas tworzenia lub zmiany profilu użytkownika, system umieszcza odpowiednie uprawnienia specjalne w profilu, tak jakby zostały wprowadzone przez użytkownika. Podczas wyświetlania profili nie widać, czy uprawnienia specjalne zostały podane pojedynczo, czy wprowadzone przez system w oparciu o klasę użytkownika. Tabela 52 na stronie 63 opisuje domyślne uprawnienia specjalne dla każdej klasy użytkownika.
***NONE**	Temu użytkownikowi nie są nadawane żadne uprawnienia specjalne.
nazwa_uprawnień_specjalnych	Należy podać jedno lub więcej uprawnień specjalnych. Uprawnienia specjalne zostały opisane w następnych sekcjach.

Uprawnienia specjalne *ALLOBJ

Uprawnienie specjalne *ALLOBJ umożliwia użytkownikowi dostęp do dowolnych zasobów na systemie, gdy dla tego użytkownika istnieje uprawnienie prywatne. Nawet jeśli użytkownik ma uprawnienia *EXCLUDE do danego obiektu, uprawnienia specjalne *ALLOBJ nadal umożliwiają mu dostęp do tego obiektu.

Ryzyko: Uprawnienia specjalne *ALLOBJ dają użytkownikowi obszerne uprawnienia do wszystkich zasobów w systemie. Użytkownik może przeglądać, zmieniać lub usuwać dowolne obiekty. Użytkownik może także nadawać uprawnienia do korzystania z obiektów innym użytkownikom.

Użytkownik z uprawnieniami *ALLOBJ nie może bezpośrednio wykonywać operacji, które wymagają innych uprawnień specjalnych. Na przykład uprawnienia specjalne *ALLOBJ nie umożliwiają użytkownikowi tworzenie innego profilu użytkownika, ponieważ tworzenie profili wymaga uprawnień specjalnych *SECADM. Jednak użytkownik z uprawnieniami specjalnymi *ALLOBJ może wprowadzić zadanie wsadowe, w celu skorzystania z profilu, które ma wymagane uprawnienia specjalne. Nadanie uprawnień specjalnych *ALLOBJ praktycznie daje użytkownikowi dostęp do wszystkich funkcji w systemie.

Uprawnienia specjalne *SECADM

Uprawnienia specjalne administratora ochrony (*SECADM) umożliwiają użytkownikowi tworzenie, zmienianie i usuwanie profili użytkowników. Użytkownik z uprawnieniami specjalnymi *SECADM może:

- dodawać użytkowników do katalogu dystrybucyjnego systemu,
- wyświetlać uprawnienia do dokumentów lub folderów,
- dodawać i usuwać z systemu kody dostępu,
- nadawać i usuwać uprawnienia użytkownika do kodu dostępu,
- dawać i usuwać użytkownikowi pozwolenie na pracę w imieniu innego użytkownika,
- usuwać dokumenty i foldery,
- usuwać listy dokumentów,
- zmieniać listy dystrybucyjne utworzone przez innych użytkowników.

Uprawnienia specjalne *SECADM innemu użytkownikowi może nadać tylko użytkownik z uprawnieniami *SECADM i *ALLOBJ.

Uprawnienia specjalne *JOBCTL

Uprawnienia specjalne sterowania zadaniem (*JOBCTL) umożliwiają użytkownikowi:

- zmianę, usuwanie, wstrzymywanie i zwalnianie wszystkich zbiorów w dowolnych kolejkach wyjściowych z parametrem OPRCTL(*YES),

- wyświetlanie, wysyłanie i kopiowanie wszystkich zbiorów w kolejkach wyjściowych z parametrami DSPDTA(*YES lub *NO) i OPRCTL(*YES),
- wstrzymywanie, zwalnianie i usuwanie zawartości kolejek zadań z parametrem OPRCTL(*YES),
- wstrzymywanie, zwalnianie i usuwanie zawartości kolejek wyjściowych z parametrem OPRCTL(*YES),
- wstrzymywanie, zwalnianie i usuwanie zadań innych użytkowników,
- uruchamianie, zmianę, zatrzymywanie, wstrzymywanie i zwalnianie programów piszących, jeśli kolejka wyjściowa ma podany parametr OPRCTL(*YES),
- zmianę atrybutów uruchomieniowych zadania, takich jak drukarka dla zadania,
- zatrzymywanie podsystemów,
- przeprowadzanie ładowania programu początkowego (IPL).

Ochrona zbiorów wydruków oraz kolejek wyjściowych omówiona została w sekcji “Drukowanie” na stronie 190.

Użytkownik może zmienić priorytet zadania (JOBPTY) oraz priorytet wyjścia (OUTPTY) własnego zadania bez konieczności posiadania uprawnień specjalnych sterowania zadaniem. Aby zmienić priorytet uruchomienia (RUNPTY) własnego zadania, uprawnienia *JOBCTL są wymagane.

Zmiany priorytetu wyjścia oraz priorytetu zadania są ograniczone przez limit priorytetu (PTYLMT) w profilu użytkownika dokonującego zmiany.

Ryzyko: Użytkownik z uprawnieniami specjalnymi *JOBCTL może zmienić priorytet zadań oraz drukowania, zakończyć zadanie przed jego wykonaniem lub usunąć wyjście, zanim zostanie wydrukowane. Uprawnienia specjalne *JOBCTL mogą dać użytkownikowi dostęp do poufnych zbiorów wydruku, jeśli w kolejkach wyjściowych podano parametr OPRCTL(*YES). Użytkownik, który niepoprawnie wykorzystuje uprawnienie specjalne *JOBCTL może spowodować pogorszenie wykonywania pojedynczych zadań, a przez to spadek wydajności całego systemu.

Uprawnienia specjalne *SPLCTL

Uprawnienia specjalne kontroli bufora (*SPLCTL) umożliwiają użytkownikowi wykonywanie wszystkich funkcji dotyczących kontroli bufora, takich jak zmienianie, usuwanie, wyświetlanie, wstrzymywanie i zwalnianie zbiorów buforowych. Użytkownik może wykonywać te funkcje na wszystkich kolejkach wyjściowych, niezależnie od uprawnień do kolejki wyjściowej lub parametru OPRCTL kolejki wyjściowej.

Uprawnienia specjalne *SPLCTL umożliwiają także zarządzanie kolejkami zadań, co obejmuje wstrzymywanie, zwalnianie i usuwanie zawartości kolejki zadań. Użytkownik może wykonywać te funkcje na wszystkich kolejkach zadań, niezależnie od uprawnień do kolejki zadań lub parametru OPRCTL kolejki zadań.

Ryzyko: Użytkownik z uprawnieniami specjalnymi *SPLCTL może wykonywać dowolne operacje na wszystkich zbiorach buforowych w systemie. Poufne zbiory buforowe nie mogą być zabezpieczone przed użytkownikiem z uprawnieniami specjalnymi *SPLCTL.

Uprawnienia specjalne *SAVSYS

Uprawnienie specjalne *SAVSYS nadaje użytkownikowi uprawnienie do składowania, odtwarzania i zwalniania pamięci dla wszystkich obiektów w systemie, bez względu na to, czy użytkownik ma uprawnienie Istnienie do tych obiektów.

Ryzyko: Użytkownik z uprawnieniami specjalnymi *SAVSYS może:

- składować obiekt i przenieść go do innego systemu iSeries w celu odtworzenia,
- składować obiekt i wyświetlić taśmę w celu przeglądania danych,
- składować obiekt i zwolnić pamięć, a zatem usunąć część danych obiektu,
- składować i usunąć dokument.

Uprawnienia specjalne *SERVICE

Uprawnienia specjalne serwisu (*SERVICE) umożliwiają użytkownikowi uruchomienie narzędzi SST za pomocą komendy STRSST. Umożliwiają także debugowanie programu, do którego ma on tylko uprawnienie *USE oraz wyświetlanie i zmienianie funkcji serwisowych. Funkcja zrzutu może być wykonana bez uprawnień *SERVICE. Uprawnienia te umożliwiają także wykonywanie różnych funkcji śledzenia.

Ryzyko: Użytkownik z uprawnieniami specjalnymi *SERVICE może wyświetlić i zmienić poufne dane korzystając z funkcji serwisowych. Aby zmienić informacje korzystając z funkcji serwisowych, użytkownik musi mieć uprawnienia specjalne *ALLOBJ.

Aby zminimalizować ryzyko dla komend śledzenia, użytkownicy mogą mieć nadane uprawnienia do wykonywania śledzenia serwisowego, bez konieczności nadawania im uprawnień specjalnych *SERVICE. W ten sposób tylko konkretni użytkownicy będą mieli możliwość wykonywania komendy śledzenia, która może dać im dostęp do wrażliwych danych. Użytkownik musi być uprawniony do komendy oraz mieć uprawnienia specjalne *SERVICE lub być uprawniony do funkcji śledzenia serwisowego systemu operacyjnego za pomocą opcji Administrowanie aplikacjami programu iSeries Navigator. Komenda Zmiana informacji o użyciu funkcji (Change Function Usage - QSYCHFUI), o identyfikatorze QIBM_SERVICE_TRACE, może być stosowana do zmiany listy użytkowników uprawnionych do wykonania operacji śledzenia.

Komendy, do których można w ten sposób nadać dostęp, obejmują:

Tabela 63.

STRCMNTRC	Uruchomienie śledzenia komunikacji (Start Communications Trace)
ENDCMNTRC	Zakończenie śledzenia komunikacji (End Communications Trace)
PRTCMNTRC	Drukowanie śledzenia komunikacji (Print Communications Trace)
DLTCMNTRC	Usunięcie śledzenia komunikacji (Delete Communications Trace)
CHKCMNTRC	Sprawdzenie śledzenia komunikacji (Check Communications Trace)
TRCCNN	Śledzenie połączenia (Trace Connection) (patrz sekcja “Nadawanie dostępu do opcji śledzenia”)
TRCINT	Śledzenie wewnętrzne (Trace Internal)
STRTRC	Uruchomienie śledzenia zadania (Start Job Trace)
ENDTRC	Zakończenie śledzenia zadania (End Job Trace)
PRTTRC	Drukowanie śledzenia zadania (Print Job Trace)
DLTTRC	Usunięcie śledzenia zadania (Delete Job Trace)

Nadawanie dostępu do opcji śledzenia: Komendy śledzenia, takie jak TRCCNN (Śledzenie połączenia - Trace Connection) są komendami o dużych możliwościach i dostęp do nich nie powinien być nadawany wszystkim użytkownikom, którzy wymagają dostępu do pozostałych narzędzi serwisowych oraz debugowania. Przedstawione poniżej czynności umożliwiają ograniczenie liczby użytkowników, którzy mogą mieć dostęp do komend śledzenia bez użycia uprawnień *SERVICE:

1. W programie iSeries Navigator otwórz Użytkownicy i grupy.
2. Aby wyświetlić listę profili użytkowników, wybierz Wszyscy użytkownicy.
3. Prawym przyciskiem myszy kliknij profil użytkownika, który ma być zmieniony.
4. Wybierz Właściwości.
5. Kliknij Możliwości.
6. Otwórz zakładkę Aplikacje.
7. Wybierz Dostęp do.
8. Zaznacz Aplikacje hosta.
9. Zaznacz System operacyjny.

10. Zaznacz Usługa.
11. Za pomocą pola wyboru nadaj lub odbierz dostęp do komendy śledzenia.

Uprawnienia specjalne *AUDIT

Uprawnienia specjalne kontroli (*AUDIT) dają użytkownikowi możliwość zmiany charakterystyk kontroli. Użytkownik może:

- zmienić wartości systemowe sterujące kontrolą,
- użyć komend CHGOBJAUT, CHGDLOAUD i CHGAUD, aby zmienić kontrolę dla obiektów,
- użyć komendy CHGUSRAUD, aby zmienić kontrolę dla użytkownika.

Ryzyko: Użytkownik z uprawnieniami specjalnymi *AUDIT może zatrzymać i uruchomić kontrolę systemu lub zapobiec kontrolowaniu poszczególnych działań. Jeśli posiadanie rekordów kontroli dla zdarzeń związanych z kontrolą jest ważne dla systemu, należy uważnie sterować i monitorować użycie uprawnień specjalnych *AUDIT.

Uwaga: Tylko użytkownik z uprawnieniami specjalnymi *ALLOBJ, *SECADM i *AUDIT może nadać innemu użytkownikowi uprawnienia *AUDIT.

Uprawnienia specjalne *IOSYSCFG

Uprawnienia specjalne konfiguracji systemu (*IOSYSCFG) dają użytkownikowi możliwość zmiany konfiguracji systemu. Na przykład możliwość dodawania lub usuwania informacji o konfiguracji komunikacji, pracy z serwerami TCP/IP oraz konfigurowania serwera do połączenia z siecią Internet. Większość komend do konfigurowania komunikacji wymaga uprawnień specjalnych *IOSYSCFG. Dodatek D pokazuje, jakie uprawnienia specjalne wymagane są dla poszczególnych komend.

Uwaga: Aby zmienić dane za pomocą funkcji serwisowych, wymagane są uprawnienia *ALLOBJ.

Zalecenia dla uprawnień specjalnych: Nadawanie uprawnień specjalnych użytkownikom stanowi ryzyko naruszenia ochrony. W przypadku każdego użytkownika należy uważnie sprawdzić potrzebę posiadania uprawnień specjalnych. Należy śledzić, którzy użytkownicy mają uprawnienia specjalne i okresowo przeglądać ich wymagania dotyczące uprawnień.

Dodatkowo należy kontrolować następujące sytuacje dla profili użytkowników i programów:

- czy profile użytkowników z uprawnieniami specjalnymi mogą być używane do wprowadzania zadań,
- czy programy tworzone przez tych użytkowników mogą uruchamiać się z uprawnieniami właściciela programu.

Programy adoptują uprawnienia specjalne *ALLOBJ właściciela, jeśli:

- programy są tworzone przez użytkowników mających uprawnienia specjalne *ALLOBJ,
- w komendzie tworzącej program użytkownik podał parametr USRPRF(*OWNER).

W jaki sposób program LAN Server korzysta z uprawnień specjalnych

Program licencjonowany LAN Server korzysta z uprawnień specjalnych profilu użytkownika, aby określić, jakie możliwości operatora użytkownik powinien mieć w środowisku serwera LAN. Poniżej przedstawiono możliwości operatora, jakie system daje użytkownikom serwera LAN:

***ALLOBJ**
Administrator systemu

***IOSYSCFG**
Uprawnienie operatora zasobu serwera

***JOBCTL**
Uprawnienie operatora urządzenia komunikacyjnego

***SECADM**
Uprawnienie operatora kont

***SPLCTL**
Uprawnienie operatora drukowania

- Uprawnienia specjalne *SAVSYS mają zastosowanie podczas składowania informacji w katalogu /QFPNWSSTG. Uprawnienia specjalne *SAVSYS nie mają zastosowania podczas składowania w katalogu /QLANSrv. Użytkownik musi wtedy mieć odpowiednie uprawnienia do obiektu lub uprawnienia administratora LAN.
- Uprawnienia specjalne *ALLOBJ dają wystarczające uprawnienia do składowania obiektów /QLANSrv oraz ich informacji o uprawnieniach, jeśli spełnione są następujące warunki:
  - użytkownik jest zdefiniowany w domenie LAN,
  - kontrolerem domeny jest procesor we/wy serwera plików w lokalnym systemie iSeries.

Środowisko specjalne

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
SPCENV

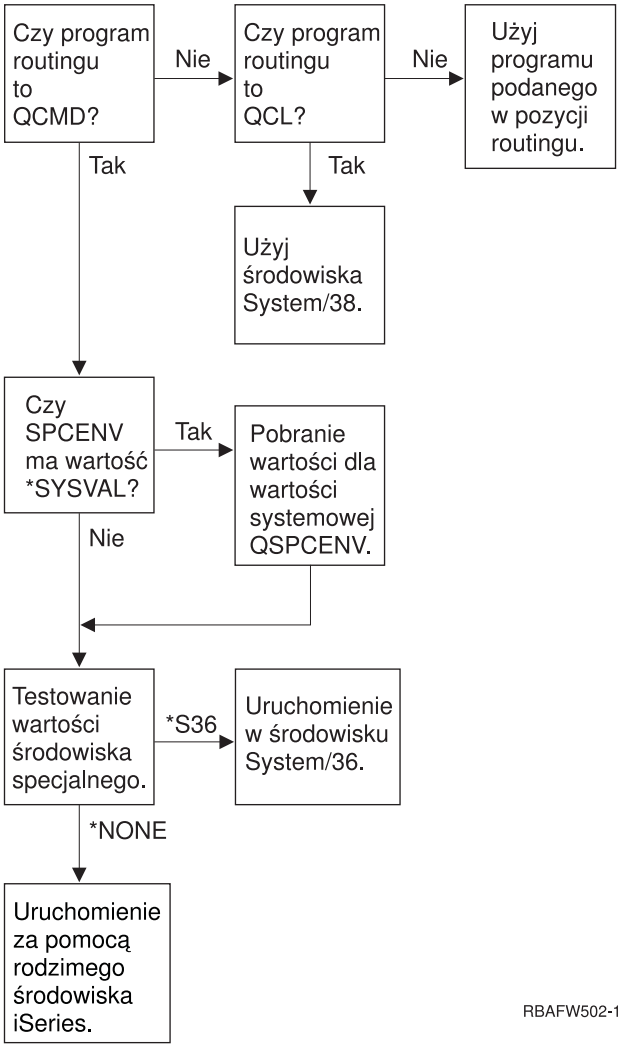
Długość:
10

Środowisko specjalne określa środowisko, w którym działa użytkownik po wpisaniu się. Użytkownik może działać w systemie iSeries, System/36 lub środowisku System/38. Gdy użytkownik wpisze się, system korzysta z programu routingu oraz parametru środowisko specjalne w profilu użytkownika, aby określić środowisko tego użytkownika. Patrz Rys. 2 na stronie 74.

Tabela 64. Możliwe wartości parametru SPCENV:

***SYSVAL**	Wartość systemowa QSPCENV używana jest do określenia środowiska, gdy użytkownik wpisuje się, a programem routingu użytkownika jest program QCMD.
***NONE**	Użytkownik działa w środowisku iSeries.
***S36**	Użytkownik działa w środowisku System/36, jeśli jego programem routingu jest program QCMD.

Zalecenia: Jeśli użytkownik uruchamia kombinację aplikacji systemu iSeries i System/36, przed uruchomieniem aplikacji systemu System/36 należy użyć komendy Uruchomienie System/36 (Start System/36 - STRS36), a nie podawać środowiska System/36 w profilu użytkownika. Zapewnia to lepszą wydajność aplikacji systemu iSeries.



Rysunek 2. Opis środowiska specjalnego

Opis środowiska specjalnego

Środowisko specjalne określa środowisko, w którym działa użytkownik po wpisaniu się. Użytkownik może działać w systemie iSeries, System/36 lub środowisku System/38. Gdy użytkownik wpisze się, system korzysta z programu routingu oraz parametru środowisko specjalne w profilu użytkownika, aby określić środowisko tego użytkownika. Przedstawiony poniżej opis dotyczy Rys. 2.

System określa, czy programem routingu jest program QCMD. Jeśli nie jest, wtedy system sprawdza, czy programem routingu jest program QCL. Jeśli jest to program QCL, system użyje środowiska specjalnego System/38. Jeśli programem routingu nie jest program QCL, system używa programu podanego w pozycji routingu.

Jeśli programem routingu jest program QCMD, system określa, czy wartość systemowa SPCENV jest ustawiona. Jeśli tak jest, system pobiera jej wartość oraz testuje wartość środowiska specjalnego. Jeśli wartość systemowa SPCENV nie jest ustawiona, system testuje wartość środowiska specjalnego.

Jeśli wartość środowiska specjalnego ustawiona jest na *S36, system uruchamia środowisko specjalne System/36. Jeśli wartość środowiska specjalnego ustawiona jest na wartość *NONE, system uruchamia rodzime środowisko iSeries.

Wyświetlenie informacji wpisania się

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
DSPSGNINF

Długość:
7

Pole *Wyświetlenie informacji wpisania się* określa, czy podczas wpisywania się wyświetlany jest ekran Informacje wpisania się (Sing-On Information). Rys. 3 opisuje ekran. Informacje o wygaśnięciu hasła wyświetlane są tylko wtedy, gdy do wygaśnięcia hasła zostało mniej niż siedem dni.

```
                    Informacje wpisania się
                     (Sign-on Information)
                                                          System:
Poprzednie wpisanie się  . . . . . :   10/30/91  14:15:00

Niepoprawne próby wpisania się . . . . . :   3

Do wygaśnięcia hasła pozostało dni . . . . :   5
```

Rysunek 3. Ekran Informacje wpisania się

Tabela 65. Możliwe wartości parametru DSPSGNINF:

***SYSVAL**	Zastosowana zostanie wartość systemowa QDSPSGNINF.
***NO**	Podczas wpisywania się użytkownika ekran Informacje wpisania się nie jest wyświetlany.
***YES**	Podczas wpisywania się użytkownika ekran Informacje wpisania się jest wyświetlany.

Zalecenia: Ekran Informacje wpisania się (Sing-On Information) jest narzędziem dla użytkowników do monitorowania swoich profili oraz do wykrywania próby niewłaściwego jego użycia. Zalecane jest ustawienie wyświetlania tego ekranu wszystkim użytkownikom. Użytkownicy z uprawnieniami specjalnymi lub uprawnieniami do krytycznych obiektów powinni używać tego ekranu do upewniania się, że nikt nie próbował używać ich profili.

Okres ważności hasła

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
PWDEXPITV

Długość:
5,0

Zobowiązanie użytkowników do zmiany hasła w określonym terminie zmniejsza ryzyko uzyskania dostępu do systemu przez osoby nieuprawnione. Okres ważności hasła steruje liczbą dni, przez które hasło może być używane, zanim trzeba będzie je zmienić.

Gdy hasło użytkownika wygaśnie, na ekranie wpisywania się otrzyma on komunikat. Użytkownik może nacisnąć klawisz Enter, aby podać nowe hasło lub klawisz F3 (Wyjście), aby anulować próbę wpisywania się bez podawania nowego hasła. Jeśli użytkownik wybierze zmianę hasła, wyświetlany jest ekran Zmiana hasła (Change Password), a dla nowego hasła przeprowadzane jest pełne sprawdzanie. Rys. 1 na stronie 62 pokazuje przykład komunikatu o utracie ważności hasła.

Zalecenia: Okresu ważności hasła należy używać do żądania częstszej zmiany hasła przez profile mające uprawnienia specjalne *SERVICE, *SAVSYS lub *ALLOBJ.

Tabela 66. Możliwe wartości parametru PWDEXPITV:

***SYSVAL**	Zastosowana zostanie wartość systemowa QPWDEXPITV.
***NOMAX**	System nie wymaga od użytkownika zmiany hasła.
okres_ważności_hasła	Należy podać liczbę z zakresu od 1 do 366.

Zalecenia: Wartość systemową QPWDEXPITV należy ustawić na odpowiedni okres, na przykład od 60 do 90 dni. Za pomocą pola *Okres ważności hasła* w profilu użytkownika dla pojedynczych użytkowników należy zmusić użytkowników, takich jak administratorzy ochrony, do częstszej zmiany hasła.

Lokalne zarządzanie hasłem

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
LCLPWDMGT

Długość:
4

Określa, czy hasło profilu użytkownika powinno być zarządzane lokalnie. Jeśli hasło zarządzane jest lokalnie, przechowywane jest razem z profilem użytkownika. Jest to tradycyjna metoda przechowywania hasła.

Jeśli hasło nie ma być zarządzane lokalnie, wtedy lokalne hasło systemu OS/400 ustawione jest na wartość *NONE. Wartość hasła określona w parametrze hasła zostanie wysłana do produktów IBM obsługujących synchronizację haseł, jak IBM iSeries Integration for Windows Server. Użytkownik nie będzie mógł zmienić swojego hasła za pomocą komendy Zmiana hasła (Change Password - CHGPWD). Dodatkowo nie będzie mógł bezpośrednio wpisać się do systemu. Określenie tej wartości wpłynie na inne produkty IBM obsługujące synchronizację haseł, jak IBM Integration for Windows Server. Szczegółowe informacje na ten temat zawiera dokumentacja produktu.

Ten parametr nie powinien mieć wartości *NO, chyba że użytkownik wymaga jedynie dostępu do systemu poprzez inną platformę, taką jak system Windows.

Tabela 67. Możliwe wartości parametru LCLPWDMGT:

***YES**	Hasło zarządzane jest lokalnie.
***NO**	Hasło nie jest zarządzane lokalnie.

Ograniczenie sesji urządzeń

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
LMTDEVSSN

Długość:
7

Pole *Ograniczenie sesji urządzeń* określa, czy użytkownik może być wpisany w tym samym czasie do więcej niż jednej stacji roboczej. Ta wartość nie ogranicza użycia menu System Request lub drugiego wpisywania się do tego samego urządzenia.

Tabela 68. Możliwe wartości parametru LMTDEVSSN:

***SYSVAL**	Zastosowana zostanie wartość systemowa QLMTDEVSSN.
***NO**	Użytkownik może być wpisany w tym samym czasie do więcej niż jednej stacji roboczej.
***YES**	Użytkownik nie może być wpisany w tym samym czasie do więcej niż jednej stacji roboczej.

Zalecenia: Ograniczanie użytkowników do jednej stacji roboczej jest jednym ze sposobów na zniechęcanie współużytkowania profili użytkowników. Wartość systemową QLMTDEVSSN należy ustawić na 1 (Tak). Jeśli niektórzy użytkownicy wymagają wpisywania się do wielu stacji roboczych, należy użyć pola *Ograniczenie sesji urządzeń* w ich profilach użytkowników.

Buforowanie klawiatury

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
KBDBUF

Długość:
10

Ten parametr określa wartość buforowania klawiatury, która używana jest podczas inicjowania zadania dla danego użytkownika. Nowa wartość zostanie zastosowana podczas następnego wpisywania się.

Pole buforowania klawiatury kontroluje dwie funkcje:

Pisanie z wyprzedzeniem:
Umożliwia użytkownikowi wpisywanie danych szybciej niż mogą być wysłane do systemu.

Buforowanie klawisza ATTN:
Jeśli buforowanie klawisza ATTN jest aktywne, to klawisz ten traktowany będzie jak inne klawisze. Jeśli buforowanie klawisza ATTN nie jest aktywne, to naciśnięcie tego klawisza spowoduje przesłanie informacji do systemu, nawet w przypadku, gdy istnieje zakaz przyjmowania danych ze stacji roboczej.

Tabela 69. Możliwe wartości parametru KBDBUF:

***SYSVAL**	Zastosowana zostanie wartość systemowa QKBDBUF.
***NO**	Opcja wpisywania z wyprzedzeniem oraz buforowanie klawisza ATTN nie będą aktywne dla danego profilu użytkownika.
***TYPEAHEAD**	Opcja wpisywania z wyprzedzeniem będzie aktywna dla danego profilu użytkownika.
***YES**	Opcja wpisywania z wyprzedzeniem oraz buforowanie klawisza ATTN będą aktywne dla danego profilu użytkownika.

Pamięć maksymalna

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
MAXSTG

Długość:
11,0

Istnieje możliwość podania maksymalnej ilości pamięci dyskowej, która będzie użyta do przechowywania stałych obiektów, których właścicielem jest profil użytkownika, w tym także obiektów umieszczanych w bibliotece tymczasowej (QTEMP) podczas wykonywania zadania. Pamięć maksymalna podawana jest w kilobajtach (1024 bajtów).

Jeśli podczas próby utworzenia obiektu potrzebna pamięć jest większa niż podana maksymalna ilość, obiekt nie zostanie utworzony.

Wartość pamięci maksymalnej jest stosowana niezależnie dla każdej niezależnej puli dyskowej (ASP) w systemie. Dlatego podanie wartości 5000 oznacza, że profil użytkownika może użyć następującej ilości pamięci:

- 5000 kB pamięci dyskowej z systemowej ASP i podstawowych pul ASP użytkownika,
- 5000 kB pamięci dyskowej z niezależnej puli ASP 00033 (jeśli istnieje),
- 5000 kB pamięci dyskowej z niezależnej puli ASP 00034 (jeśli istnieje),

Daje to 15 000 kB pamięci dyskowej z całego systemu.

Podczas planowania pamięci maksymalnej dla profilu użytkownika należy rozważyć następujące funkcje systemowe, które mogą wpływać na wymaganą przez użytkownika pamięć maksymalną:

- Operacja odtwarzania najpierw przydziela pamięć użytkownikowi przeprowadzającemu odtwarzanie, a następnie przenosi obiekty do biblioteki OWNER. Użytkownicy przeprowadzający duże operacje odtwarzania powinni mieć ustawioną wartość MAXSTG(*NOMAX).
- Profil użytkownika, który jest właścicielem dziennika, podczas jego rozrostu ma przydzielaną dodatkową pamięć. Jeśli tworzone są nowe dzienniki, pamięć jest przydzielana profilowi użytkownika, który jest właścicielem aktywnego dziennika. Użytkownicy, którzy są włścicielami aktywnych dzienników, powinni mieć ustawiony parametr MAXSTG(*NOMAX).
- Jeśli profil użytkownika ma parametr OWNER(*GRPPRF), prawo własności do tworzonych przez niego obiektów przenoszone jest na profil grupowy. Jednak użytkownik tworzący obiekt musi mieć odpowiednią ilość pamięci, aby pomieściła dowolny obiekt, zanim prawo własności zostanie przeniesione na profil grupowy.
- Właścicielowi biblioteki jest przypisywana pamięć dla opisów obiektów, które umieszczane są w bibliotece, nawet jeśli właścicielem obiektów jest inny profil użytkownika. Przykładami takich opisów są odniesienia do tekstu i programu.
- Pamięć przydzielana jest także dla obiektów tymczasowych, które używane są podczas przetwarzania zadania. Przykładem takich obiektów są bloki kontroli transakcji, przestrzenie edycji zbiorów oraz dokumenty.

Tabela 70. Możliwe wartości parametru MAXSTG:

***NOMAX**	Dla profilu przydzielona zostanie wymagana ilość pamięci.
maksimum- kB	Należy podać maksymalną ilość pamięci w kilobajtach (1 kilobajt równa się 1024 bajtów), która może być przypisana profilowi użytkownika.

Ograniczenie priorytetu

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
PTYLMT

Długość:
1

Zadanie wsadowe ma trzy różne wartości priorytetu:

Priorytet uruchamiania:
Określa w jaki sposób zadanie ubiega się o zasoby sprzętowe gdy jest uruchomione. Priorytet uruchamiania określony jest przez klasę zadania.

Priorytet zadania:
Określa priorytet harmonogramu dla każdego zadania wsadowego, gdy zadanie jest w kolejce zadań. Priorytet zadania może być ustawiony w opisie zadania lub w komendzie wprowadzania.

Priorytet wyjścia:
Określa priorytet harmonogramu dla wyjścia tworzonego przez zadanie w kolejce wyjściowej. Priorytet wyjścia może być ustawiony w opisie zadania lub w komendzie wprowadzania.

Ograniczenie priorytetu w profilu użytkownika określa maksymalne priorytety harmonogramu (priorytet zadania i wyjścia) dozwolone dla zadań, które wprowadza użytkownik. Kontroluje priorytet podczas wprowadzania zadania, a także wszelkie zmiany dokonywane podczas działania danego zadania lub jego oczekiwania w kolejce.

Ograniczenie priorytetu ogranicza także zmiany, które może przeprowadzić użytkownik z uprawnieniami specjalnymi *JOBCTL w zadaniu innego użytkownika. Nie można nadać innemu zadaniu użytkownika wyższego priorytetu, niż limit określony we własnym profilu użytkownika.

Jeśli zadanie wsadowe działa pod innym profilem użytkownika niż użytkownik wprowadzający zadanie, wtedy ograniczenia priorytetu dla zadania wsadowego określane są przez profil, pod którym zadanie jest uruchomione. Jeśli żądany priorytet harmonogramu wprowadzanego zadania jest wyższy niż ograniczenie priorytetu w profilu użytkownika, zostanie on zredukowany do poziomu, na który zezwala dany profil.

Tabela 71. Możliwe wartości parametru PTYLMT:

3	Domyślnym ograniczeniem priorytetu dla profili użytkowników jest poziom 3. Domyślnym priorytetem zarówno dla priorytetu zadania jak i priorytetu wyjścia dla opisu zadania jest poziom 5. Ustawienie ograniczenia priorytetu do poziomu 3 daje użytkownikowi możliwość przeniesienia niektórych zadań w kolejkach przed inne.
ograniczenie- priorytetu	Należy podać wartość od 1 do 9. Najwyższym priorytetem jest 1; najniższym - 9.

Zalecenia: używanie wartości priorytetu w opisach zadań i w komendach wprowadzania zadań jest często lepszym sposobem zarządzania użyciem zasobów systemowych niż zmienianie limitu priorytetu w profilach użytkowników.

Ograniczenia priorytetu należy używać w celu kontrolowania zmian, które użytkownicy mogą dokonać we wprowadzonych zadaniach. Na przykład operatorzy systemu mogą żądać wyższego ograniczenia priorytetu, aby mogli przenosić w kolejkach swoje zadania.

Opis zadania

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
JOBD

Długość:
10 (nazwa opisu zadania) 10 (nazwa biblioteki)

Uprawnienia:
*USE do opisu zadania, *READ i *EXECUTE do biblioteki

Gdy użytkownik wpisuje się, system sprawdza pozycję stacji roboczej w opisie podsystemu, aby określić jaki opis zadania ma być użyty dla zadania interaktywnego. Jeśli pozycja stacji roboczej określa wartość *USRPRF dla opisu zadania, używany jest opis zadania podany w profilu użytkownika.

Opis zadania dla zadania wsadowego jest podawany, gdy zadanie jest uruchamiane. Może to być jego nazwa lub opis zadania z profilu użytkownika, który uruchamia zadanie.

Opis zadania zawiera określony zestaw atrybutów związanych z zadaniem, takich jak kolejka zadania, która ma być użyta, harmonogram priorytetu, dane routingu, ważność kolejki komunikatów, lista bibliotek oraz informacje wyjściowe. Atrybuty określają, jak każde zadanie jest uruchamiane w systemie.

Więcej informacji dotyczących opisów zadań oraz ich użycia zawiera podręcznik *Zarządzanie pracą w systemie AS/400*.

Tabela 72. Możliwe wartości parametru JOBD:

QDFTJOBD	Używany jest opis zadania podany przez system z biblioteki QGPL. Aby sprawdzić atrybuty tego opisu zadania, można użyć komendy Wyświetlenie opisu zadania (Display Job Description - DSPJOBD).
nazwa_opisu_zadania	Należy podać nazwę opisu zadania (maksymalnie 10 znaków).

Tabela 73. Możliwe wartości dla biblioteki JOBD:

***LIBL**	Do odszukania opisu zadania użyta zostanie lista bibliotek.
***CURLIB**	Do odszukania opisu zadania użyta zostanie biblioteka domyślna dla zadania. Jeśli na liście bibliotek nie znajduje się biblioteka bieżąca, używana jest biblioteka QGPL.
nazwa_biblioteki	Należy podać bibliotekę, w której znajduje się opis zadania (maksymalnie 10 znaków).

Zalecenia: W przypadku zadań interaktywnych, opis zadania jest dobrym sposobem na kontrolowanie dostępu do biblioteki. Opis zadania można wykorzystać dla pojedynczych użytkowników, w celu określenia unikalnej listy bibliotek, zamiast korzystania z wartości systemowej QUSRLIBL.

Profil grupowy

Podpowiedź ekranu Dodanie użytkownika:
Grupa użytkowników

Parametr CL:
GRPPRF

Długość:
10

Uprawnienia:
Aby podczas tworzenia lub zmiany profilu użytkownika podać grupę, użytkownik musi mieć uprawnienia *OBJMGT, *OBJOPR, *READ, *ADD, *UPD i *DLT do danego profilu grupowego.

Uwaga:
Podczas sprawdzania uprawnień *OBJMGT do profilu grupowego nie są używane uprawnienia adoptowane. Więcej informacji na temat uprawnień adoptowanych zawiera sekcja “Obiekty, które adoptują uprawnienia właściciela” na stronie 128.

Podanie nazwy profilu grupowego powoduje, że użytkownik staje się członkiem tego profilu. Profil grupowy może zapewnić użytkownikowi uprawnienia do obiektów, do których dany użytkownik nie ma odpowiednich uprawnień. Dla każdego użytkownika, w parametrze *Dodatkowe profile grupowe* (SUPGRPPRF), można podać do 15 dodatkowych grup.

Gdy w profilu użytkownika podawany jest profil grupowy, taki użytkownik automatycznie otrzymuje uprawnienia *OBJMGT, *OBJOPR, *READ, *ADD, *UPD i *DLT do profilu grupowego, jeśli profil grupowy nie jest już jednym z profili grupowych użytkownika. Te uprawnienia są wymagane do wykonywania funkcji systemowych i nie powinny być usuwane.

Jeśli profil podany w parametrze GRPPRF nie jest jeszcze profilem grupowym, system ustawia informacje w takim profilu, oznaczające go jako profil grupowy. System generuje także identyfikator gid dla profilu grupowego, jeśli ten jeszcze takiego nie ma.

Więcej informacji na temat używania profili grupowych zawiera sekcja “Planowanie profili grupowych” na stronie 218.

Tabela 74. Możliwe wartości parametru GRPPRF:

***NONE**	Dla tego profilu użytkownika nie jest używany żaden profil grupowy.
nazwa-profilu-użytkownika	Należy podać nazwę profilu grupowego, którego członkiem jest dany profil użytkownika.

Właściciel

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
OWNER

Długość:
10

Jeśli użytkownik jest członkiem grupy, w jego profilu używany jest parametr *Właściciel*, umożliwiający określenie, kto ma być właścicielem nowych obiektów tworzonych przez tego użytkownika. Obiekty mogą należeć albo do użytkownika albo do jego grupy podstawowej (wartość parametru GRPPRF). Pole *Właściciel* może być wypełnione tylko wtedy, gdy wypełnione jest pole *Profil grupowy*.

Tabela 75. Możliwe wartości parametru OWNER:

***USRPRF**	Ten profil użytkownika jest właścicielem wszystkich tworzonych przez siebie obiektów.
***GRPPRF**	Właścicielem wszystkich obiektów tworzonych przez użytkownika jest profil grupowy. Ma on także nadawane uprawnienia *ALL do tych obiektów. Profil użytkownika nie ma nadawanych żadnych określonych uprawnień do nowo tworzonych obiektów. Jeśli podano parametr *GRPPRF, dla parametru GRPPRF trzeba podać nazwę profilu grupowego, a wartość parametru GRPAUT musi być równa *NONE. **Uwagi:** 1. Jeśli prawo własności zostanie nadane grupie, wszyscy członkowie grupy mogą zmieniać, zastępować i usuwać obiekt. 2. Parametr *GRPPRF jest ignorowany dla wszystkich systemów plików, z wyjątkiem systemu QSYS.LIB. W przypadkach, gdy ten parametr jest ignorowany, użytkownik zachowuje prawo własności do obiektu.

Uprawnienia grupowe

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
GRPAUT

Długość:
10

Jeśli profil użytkownika jest członkiem grupy i ma określony parametr OWNER(*USRPRF), pole *Uprawnienia grupowe* określa, jakie uprawnienia nadawane są profilowi grupowemu do obiektów utworzonych przez tego użytkownika.

Uprawnienia grupowe mogą być określone tylko wtedy, gdy parametr GRPPRF nie ma wartości *NONE, a OWNER ma wartość *USRPRF. Uprawnienia grupowe mają zastosowanie dla profilu podanego w parametrze GRPPRF. Nie mają zastosowania dla dodatkowych profili grupowych podanych w parametrze SUPGRPPRF.

Tabela 76. Możliwe wartości parametru GRPAUT:

***NONE**	Podczas tworzenia obiektu przez tego użytkownika, profilowi grupowemu nie są nadawane żadne uprawnienia.
***ALL**	Profil grupowy otrzymuje wszystkie uprawnienia do zarządzania oraz uprawnienia do danych do wszystkich obiektów, które tworzy użytkownik.
***CHANGE**	Profil grupowy otrzymuje uprawnienia do zmiany obiektów.
***USE**	Profil grupowy otrzymuje uprawnienia do przeglądania obiektów tworzonych przez użytkownika.
***EXCLUDE**	Profil grupowy ma wyraźnie odmówiony dostęp do wszystkich obiektów tworzonych przez użytkownika.

Pełne wyjaśnienie uprawnień, które mogą być nadane, zawiera sekcja “Definiowanie sposobu dostępu do informacji” na stronie 114.

Typ uprawnień grupowych

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
GRPAUTTYP

Długość:
10

Gdy użytkownik tworzy nowy obiekt, parametr *Typ uprawnień grupowych* w jego profilu określa, jaki typ uprawnień do tego obiektu otrzymuje grupa użytkownika. Parametr GRPAUTTYP współpracuje z parametrami OWNER, GRPPRF i GRPAUT, aby określić uprawnienia grupy do nowego obiektu.

Tabela 77. Możliwe wartości parametru GRPAUTTYP: [1]

***PRIVATE**	Uprawnienia zdefiniowane w parametrze GRPAUT przypisywane są profilowi grupowemu jako uprawnienia prywatne.
***PGP**	Profil grupowy zdefiniowany w parametrze GRPPRF jest grupą podstawową dla nowo tworzonych obiektów. Uprawnienia grupy podstawowej dla obiektu są uprawnieniami podanymi w parametrze GRPAUT.

[1] Uprawnienia prywatne i uprawnienia grupy podstawowej udostępniają ten sam sposób dostępu do obiektu, ale mają różne parametry wydajności. Sekcja “Grupa podstawowa dla obiektu” na stronie 123 wyjaśnia sposób działania uprawnień grupy podstawowej.

Zalecenia: Podanie wartości *PGP jest metodą na rozpoczęcie korzystania z uprawnień grupy podstawowej. Ustawienie GRPAUTTYP(*PGP) należy rozważyć dla użytkowników, którzy często tworzą nowe obiekty.

Grupy dodatkowe

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
SUPGRPPRF

Długość:
150

Uprawnienia:
Aby podczas tworzenia lub zmiany profilu użytkownika podać grupy dodatkowe, użytkownik musi mieć uprawnienia *OBJMGT, *OBJOPR, *READ, *ADD, *UPD i *DLT do danego profilu grupowego.

Uwaga:

Uprawnienia *OBJMGT nie mogą pochodzić z uprawnień grupowych. Więcej informacji na ten temat zawiera sekcja “Obiekty, które adoptują uprawnienia właściciela” na stronie 128.

Istnieje możliwość podania do 15 profili, z których dany użytkownik otrzyma uprawnienia. Użytkownik staje się członkiem każdego dodatkowego profilu grupowego. Użytkownik nie może mieć dodatkowych profili grupowych, jeśli parametr GRPPRF ma wartość *NONE.

Gdy w profilu użytkownika podawane są dodatkowe profile grupowe, taki użytkownik automatycznie otrzymuje uprawnienia *OBJMGT, *OBJOPR, *READ, *ADD, *UPD i *DLT do profilu grupowego, jeśli profil grupowy nie jest już jednym z profili grupowych użytkownika. Te uprawnienia są wymagane do wykonywania funkcji systemowych i nie powinny być usuwane. Jeśli profil podany w parametrze SUPGRPPRF nie jest jeszcze profilem grupowym, system ustawia informacje w takim profilu, oznaczające go jako profil grupowy. System generuje także identyfikator gid dla profilu grupowego, jeśli ten jeszcze takiego nie ma.

Więcej informacji na temat używania profili grupowych zawiera sekcja “Planowanie profili grupowych” na stronie 218.

Tabela 78. Możliwe wartości parametru SUPGRPPRF:

***NONE**	Z tym profilem użytkownika nie są używane żadne dodatkowe grupy.
nazwa_profilu_grupowego	Należy podać do 15 nazw profili grupowych, które mają być użyte z tym profilem użytkownika. Te profile, razem z profilem podanym w parametrze GRPPRF, używane są do nadania użytkownikowi dostępu do obiektów.

Kod rozliczeniowy

Podpowiedź ekranu Dodanie użytkownika:

Brak

Parametr CL:

ACGCDE

Długość:

15

Rozliczanie zadania jest funkcją opcjonalną, używaną do zbierania informacji o użyciu zasobów systemowych. Wartość systemowa poziomu rozliczania (QACGLVL) określa, czy rozliczanie zadania jest aktywne. Kod rozliczeniowy dla zadania pochodzi albo z opisu zadania, albo z profilu użytkownika. Kod rozliczeniowy może być podany także podczas uruchamiania zadania za pomocą komendy Zmiana kodu rozliczeniowego (Change Accounting Code - CHGACGCDE).

Więcej informacji na temat rozliczania zadań zawiera podręcznik *Zarządzanie pracą w systemie AS/400*.

Tabela 79. Możliwe wartości parametru ACGCDE:

***BLANK**	Profilowi użytkownika przypisywany jest kod rozliczeniowy składający się z 15 pustych znaków.
kod_rozliczeniowy	Należy podać 15 znaków kodu rozliczeniowego. Jeśli podano mniej niż 15 znaków, do łańcucha po prawej stronie dodawane są puste znaki.

Hasło do dokumentu

Podpowiedź ekranu Dodanie użytkownika:

Brak

Parametr CL:

DOCPWD

Długość:
8

Istnieje możliwość podania hasła do dokumentu, w celu zabezpieczenia dystrybucji poczty osobistej przed przeglądaniem przez osoby pracujące w imieniu użytkownika. Hasło do dokumentu obsługiwane jest przez niektóre produkty Document Interchange Architecture (DIA), takie jak Displaywriter.

Tabela 80. Możliwe wartości parametru DOCPWD:

***NONE**	Dla danego użytkownika nie jest używane hasło do dokumentów.
hasło_do_dokumentu	Należy podać hasło do dokumentu dla tego użytkownika. Hasło może składać się z od 1 do 8 znaków (liter od A do Z i cyfr od 0 do 9). Pierwszym znakiem tego hasła musi być litera alfabetu; pozostałe znaki mogą być alfanumeryczne. Nie są dozwolone spacje wewnętrzne, poprzedzające oraz znaki specjalne.

Kolejka komunikatów

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
MSGQ

Długość:
10 (nazwa kolejki komunikatów) 10 (nazwa biblioteki)

Uprawnienia:
*USE do kolejki komunikatów, jeśli istnieje; *EXECUTE do biblioteki kolejki komunikatów.

Dla użytkownika można podać nazwę kolejki komunikatów. **Kolejka komunikatów** jest obiektem, w którym umieszczane są komunikaty wysyłane do osoby lub programu. Kolejka komunikatów jest używana, gdy użytkownik wysyła lub otrzymuje komunikaty. Jeśli kolejka komunikatów nie istnieje, jest tworzona podczas tworzenia lub zmiany profilu. Właścicielem kolejki komunikatów jest dany profil użytkownika. Użytkownik tworzący profil ma do takiej kolejki komunikatów, ma uprawnienia *ALL.

Jeśli kolejka komunikatów dla profilu użytkownika zostanie zmieniona za pomocą komendy Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF), poprzednia kolejka nie jest automatycznie usuwana przez system.

Tabela 81. Możliwe wartości parametru MSGQ:

***USRPRF**	Jako kolejka komunikatów dla tego użytkownika używana będzie kolejka o takiej samej nazwie, jak nazwa profilu użytkownika. Jeśli kolejka komunikatów nie istnieje, zostanie utworzona w bibliotece QUSRSYS.
nazwa_kolejki_komunikatów	Należy podać nazwę kolejki komunikatów, która będzie używana dla tego użytkownika. Jeśli podana zostanie nazwa kolejki komunikatów, należy podać parametr biblioteki.

Tabela 82. Możliwe wartości dla biblioteki MSGQ:

***LIBL**	Do odszukania kolejki komunikatów używana jest lista bibliotek. Jeśli kolejka komunikatów nie istnieje, nie można podać parametru *LIBL.
***CURLIB**	Do odnalezienia kolejki komunikatów wykorzystywana jest bieżąca biblioteka zadania. Jeśli na liście bibliotek nie znajduje się biblioteka bieżąca, używana jest biblioteka QGPL. Jeśli kolejka komunikatów nie istnieje, zostanie utworzona w bibliotece bieżącej lub bibliotece QGPL.
nazwa_biblioteki	Należy podać bibliotekę, w której znajduje się kolejka komunikatów. Jeśli kolejka komunikatów nie istnieje, zostanie utworzona w tej bibliotece.

Zalecenia: Gdy użytkownik wpisuje się, kolejka komunikatów profilu użytkownika przydzielana jest do zadania tego użytkownika. Jeśli kolejka komunikatów jest już przydzielona do innego zadania, użytkownik otrzyma komunikat ostrzegawczy. Aby uniknąć takiej sytuacji, każdemu profilowi użytkownika należy przydzielić unikalną kolejkę komunikatów, najlepiej o takiej nazwie, jak nazwa profilu.

Dostarczenie

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
DLVRY

Długość:
10

Tryb dostarczenia kolejki komunikatów określa, czy użytkownik jest powiadamiany o nowym komunikacie w kolejce. Tryb dostarczenia podany w profilu użytkownika ma zastosowanie do osobistej kolejki komunikatów. Jeśli tryb dostarczenia dla kolejki komunikatów zostanie zmieniony, a użytkownik jest wpisany do systemu, zmiany zostaną uwzględnione podczas następnego wpisywania się. Parametr dostarczenia dla kolejki komunikatów można zmienić także za pomocą komendy Zmiana kolejki komunikatów (Change Message Queue - CHGMSGQ).

Tabela 83. Możliwe wartości parametru DLVRY:

***NOTIFY**	Zadanie, do którego przypisana jest kolejka komunikatów, powiadamiane jest w momencie nadejścia komunikatu. Dla zadań interaktywnych na stacjach roboczych słyszalny jest dźwięk i włącza się kontrolka komunikat-oczekujący. Rodzaj dostarczenia nie może być zmieniony na *NOTIFY, jeśli kolejka komunikatów jest używana także przez innego użytkownika.
***BREAK**	Zadanie, do którego przypisana jest kolejka komunikatów, jest przerywane w momencie nadejścia komunikatu. Jeśli jest to zadanie interaktywne słyszalny jest dźwięk (jeśli zainstalowany jest alarm). Rodzaj dostarczenia nie może być zmieniony na *BREAK, jeśli kolejka komunikatów jest używana także przez innego użytkownika.
***HOLD**	Komunikaty są przechowywane w kolejce komunikatów do czasu aż zostaną sprawdzone przez użytkownika lub program.
***DFT**	Na komunikaty wymagające odpowiedzi wysyłana jest odpowiedź domyślna; komunikaty informacyjne są ignorowane.

Ważność

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
SEV

Długość:
2,0

Jeśli kolejka komunikatów jest w trybie *BREAK lub *NOTIFY, kod ważności określa najniższy poziom komunikatów, które dostarczane są do użytkownika. Komunikaty, których ważność jest niższa niż podany kod ważności, są wstrzymywane w kolejce komunikatów, bez powiadamiania użytkownika.

Jeśli ważność dla kolejki komunikatów zostanie zmieniona, a użytkownik jest wpisany do systemu, zmiany zostaną uwzględnione podczas następnego wpisywania się. Parametr ważności dla kolejki komunikatów można zmienić także za pomocą komendy CHGMSGQ.

Tabela 84. Możliwe wartości parametru SEV:

00:	Jeśli nie podano kodu ważności, użyta zostanie wartość 00. Jeśli kolejka komunikatów jest w trybie *NOTIFY lub *BREAK, użytkownik powiadamiany jest o wszystkich komunikatach.
kod_ważności	Należy podać wartość od 00 do 99 dla najniższego poziomu ważności, który będzie powodował powiadamianie użytkownika. Można podać dowolną wartość dwucyfrową, nawet jeśli nie został dla niej zdefiniowany żaden kod ważności (zdefiniowany przez system lub przez użytkownika).

Drukarka

Podpowiedź ekranu Dodanie użytkownika:
Drukarka domyślna

Parametr CL:
PRTDEV

Długość:
10

Dla użytkownika można podać drukarkę, która ma być używana do drukowania zbiorów wyjściowych. Jeśli jako kolejka wyjściowa (OUTQ) podana zostanie drukarka (*DEV), zbiory buforowe umieszczane są w kolejce wyjściowej o takiej samej nazwie, jak drukarka.

Informacje o drukarce lub kolejce wyjściowej z profilu użytkownika używane są tylko wtedy, jeśli zbiór drukarkowy ma wartość *JOB, a opis zadania *USRPRF. Więcej informacji na temat kierowania zbiorów wydruku zawiera podręcznik *Printer Device Programming*.

Tabela 85. Możliwe wartości parametru PRTDEV:

***WRKSTN**	Używana jest drukarka przypisana do stacji roboczej użytkownika (w opisie urządzenia).
***SYSVAL**	Używana jest domyślna drukarka systemowa podana w wartości systemowej QPRTDEV.
nazwa_drukarki	Należy podać nazwę drukarki, która będzie używana do drukowania zbiorów wyjściowych danego użytkownika.

Kolejka wyjściowa

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
OUTQ

Długość:
10 (nazwa kolejki wyjściowej) 10 (nazwa biblioteki)

Uprawnienia:
*USE do kolejki wyjściowej, *EXECUTE do biblioteki

Zarówno przetwarzanie interaktywne, jak i przetwarzanie wsadowe może spowodować utworzenie zbiorów buforowych, które są wysyłane do drukarki. Zbiory buforowe umieszczane są w kolejce wyjściowej. W systemie może być wiele różnych kolejek wyjściowych. Kolejka wyjściowa nie musi być przyłączona do drukarki, aby otrzymywać nowe zbiory buforowe.

Informacje o drukarce lub kolejce wyjściowej z profilu użytkownika używane są tylko wtedy, jeśli zbiór drukarkowy ma wartość *JOB, a opis zadania *USRPRF. Więcej informacji na temat kierowania zbiorów wydruku zawiera

podręcznik *Printer Device Programming*.

Tabela 86. Możliwe wartości parametru OUTQ:

***WRKSTN**	Używana jest kolejka wyjściowa przypisana do stacji roboczej użytkownika (w opisie urządzenia).
***DEV**	Używana jest kolejka wyjściowa o takiej samej nazwie, jak drukarka podana w parametrze PRTDEV.
nazwa_kolejki_wyjściowej	Należy podać nazwę kolejki wyjściowej, która ma być użyta. Kolejka wyjściowa musi istnieć. Jeśli podano kolejkę wyjściową, należy podać także bibliotekę.

Tabela 87. Możliwe wartości dla biblioteki OUTQ:

***LIBL**	Do odszukania kolejki wyjściowej używana jest lista bibliotek.
***CURLIB**	Do odnalezienia kolejki wyjściowej wykorzystywana jest bieżąca biblioteka zadania. Jeśli na liście bibliotek nie znajduje się biblioteka bieżąca, używana jest biblioteka QGPL.
nazwa_biblioteki	Należy podać bibliotekę, w ktorej znajduje się kolejka wyjściowa.

Program obsługi klawisza ATTN

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
ATNPGM

Długość:
10 (nazwa programu) 10 (nazwa biblioteki)

Uprawnienia:
*USE do programu

*EXECUTE do biblioteki

Program obsługi klawisza ATTN (ATNPGM) jest programem, który jest wywoływany, gdy podczas działania zadania interaktywnego użytkownik naciska klawisz ATTN.

Program ATNPGM aktywowany jest tylko wtedy, jeśli programem routingu użytkownika jest program QCMD. Program ATNPGM aktywowany jest przed wywołaniem programu początkowego. Jeśli program początkowy zmienia program ATNPGM, nowy program ATNPGM pozostaje aktywny tylko przez czas działania programu początkowego. Jeśli z poziomu wiersza komend lub w aplikacji uruchamiana jest komenda Ustawienie programu Attention (Set Attention-Key-Handling Program - SETATNPGM), podany nowy program ATNPGM przesłania program ATNPGM z profilu użytkownika.

Uwaga: Więcej informacji na temat przetwarzania sekwencji wpisywania się użytkownika zawiera sekcja “Uruchamianie zadania interaktywnego” na stronie 179.

Pole *Ograniczenie możliwości* określa, czy użytkownik może za pomocą komendy Zmiana profilu (Change Profile - CHGPRF) podać inny program obsługi klawisza ATTN.

Tabela 88. Możliwe wartości parametru ATNPGM:

***SYSVAL**	Użyta zostanie wartość systemowa QATNPGM.
***NONE**	Przez tego użytkownika nie jest używany żaden program obsługi klawisza ATTN.
***ASSIST**	Użyty zostanie program klawisza ATTN Asysty Operacyjnej (QEZMAIN).
nazwa_programu	Należy podać nazwę programu obsługi klawisza ATTN. Jeśli podana zostanie nazwa programu, należy podać także bibliotekę.

Tabela 89. Możliwe wartości dla biblioteki ATNPGM:

***LIBL**	Do odnalezienia programu obsługi klawisza ATTN używana jest lista bibliotek.
***CURLIB**	Do odnalezienia programu obsługi klawisza ATTN wykorzystywana jest bieżąca biblioteka zadania. Jeśli na liście bibliotek nie znajduje się biblioteka bieżąca, używana jest biblioteka QGPL.
nazwa_biblioteki	Należy podać bibliotekę, w której znajduje się program obsługi klawisza ATTN.

Kolejność sortowania

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
SRTSEQ

Długość:
10 (wartość lub nazwa tabeli) 10 (nazwa biblioteki)

Uprawnienia:
*USE do tabeli, *EXECUTE do biblioteki

Istnieje możliwość podania kolejności sortowania, która ma być używana dla zbiorów wyjściowych danego użytkownika. Można użyć tabel sortowania udostępnianych przez system lub utworzyć własne. Tabela sortowania może być związana z identyfikatorem języka w systemie.

Tabela 90. Możliwe wartości parametru SRTSEQ:

***SYSVAL**	Zastosowana zostanie wartość systemowa QSRTSEQ.
***HEX**	Dla tego użytkownika zastosowana zostanie standardowa szesnastkowa kolejność sortowania.
***LANGIDSHR**	Użyta zostanie tabela kolejności sortowania związana z identyfikatorem języka użytkownika. Tabela może zawierać taką samą wagę dla wielu znaków.
***LANGIDUNQ**	Użyta zostanie tabela kolejności sortowania związana z identyfikatorem języka użytkownika. Tabela musi zawierać unikalne wagi dla każdego znaku ze strony kodowej.
nazwa_tabeli	Należy podać nazwę tabeli kolejności sortowania.

Tabela 91. Możliwe wartości dla biblioteki SRTSEQ:

***LIBL**	Do odszukania tabeli podanej dla wartości SRTSEQ używana jest lista bibliotek.
***CURLIB**	Do odszukania tabeli podanej dla wartości SRTSEQ używana jest biblioteka bieżąca. Jeśli na liście bibliotek nie znajduje się biblioteka bieżąca, używana jest biblioteka QGPL.
nazwa_biblioteki	Należy podać bibliotekę, w której znajduje się tabela kolejności sortowania.

Identyfikator języka

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
LANGID

Długość:
10

Dla użytkownika można podać identyfikator języka, który będzie używany przez system. Aby sprawdzić listę identyfikatorów języków, na ekranie Tworzenie profilu użytkownika (Create User Profile) lub Zmiana profilu użytkownika (Change User Profile) dla parametru identyfikator języka, należy nacisnąć klawisz F4 (podpowiedź).

Tabela 92. Możliwe wartości parametru LANGID:

***SYSVAL:**	Do określania identyfikatora języka używana jest wartość systemowa QLANGID.
identyfikator_języka	Należy podać identyfikator języka.

Identyfikator kraju lub regionu

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
CNTRYID

Długość:
10

Dla użytkownika można podać identyfikator kraju lub regionu, który będzie używany przez system. Aby sprawdzić listę identyfikatorów krajów lub regionów, na ekranie Tworzenie profilu użytkownika (Create User Profile) lub Zmiana profilu użytkownika (Change User Profile) dla parametru identyfikator kraju lub regionu, należy nacisnąć klawisz F4 (podpowiedź).

Tabela 93. Możliwe wartości parametru CNTRYID:

***SYSVAL**	Do określania identyfikatora kraju lub regionu używana jest wartość systemowa QCNTRYID.
identyfikator_kraju_lub_regionu	Należy podać identyfikator kraju lub regionu.

Identyfikator kodowanego zestawu znaków (CCSID)

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
Identyfikator CCSID

Długość:
5,0

Dla użytkownika można podać identyfikator kodowanego zestawu znaków, który będzie używany przez system. Aby sprawdzić listę identyfikatorów kodowanego zestawu znaków, na ekranie Tworzenie profilu użytkownika (Create User Profile) lub Zmiana profilu użytkownika (Change User Profile) dla parametru identyfikator kodowanego zestawu znaków, należy nacisnąć klawisz F4 (podpowiedź).

Tabela 94. Możliwe wartości parametru CCSID:

***SYSVAL**	Do określenia identyfikatora kodowanego zestawu znaków używana jest wartość systemowa QCCSID.
identyfikator_kodowanego_zestawu_znaków	Należy podać identyfikator kodowanego zestawu znaków.

Sterowanie identyfikatorem znaku

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
CHRIDCTL

Długość:
10

Atrybut *CHRIDCTL* steruje typem konwersji kodowanego zestawu znaków, która występuje dla zbiorów ekranowych, zbiorów drukarkowych i paneli grupowych. Informacje o sterowaniu identyfikatorem znaku z profilu użytkownika używane są tylko wtedy, gdy dla parametru CHRID komend tworzenia, zmiany lub zastępowania zbiorów ekranowych, drukarkowych i paneli grupowych podana jest wartość specjalna *CHRIDCTL.

Tabela 95. Możliwe wartości parametru CHRIDCTL:

***SYSVAL**	Do określania sterowania identyfikatorem znaku używana jest wartość systemowa QCHRIDCTL.
***DEVD**	Do reprezentowania identyfikatora CCSID danych używany jest parametr CHRID urządzenia. Nie występuje żadna konwersja, gdyż identyfikator CCSID danych zawsze jest taki sam jak parametr CHRID urządzenia.
***JOBCCSID**	Konwersja znaku występuje, gdy między parametrem CHRID urządzenia, identyfikatorem CCSID zadania lub wartościami CCSID danych występują różnice. Na wejściu, jeśli jest to konieczne, dane znakowe są przekształcane z CHRID urządzenia do identyfikatora CCSID zadania. Na wyjściu, jeśli jest to konieczne, dane znakowe są przekształcane z identyfikatora CCSID zadania na CHRID urządzenia. Na wyjściu, jeśli jest to konieczne, dane znakowe są przekształcane z identyfikatora CCSID zbioru lub panelu grupowego na CHRID urządzenia.

Atrybuty zadania

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
SETJOBATR

Długość:
160

Pole *SETJOBATR* określa, które atrybuty zadania pobierane są podczas inicjalizacji zadania z ustawień narodowych w parametrze LOCALE.

Tabela 96. Możliwe wartości parametru SETJOBATR:

***SYSVAL**	Do określenia które atrybuty zadania mają być pobrane z ustawień narodowych używana jest wartość systemowa QSETJOBATR.
***NONE**	Z ustawień narodowych nie są pobierane żadne atrybuty.
	Można podać kombinację następujących wartości:
***CCSID**	Użyty zostanie identyfikator kodowanego zestawu znaków z ustawień narodowych. Wartość CCSID z ustawień narodowych przesłoni CCSID profilu użytkownika.
***DATFMT**	Użyty zostanie format daty z ustawień narodowych.
***DATSEP**	Użyty zostanie separator daty z ustawień narodowych.
***DECFMT**	Użyty zostanie format dziesiętny z ustawień narodowych.
***SRTSEQ**	Użyta zostanie kolejność sortowania z ustawień narodowych. Kolejność sortowania z ustawień narodowych przesłoni kolejność sortowania profilu użytkownika.
***TIMSEP**	Użyty zostanie separator godziny z ustawień narodowych.

Ustawienia narodowe

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
LOCALE

Długość:
2048

Pole *LOCALE* określa nazwę ścieżki ustawień narodowych, które przypisane są zmiennej środowiskowej LANG dla danego użytkownika.

Tabela 97. Możliwe wartości parametru LOCALE:

***SYSVAL**	Do określenia nazwy ścieżki ustawień narodowych, która przypisana jest danemu użytkownikowi, użyta zostanie wartość systemowa QLOCALE.
***NONE**	Danemu użytkownikowi nie są przypisywane żadne ustawienia narodowe.
***C**	Danemu użytkownikowi przypisywane są ustawienia narodowe C.
***POSIX**	Danemu użytkownikowi przypisywane są ustawienia narodowe POSIX.
nazwa_ścieżki_do_ustawień_narodowych	Nazwa ścieżki ustawień narodowych, które mają być przypisane danemu użytkownikowi.

Opcje użytkownika

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
USROPT

Długość:
240 (10 znaków każda)

Pole *Opcje użytkownika* umożliwia dostosowanie pewnych ekranów systemowych oraz funkcji do użytkownika. Dla parametru opcji użytkownika można podać wiele wartości.

Tabela 98. Możliwe wartości parametru USROPT:

***NONE**	Dla użytkownika nie są używane żadne opcje specjalne. Użyty zostanie standardowy interfejs systemowy.
***CLKWD**	Zamiast wartości parametrów, podczas wyświetlania podpowiedzi komend CL, pokazywane są słowa kluczowe. Jest to równoznaczne z naciśnięciem klawisza F11 na zwykłym ekranie podpowiedzi komendy CL.
***EXPERT**	Gdy użytkownik przegląda ekrany wyświetlające uprawnienia do obiektów, na przykład Edycja uprawnień dla obiektu (Edit Object Authority) lub Edycja listy autoryzacji (Edit Authorization List), szczegółowe informacje o uprawnieniach wyświetlane są bez konieczności naciskania klawisza F11 (Szczegóły ekranu). W sekcji “Ekrany uprawnień” na stronie 133 przedstawiono przykład ekranu w wersji dla eksperta.
***HLPFULL**	Zamiast okna użytkownik widzi informacje pomocy pełnoekranowej.
***PRTMSG**	Gdy zbiór buforowy jest drukowany, do kolejki komunikatów użytkownika wysyłany jest komunikat.
***ROLLKEY**	Działanie klawiszy Page Up i Page Down zostaje odwrócone.
***NOSTSMSG**	Komunikaty o statusie najczęściej wyświetlane w dolnej części ekranu nie są widoczne dla użytkownika.
***STSMSG**	Komunikaty o statusie wyświetlane są podczas wysyłania do użytkownika.

Numer identyfikacyjny użytkownika

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
UID

Długość:
10,0

zintegrowany system plików korzysta z numeru identyfikacyjnego użytkownika (uid) do identyfikowania użytkownika oraz sprawdzania jego uprawnień. Każdy użytkownik w systemie ma unikalny uid.

Tabela 99. Możliwe wartości parametru UID:

***GEN**	Dla danego użytkownika system generuje unikalny uid. Wygenerowany uid będzie większy niż 100.
uid	Wartość od 1 do 4294967294, która ma być użyta jako uid dla tego użytkownika. uid nie może być już przypisany innemu użytkownikowi.

Zalecenia: W przypadku większości instalacji należy podać parametr UID(*GEN) i generowanie uid pozostawić systemowi. Jednak jeśli system jest częścią sieci, może istnieć konieczność przypisywania uid, które są zgodne z tymi w pozostałych systemach. W tym celu należy skonsultować się z administratorem sieci.

Numer identyfikacyjny grupy

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
GID

Długość:
10,0

Do identyfikowania tych profili, które są profilami grupowymi, zintegrowany system plików używa numeru identyfikacyjnego grupy (gid). Profil używany przez zintegrowany system plików jako profil grupowy musi mieć gid.

Tabela 100. Możliwe wartości parametru GID:

***NONE**	Dany profil nie ma gid.
***GEN**	Dla danego profilu system generuje unikalny gid. Wygenerowany gid będzie większy niż 100.
gid	Wartość od 1 do 4294967294, która ma być użyta jako gid dla tego profilu. gid nie może być już przypisany innemu profilowi.

Zalecenia: W przypadku większości instalacji należy podać parametr GID(*GEN) i generowanie gid pozostawić systemowi. Jednak jeśli system jest częścią sieci, może istnieć konieczność przypisywania gid, które są zgodne z tymi w pozostałych systemach. W tym celu należy skonsultować się z administratorem sieci.

Nie należy przypisywać gid profilowi użytkownika, który nie ma być profilem grupowym. W niektórych środowiskach użytkownik, który jest wpisany i ma gid, ma ograniczone wykonywanie niektórych funkcji.

Katalog osobisty

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
HOMEDIR

Długość:
2048

Katalog osobisty jest początkowym katalogiem roboczym użytkownika dla zintegrowany system plików. Katalog osobisty jest katalogiem bieżącym użytkownika, jeśli nie podano innego katalogu bieżącego. Jeśli katalog osobisty podany w profilu użytkownika nie istnieje, gdy użytkownik się wpisuje, katalogiem osobistym użytkownika będzie katalog główny (/).

Tabela 101. Możliwe wartości parametru HOMEDIR:

***USRPRF**	Katalogiem osobistym użytkownika jest katalog /home/xxxxx, gdzie xxxxx to nazwa profilu użytkownika.
katalog_osobisty	Nazwa katalogu osobistego dla użytkownika.

Powiązanie EIM

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
EIMASSOC

Długość:
128

Określa, czy dla danego użytkownika należy dodać powiązanie EIM (Enterprise Identity Mapping) do identyfikatora EIM. Opcjonalnie, jeśli identyfikator EIM jeszcze nie istnieje, to zostanie utworzony.

Uwaga:

1. Te informacje nie są przechowywane w profilu użytkownika. Nie są składowane i odtwarzane razem z profilem użytkownika.
2. Jeśli system nie jest skonfigurowany dla powiązań EIM, wtedy przetwarzanie nie jest wykonywane. Brak możliwości wykonywania operacji EIM nie powoduje niepowodzenia w wykonywaniu komendy.

Tabela 102. Możliwe wartości parametru EIMASSOC:

Pojedyncze wartości

***NOCHG**	Powiązania EIM nie będą dodawane.

Tabela 103. Możliwe wartości dla parametru EIMASSOC, Element 1:

Element 1: Identyfikator EIM

Określa identyfikator EIM dla danego powiązania.

***USRPRF**	Nazwa identyfikatora EIM jest taka sama, jak nazwa profilu użytkownika.
wartość_znakowa	Określa nazwę identyfikatora EIM.

Tabela 104. Możliwe wartości dla parametru EIMASSOC, Element 2:

Element 2: Typ powiązania

Określa typ powiązania. Zalecane jest, aby dla użytkownika systemu OS/400 było dodawane powiązanie docelowe.

Powiązania docelowe używane są przede wszystkim do zabezpieczania istniejących danych. Są one rezultatem operacji odwzorowywania wyszukiwania (na przykład eimGetTargetFromSource()), ale nie mogą być używane jako tożsamość źródłowa dla operacji odwzorowywania wyszukiwania.

Powiązania źródłowe używane są przede wszystkim w celu uwierzytelnienia. Mogą być użyte jako tożsamość źródłowa operacji odwzorowywania wyszukiwania, ale nie mogą być tożsamościami docelowymi dla tej operacji.

Powiązania administracyjne używane są do pokazywania, że tożsamość powiązana jest z identyfikatorem EIM, ale nie mogą być używane jako źródłowe i docelowe dla operacji odwzorowywania wyszukiwania.

***TARGET**	Przetwarzanie powiązania docelowego.
***SOURCE**	Przetwarzanie powiązania źródłowego.
***TGTSRC**	Przetwarzanie powiązań źródłowych i docelowych.
***ADMIN**	Przetwarzanie powiązania administracyjnego.
***ALL**	Przetwarzanie wszystkich rodzajów powiązań.

Tabela 105. Możliwe wartości dla parametru EIMASSOC, Element 3:

Element 3: Działanie powiązania

***REPLACE**	Powiązania podanego rodzaju zostaną usunięte ze wszystkich identyfikatorów EIM, które mają powiązanie dla danego profilu użytkownika oraz lokalnego rejestru EIM. Nowe powiązanie zostanie dodane do określonego identyfikatora EIM.
***ADD**	Dodanie powiązania.
***REMOVE**	Usunięcie powiązania.

Tabela 106. Możliwe wartości dla parametru EIMASSOC, Element 4:

Element 4: Tworzenie identyfikatora EIM

Określa, czy identyfikator EIM ma być utworzony, jeśli nie istnieje.

***NOCRTEIMID**	Identyfikator EIM nie jest tworzony.
***CRTEIMID**	Identyfikator EIM jest tworzony, jeśli nie istnieje.

Uprawnienia

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
AUT

Długość:
10

Pole *Uprawnienia* określa uprawnienia publiczne do profilu użytkownika. Uprawnienia do profilu sterują wieloma funkcjami związanymi z profilem, takimi jak:

zmienianie profilu,

wyświetlanie,

usuwanie,

wprowadzanie za jego pomocą zadania,

określanie go w opisie zadania,

przenoszenie na niego prawa własności do obiektu,

dodawanie członków, jeśli jest to profil grupowy.

Tabela 107. Możliwe wartości parametru AUT:

***EXCLUDE**	Użytkownicy publiczni mają wyraźnie odmówiony dostęp do tego profilu użytkownika.
***ALL**	Użytkownicy publiczni mają nadane wszystkie uprawnienia do zarządzania i do danych.
***CHANGE**	Użytkownicy publiczni mają nadane uprawnienia do zmiany profilu użytkownika.
***USE**	Użytkownicy publiczni mają uprawnienia do przeglądania profilu.

Pełne wyjaśnienie uprawnień, które mogą być nadane, zawiera sekcja “Definiowanie sposobu dostępu do informacji” na stronie 114.

Zalecenia: Aby zapobiec nieprawidłowemu użyciu profili użytkowników, które mają uprawnienia do obiektów krytycznych, należy upewnić się, że uprawnienia publiczne do nich mają wartość *EXCLUDE. Nieprawidłowe użycie profilu to na przykład wprowadzanie zadania, które uruchamiane jest pod tym profilem lub zmienianie programu, który adoptuje uprawnienia takiego profilu.

Kontrolowanie obiektu

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
OBJAUD

Długość:
10

Wartość kontrolowania obiektu dla profilu użytkownika współpracuje z wartością kontrolowania obiektu dla obiektu, w celu określenia, czy użytkownik ma dostęp do kontrolowanego obiektu. Kontrolowanie obiektu dla profilu użytkownika nie może być określone na żadnym z ekranów profilu. Aby określić kontrolowanie obiektu dla użytkownika, należy użyć komendy CHGUSRAUD. Komendy CHGUSRAUD może użyć tylko użytkownik z uprawnieniami specjalnymi *AUDIT.

Tabela 108. Możliwe wartości parametru OBJAUD:

***NONE**	Wartość parametru OBJAUD decyduje, czy dla danego użytkownika wykonywane jest kontrolowanie obiektu.
***CHANGE**	Jeśli wartość parametru OBJAUD dla obiektu jest równa *USRPRF, rekord kontroli jest zapisywany, gdy dany użytkownik zmienia obiekt.
***ALL**	Jeśli wartość parametru OBJAUD dla obiektu jest równa *USRPRF, rekord kontroli jest zapisywany, gdy dany użytkownik zmienia lub odczytuje obiekt.

Tabela 109 pokazuje, w jaki sposób współpracują ze sobą wartości parametrów OBJAUD dla użytkownika i dla obiektu:

Tabela 109. Kontrola przeprowadzana dla dostępu do obiektu

Wartość OBJAUD dla obiektu	**Wartość OBJAUD dla użytkownika**		
	***NONE**	***CHANGE**	***ALL**
*NONE	Brak	Brak	Brak
*USRPRF	Brak	Zmiana	Zmiana i użycie
*CHANGE	Zmiana	Zmiana	Zmiana
*ALL	Zmiana i użycie	Zmiana i użycie	Zmiana i użycie

Sekcja “Planowanie kontroli dostępu do obiektu” na stronie 256 udostępnia informacje dotyczące sposobu użycia wartości systemowych oraz wartości kontrolowania obiektu dla użytkowników i obiektów tak, aby spełniały wymagania ochrony.

Kontrolowanie działania

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
AUDLVL

Długość:
640

Dla pojedynczego użytkownika można określić, które działania związane z ochroną mają być zapisywane w kronice kontroli. Działania określone dla pojedynczego użytkownika są kontrolowane oprócz działań określonych dla wszystkich użytkowników w wartościach systemowych QAUDLVL i QAUDLVL2. Kontrolowanie działań dla profilu użytkownika nie może być określone na żadnym z ekranów profilu. Definiowane jest za pomocą komendy CHGUSRAUD. Komendy CHGUSRAUD może użyć tylko użytkownik z uprawnieniami specjalnymi *AUDIT.

Tabela 110. Możliwe wartości parametru AUDLVL:

***NONE**	Kontrolą działania steruje wartość systemowa QAUDLVL. Nie jest przeprowadzane żadne dodatkowe kontrolowanie.
***CMD**	Protokołowane są łańcuchy komend. Wartość *****CMD może być określona tylko dla pojedynczego użytkownika. Kontrolowanie łańcucha komendy nie jest dostępne jako opcja dla całego systemu dla wartości systemowej QAUDLVL.
***CREATE**	Protokołowane są operacje tworzenia obiektu.
***DELETE**	Protokołowane są operacje usunięcia obiektu.
***JOBDTA**	Protokołowane są zmiany zadania.
***OBJMGT**	Protokołowane są operacje przenoszenia i zmiany nazwy obiektu.
***OFCSRV**	Protokołowane są zmiany katalogu dystrybucyjnego systemu oraz działania poczty.
***PGMADP**	Protokołowane jest uzyskiwanie uprawnień do obiektu z programów, które adoptują uprawnienia.
***SAVRST**	Protokołowane są operacje składowania i odtwarzania.
***SECURITY**	Protokołowane są funkcje związane z ochroną.
***SERVICE**	Protokołowane jest użycie narzędzi serwisowych.
***SPLFDTA**	Protokołowane są działania wykonywane na zbiorach buforowych.
***SYSMGT**	Użycie funkcji zarządzania systemem jest protokołowane.

Sekcja “Planowanie kontroli działania” na stronie 238 udostępnia informacje dotyczące sposobu użycia wartości systemowych oraz wartości kontrolowania działań użytkowników tak, aby spełniały wymagania ochrony.

Informacje dodatkowe związane z profilem użytkownika

Poprzednie sekcje opisywały pola, które podawane są podczas tworzenia i zmiany profili użytkowników. Pozostałe informacje związane są z profilem użytkownika w systemie oraz składowane razem z nim. Są to:

- Uprawnienia prywatne
- informacje o posiadanych obiektach,
- informacje o grupie podstawowej.

Ilość tych informacji wpływa na czas składowania i odtwarzania profilu oraz budowania ekranów uprawnień. Informacje dotyczące składowania i odtwarzania profili użytkowników zawiera sekcja “Jak przechowywane są informacje o ochronie” na stronie 224.

Uprawnienia prywatne

Wszystkie uprawnienia prywatne, które ma użytkownik, składowane są razem z jego profilem. Gdy użytkownik potrzebuje uprawnień do obiektu, przeszukiwane mogą być jego uprawnienia prywatne. Więcej informacji na temat sprawdzania uprawnień zawiera sekcja “Schemat blokowy 3: Jak sprawdzane są uprawnienia użytkownika do obiektu” na stronie 154.

Uprawnienia prywatne użytkownika można wyświetlić za pomocą komendy Wyświetlenie profilu użytkownika (Display User Profile): DSPUSRPRF *nazwa_profilu_użytkownika* TYPE(*OBJAUT). Aby zmienić uprawnienia prywatne użytkownika, należy użyć komend, które pracują z uprawnieniami do obiektów, na przykład Edycja uprawnień dla obiektu (Edit Object Authority - EDTOBJAUT).

Za pomocą komendy Nadanie uprawnień użytkownika (Grant User Authority - GRTUSRAUT) można skopiować wszystkie uprawnienia prywatne jednego użytkownika do innego. Więcej informacji na ten temat zawiera sekcja “Kopiowanie uprawnień innego użytkownika” na stronie 146.

Uprawnienia grupy podstawowej

Nazwy wszystkich obiektów, dla których profil jest grupą podstawową, składowane są razem z profilem grupowym. Obiekty, dla których profil jest grupą podstawową, można wyświetlić za pomocą komendy DSPUSRPRF: DSPUSRPRF *nazwa_profilu_grupowego* TYPE(*OBJPGP). W tym celu można także użyć komendy Praca z obiektami według grupy podstawowej (Work with Objects by Primary Group - WRKOBJPGP).

Informacje o posiadanych obiektach

Informacje o uprawnieniach prywatnych do obiektu składowane są razem z profilem użytkownika, który jest właścicielem obiektu. Te informacje używane są do budowania ekranów systemu, które pracują z uprawnieniami do obiektu. Jeśli profil jest właścicielem dużej liczby obiektów, które mają dużo uprawnień prywatnych, może to wpływać na wydajność tworzenia ekranów uprawnień do obiektów. Wielkość profilu wpływa na szybkość wyświetlania uprawnień do obiektów i pracy z tymi uprawnieniami, a także składowania i odzyskiwania profili. Może to mieć także wpływ na wydajność całego systemu. Aby temu zapobiec, należy rozdzielić prawa własności między wiele profili. Ponieważ wielkość profilu użytkownika może wpłynąć na wydajność, zaleca się nie przypisywać wszystkich (lub prawie wszystkich) obiektów do tylko jednego profilu będącego właścicielem.

Uwierzytelnianie za pomocą podpisu (ID) cyfrowego

Infrastruktura ochrony systemu iSeries do identyfikowania umożliwia używanie certyfikatów cyfrowych x.509. Certyfikaty cyfrowe umożliwiają użytkownikom zabezpieczanie komunikacji i zapewnianie integralności komunikatów.

Funkcje API identyfikatorów cyfrowych umożliwiają tworzenie, dystrybuowanie i zarządzanie certyfikatami cyfrowymi związanymi z profilami użytkowników. Więcej informacji dotyczących wymienionych poniżej funkcji API zawiera temat Funkcje API w Centrum informacyjnym (patrz “Informacje wstępne i pokrewne” na stronie xvi):

- Add User Certificate (QSYADDUC),
- Remove User Certificate (QSYRMVUC),
- List User Certificate (QSYLSTUC),
- Find Certificate User (QSYFNDUC),
- Add Validation List Certificate (QSYADDVC),
- Remove Validation List Certificate (QSYRMVVC),
- List Validation List Certificate (QSYLSTVC),
- Check Validation List Certificate (QSYCHKVC),
- Parse Certificate (QSYPARSC).

Praca z profilami użytkowników

Ta część rozdziału opisuje komendy oraz ekrany dotyczące tworzenia, zmieniania i usuwania profili użytkowników. Nie wszystkie pola, opcje i klawisze funkcyjne zostały opisane. Aby uzyskać dodatkowe szczegóły, należy zapoznać się z informacjami elektronicznymi.

Aby tworzyć, zmieniać lub usuwać profile użytkowników, wymagane są uprawnienia specjalne *SECADM.

Tworzenie profili użytkowników

Profile użytkowników można tworzyć na kilka sposobów:

- za pomocą ekranu Praca z profilami użytkowników (Work with User Profiles - WRKUSRPRF),
- za pomocą komendy Tworzenie profilu użytkownika (Create User Profile - CRTUSRPRF),
- za pomocą opcji menu SETUP Praca z rejestrowaniem użytkowników (Work with User Enrollment),
- za pomocą ekranu programu iSeries Navigator z folderu iSeries Access.

Użytkownik tworzący profil użytkownika ma do niego prawo własności oraz uprawnienia *ALL. Profil użytkownika ma nadawane uprawnienia *OBJMGT i *CHANGE do samego siebie. Te uprawnienia są konieczne do wykonywania zwykłych operacji i nie powinny być usuwane.

Profil użytkownika nie może być utworzony z większymi uprawnieniami lub możliwościami niż ma użytkownik, który utworzył ten profil.

Uwaga: Wykonując komendę CRTUSRPRF, nie można tworzyć profilu użytkownika (*USRPRF) w niezależnej puli dyskowej. Jednak jeśli użytkownik ma uprawnienia prywatne do obiektu na niezależnej puli dyskowej, jest właścicielem obiektu na niezależnej puli dyskowej lub jest w grupie podstawowej obiektu na niezależnej puli dyskowej, to nazwa profilu przechowywana jest na niezależnej puli dyskowej. Jeśli niezależna pula dyskowa przenoszona jest do innego systemu, uprawnienia prywatne, prawa własności do obiektu oraz pozycji grupy podstawowej będą dołączone w systemie docelowym do profilu o tej samej nazwie. Jeśli w systemie docelowym dany profil nie istnieje, to zostanie utworzony. Użytkownik nie będzie miał żadnych uprawnień specjalnych, a jego hasło będzie miało wartość *NONE.

Używanie komendy Praca z profilami użytkowników (Work with User Profiles)

W komendzie WRKUSRPRF można podać nazwę profilu, jego ogólne ustawienia lub uprawnienia *ALL. Poziom asysty określa, który ekran listy zobaczy użytkownik. Podczas używania komendy WRKUSRPRF z poziomem asysty *BASIC pojawi się ekran Praca z rejestrowaniem użytkowników (Work with User Enrollment). Jeśli podano poziom asysty *INTERMED, użytkownik uzyska dostęp do ekranu Praca z profilami użytkowników (Work with User Profiles).

Parametr ASTLVL (poziom asysty) można podać w komendzie. Jeśli parametr ASTLVL nie zostanie podany, system używa poziomu asysty przechowywanego razem z profilem użytkownika.

Na ekranie Praca z profilami użytkowników (Work with User Profiles) należy wpisać 1 oraz nazwę profilu, który ma być utworzony:

```
                Praca z profilami użytkowników
                  (Work with User Profiles)

Wpisz opcje i naciśnij klawisz Enter.
  1=Utwórz   2=Zmień   3=Kopiuj   4=Usuń
  5=Wyświetlenie 12=Praca z obiektami wg właścicieli

     Profil
Opc  użytkownika Tekst
1   NEWUSER
__  DPTSM       Dział sprzedaży i marketingu
__  DPTWH       Dział hurtowni
```

Pojawi się ekran Tworzenie profilu użytkownika (Create User Profile):

```
          Tworzenie profilu użytkownika
        (Create User Profile - CRTUSRPRF)

Wpisz i naciśnij Enter.
Profil użytkownika . . . . . . . NEWUSER
Hasło użytkownika  . . . . . . . NEWUSER1
Ustawienie hasła jako wygasłe  . *YES
Status . . . . . . . . . . . . . *ENABLED
Klasa użytkownika  . . . . . . . *USER
Poziom asysty  . . . . . . . . . *SYSVAL
Biblioteka bieżąca . . . . . . . *CRTDFT
Wywoływany program początkowy  . *NONE
Biblioteka . . . . . . . . . . .
Menu początkowe  . . . . . . . . MAIN
Biblioteka . . . . . . . . . . .   QSYS
Ograniczenie możliwości  . . . . *NO
Tekst opisu  . . . . . . . . . .
```

Ekran Tworzenie profilu użytkownika (Create User Profile) zawiera wszystkie pola w profilu użytkownika. Aby wprowadzić więcej informacji, należy użyć klawisza F10 (Parametry dodatkowe) i przejść do następnej strony. Aby zobaczyć nazwy parametrów, należy użyć klawisza F11 (Wyświetlenie słów kluczowych).

Ekran Tworzenie profilu użytkownika (Create User Profile) nie dodaje użytkownika do katalogu systemowego.

Używanie komendy Tworzenie profilu użytkownika (Create User Profile)

W celu utworzenia profilu użytkownika można użyć komendy CRTUSRPRF. Parametry można podać razem z komendą lub skorzystać z podpowiedzi (F4) i przejść do ekranu Tworzenie profilu użytkownika (Create User Profile).

Używanie opcji Praca z rejestrowaniem użytkowników (Work with User Enrollment)

Z menu SETUP należy wybrać opcję Praca z rejestrowaniem użytkowników. Poziom asysty przechowywany razem z profilem użytkownika określi, czy pojawi się ekran Praca z profilami użytkowników (Work with User Profiles), czy Praca z rejestrowaniem użytkowników (Work with User Enrollment). Aby zmienić poziomy należy użyć klawisza F21 (Wybór poziomu asysty).

Na ekranie Praca z rejestrowaniem użytkowników (Work with User Enrollment) należy użyć opcji 1 (Dodawanie), aby dodać nowego użytkownika.

```
          Praca z rejestrowaniem użytkowników
             (Work with User Enrollment)

Wpisz opcje i naciśnij Enter.
1=Dodaj   2=Zmień   3=Kopiuj   4=Usuń   5=Wyświetlenie

Opc     Użytkownik        Opis
1      NEWUSER
_      DPTSM          Dział sprzedaży i marketingu
_      DPTWH          Dział hurtowni
```

Pojawi się ekran Dodawanie użytkownika (Add User):

```
      Dodawanie użytkownika
           (Add User)

Wpisz poniżej opcje i naciśnij Enter.

Użytkownik  . . . . . . . NEWUSER
Opis użytkownika  . . . .
Hasło . . . . . . . . . . NEWUSER
Typ użytkownika . . . . . *USER
Grupa użytkowników  . . . *NONE

Ograniczenie użycia wiersza komend   N
Używanie OfficeVision/400 . . Y

Biblioteka domyślna . . .
Drukarka domyślna . . . . *WRKSTN
Program wpisywania się  . *NONE
Biblioteka  . . . . . .

Menu początkowe . . . . .
Biblioteka  . . . . . .

F1=Pomoc   F3=Wyjście   F5=Odśwież   F12=Anuluj
```

Ekran Dodawanie użytkownika (Add User) zaprojektowany został dla administratorów ochrony, którzy nie mają przygotowania technicznego. Ten ekran nie opisuje wszystkich pól w profilu użytkownika. Dla wszystkich pól, które nie zostały pokazane, używane są wartości domyślne.

Uwaga: W przypadku używania ekranu Dodawanie użytkownika (Add User), nazwy profili użytkowników ograniczone są do ośmiu znaków.

Aby zobaczyć drugi ekran, należy przejść do następnej strony:

```
      Dodawanie użytkownika
           (Add User)

Wpisz poniżej opcje i naciśnij Enter.

Program klawisza Attn . *SYSVAL
Biblioteka  . . . . . .

Opcja 50 w menu OfficeVision/400:
Tekst opcji menu          Menu Asysta Operacyjna
Program  użytkownika.   QEZAST
Biblioteka. . . . . .   QSYS
```

Ekran Dodawanie użytkownika (Add User) automatycznie dodaje pozycje w katalogu systemowym z takim samym identyfikatorem użytkownika, jak nazwa profilu użytkownika (pierwszych osiem znaków) oraz adres nazwy systemu.

Menu główne obejmuje także opcje od 51 do 59. Te dodatkowe opcje (Opcje od 51 do 59) przetwarzane są podobnie jak opcja 50, z tym wyjątkiem, że wartości domyślne dla wymienionych poniżej pól są puste:

- Tekst dla opcji menu,
- Program użytkownika,
- Biblioteka.

Kopiowanie profili użytkowników

Profil użytkownika można utworzyć kopiując inny profil użytkownika lub profil grupowy. Jeden profil w grupie można skonfigurować jako wzorzec. Aby utworzyć dodatkowe profile, można skopiować pierwszy profil w grupie.

Profil można skopiować interaktywnie z ekranu Praca z rejestrowaniem użytkowników (Work with User Enrollment)lub Praca z profilami użytkowników (Work with User Profiles). Do kopiowania profilu użytkownika nie istnieje żadna komenda.

Kopiowanie z ekranu Praca z profilami użytkowników

Na ekranie Praca z profilami użytkowników (Work with User Profiles), obok profilu który ma być skopiowany, należy wpisać 3. Pojawi się ekran Tworzenie profilu użytkownika (Create User Profile):

```
          Tworzenie profilu użytkownika
        (Create User Profile - CRTUSRPRF)

Wpisz i naciśnij Enter.
Nazwa użytkownika. . . . . .                Nazwa
Hasło użytkownika  . . . . . > *USRPRF      Nazwa
Ustawienie hasła jako wygasłe  . > *NO      *NO, *YES
Status . . . . . > *ENABLED     *ENABLED,
Klasa użytkownika  . . . . . > *USER        *USER,
Poziom asysty  . . . . . > *SYSVAL      *SYSVAL,
Biblioteka bieżąca . . . . . > DPTWH        Nazwa,
Wywoływany program początkowy  . > *NONE    Nazwa,
Biblioteka . . . . . .                      Nazwa,
Menu początkowe  . . . . . > ICMAIN        Nazwa,
Biblioteka . . . . . > ICPGMLIB     Nazwa,
Ograniczenie możliwości  . . . . > *NO      *NO,
Tekst opisu  . . . . . > 'Magazyn'
```

Wszystkie wartości z kopiowanego profilu użytkownika przedstawione są na ekranie Tworzenie profilu użytkownika (Create User Profile), z wyjątkiem następujących pól:

Katalog osobisty
*USRPRF

Ustawienia narodowe zadania
Ustawienia narodowe zadania

Ustawienia narodowe
Ustawienia narodowe

Profil użytkownika
Puste. Musi być wypełnione.

Hasło *USRPRF

Kolejka komunikatów
*USRPRF

Hasło do dokumentu
*NONE

Numer identyfikacyjny użytkownika
*GEN

Numer identyfikacyjny grupy
*NONE

| **Powiązanie EIM**
| *NOCHG

Uprawnienia
*EXCLUDE

Na ekranie Tworzenie profilu użytkownika (Create User Profile) można zmieniać dowolne pola. Uprawnienia prywatne kopiowanego profilu nie są kopiowane. Nie są kopiowane także wewnętrzne obiekty zawierające preferencje użytkownika oraz inne informacje o użytkowniku.

Kopiowanie z ekranu Praca z rejestrowaniem użytkowników

Na ekranie Praca z rejestrowaniem użytkowników (Work with User Enrollment), obok profilu który ma być skopiowany, należy wpisać 3. Pojawi się ekran Kopiowanie użytkownika (Copy User):

```
     Kopiowanie użytkownika
           (Copy User)

Kopiowanie użytkownika  :   DPTWH

Wpisz poniżej opcje i naciśnij Enter.

Użytkownik  . . . . . .
Opis użytkownika  . . . . Magazyn
Hasło . . . . . .
Typ użytkownika . . . . . USER
Grupa użytkowników  . . .

Ograniczenie użycia wiersza komend   N
Używanie OfficeVision/400 . . Y

Biblioteka domyślna . . . DPTWH
Drukarka domyślna . . . . PRT04
Program wpisywania się  . *NONE
Biblioteka. . . . . .
```

Na ekranie Dodawanie użytkownika (Add User) pojawią się wszystkie wartości kopiowanego profilu z wyjątkiem następujących:

Użytkownik
Puste. Musi być wypełnione. Ograniczone do 8 znaków.

Hasło Puste. Jeśli nie zostanie wpisana wartość, profil tworzony jest z hasłem domyślnym, którego wartość podana została w parametrze PASSWORD komendy CRTUSRPRF.

Na ekranie Kopiowanie użytkowników można zmieniać dowolne pola. Pola profilu użytkownika, które nie pojawiają się, gdy jest wybranypodstawowy poziom asysty, kopiowane są z kopiowanego profilu, z wyjątkiem pól:

Kolejka komunikatów
*USRPRF

Hasło do dokumentu
*NONE

Numer identyfikacyjny użytkownika
*GEN

Numer identyfikacyjny grupy
*NONE

| **Powiązanie EIM**
| *NOCHG

Uprawnienia
*EXCLUDE

Uprawnienia prywatne kopiowanego profilu nie są kopiowane.

Kopiowanie uprawnień prywatnych

Za pomocą komendy Nadanie uprawnień użytkownika (Grant User Authority - GRTUSRAUT) można skopiować uprawnienia prywatne jednego użytkownika do innego. Może to być przydatne w niektórych sytuacjach, ale nie powinno być używane zamiast profili grupowych lub list autoryzacji. Kopiowanie uprawnień nie pomaga w zarządzaniu podobnymi uprawnieniami oraz może spowodować problemy związane z wydajnością systemu.

Więcej informacji na temat używania tej komendy zawiera temat “Kopiowanie uprawnień innego użytkownika” na stronie 146.

Zmienianie profili użytkowników

Za pomocą opcji 2 (Zmień) z ekranu Praca z profilami użytkowników (Work with User Profiles) lub z ekranu Praca z rejestrowaniem użytkowników (Work with User Enrollment) można zmienić profil użytkownika. W tym celu można także użyć komendy Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF).

Użytkownicy, którzy są uprawnieni do wprowadzania komend, za pomocą komendy Zmiana profilu (Change Profile - CHGPRF) mogą zmieniać niektóre parametry swoich profili.

Użytkownik zmieniając profil nie może nadać mu uprawnień specjalnych lub możliwości niż te, które sam posiada.

Usuwanie profili użytkowników

Nie można usunąć profilu użytkownika, który posiada obiekty. Najpierw należy usunąć wszystkie obiekty, których właścicielem jest profil, lub przenieść prawo własności do nich na inny profil. Zarówno podstawowy poziom asysty, jak i pośredni poziom asysty umożliwiają obsługę posiadanych obiektów podczas usuwania profilu.

Nie można usunąć profilu użytkownika, jeśli jest on grupą podstawową dla obiektów. Gdy podczas usuwania profilu użytkownika używany jest pośredni poziom asysty, użytkownik może zmieniać lub usuwać grupę podstawową dla obiektów. Aby wyświetlić wszystkie obiekty, dla których profil jest grupą podstawową, można użyć komendy DSPUSRPRF z opcją *OBJPGP (grupa podstawowa obiektu).

Podczas usuwania profilu użytkownika, jest on usuwany ze wszystkich list dystrybucyjnych z katalogu systemowego.

Nie trzeba zmieniać prawa własności lub usuwać kolejki komunikatów użytkownika. Gdy profil użytkownika jest usuwany, system automatycznie usuwa jego kolejkę komunikatów.

Nie można usunąć profilu grupowego, który ma członków. Aby wyświetlić listę członków profilu grupowego, należy wpisać komendę DSPUSRPRF *nazwa_profilu_grupowego* *GRPMBR. Przed usunięciem profilu grupowego należy zmienić pole GRPPRF dla każdego członka tego profilu.

Używanie komendy Usunięcie profilu użytkownika (Delete User Profile)

Komendę Usunięcie profilu użytkownika (Delete User Profile - DLTUSRPRF) można wprowadzić bezpośrednio lub można użyć opcji 4 (Usunięcie) z ekranu Praca z profilami użytkowników (Work with User Profiles). Komenda DLTUSRPRF ma parametry umożliwiające obsługę:

- wszystkich obiektów, których właścicielem jest profil,
- wszystkich obiektów, dla których profil jest grupą podstawową,
- powiązań EIM.

```
              Usunięcie profilu użytkownika
            (Delete User Profile - DLTUSRPRF)

Wpisz i naciśnij Enter.
Profil użytkownika . . . . . > HOGANR        Name
Opcja posiadanego obiektu:
  Wartość posiadan. obiektu  . . *CHGOWN       *NODLT, *DLT, *CHGOWN
  Nazwa prof. uż.,jeśli *CHGOWN    WILLISR       Nazwa
Opcja grupy głównej:
  Wartość grupy głównej  . . . . *NOCHG        *NOCHG, *PGP
  Nowa grupa podstawowa  . . . .
  Nowe uprawnienia grupy podst .
```

Użytkownik może usunąć wszystkie posiadane przez profil obiekty lub przenieść je do nowego właściciela. Jeśli obiekty mają być obsługiwane pojedynczo, można użyć komendy Praca z obiektami wg właścicieli (Work with Objects by Owner - WRKOBJOWN). Użytkownik może zmienić grupę podstawową dla wszystkich obiektów, dla których profil grupowy jest grupą podstawową. Jeśli obiekty mają być obsługiwane pojedynczo, można użyć komendy Praca z obiektami według grupy podstawowej (Work with Objects by Primary Group - WRKOBJPGP). Ekrany dla obu komend są podobne:

```
             Praca z obiekt. wg właścicieli
              (Work with Objects by Owner)

Profil użytkownika . . . . :   HOGANR

Wpisz opcje i naciśnij klawisz Enter.
  2=Edytuj uprawnienia    4=Usuń   5=Wyświetl uprawnienia
  8=Wyświetlenie opisu    9=Zmiana właściciela
                                                    Urządzenie
Opc    Obiekt      Biblioteka    Typ     Atrybut      ASP
 4   HOGANR        QUSRSYS       *MSGQ                *SYSBAS
 9   QUERY1        DPTWH         *PGM                 *SYSBAS
 9   QUERY2        DPTWH         *PGM                 *SYSBAS
```

Używanie opcji Usuwanie użytkownika

Na ekranie Praca z rejestrowaniem użytkowników (Work with User Enrollment) obok profilu, który ma być usunięty, należy wpisać 4 (Usuwanie). Pojawi się ekran Usuwanie użytkownika (Remove User):

```
              Usuwanie użytkownika
                  (Remove User)

Użytkownik . . . . . . . . :   HOGANR
Opis użytkownika . . . . . :   Sprzedaż i Marketing


Aby usunąć tego użytkownika, wpisz opcję i naciśnij Enter.

     1. Przekaż wszystkie obiekty należące do użytkownika
        nowemu właścicielowi
     2. Usuń lub zmień właściciela obiektów należących
        do tego użytkownika
```

Aby przed usunięciem profilu zmienić prawo własności do wszystkich obiektów, należy wybrać opcję 1. Pojawi się ekran żądający podania nowego właściciela.

Aby obiekty obsługiwać pojedynczo, należy wybrać opcję 2. Pojawi się szczegółowy ekran Usuwanie użytkownika (Remove User):

```
              Usuwanie użytkownika
                  (Remove User)

Użytkownik . . . . . :   HOGANR
Opis użytkownika . . . . . :   Hogan, Richard - Magazyn DPT

Nowy właściciel  . . . . . .         Nazwa, F4 dla listy

Aby usunąć użytkownika, usuń lub zmień właściciela
wszystkich obiektów.
Wypełnij poniższe pola i naciśnij Enter.
  2=Zmień właściciela   4=Usuń   5=Wyświetl szczegóły


Opc  Obiekt        Biblioteka    Opis
 4   HOGANR        QUSRSYS       Kolejka komunikatów HOGANR
 2   QUERY1        DPTWH         Zapytanie spisywania zasobów, raport dotyczący dostępnych ilości
 2   QUERY2        DPTWH         Zapytanie spisywania zasobów, raport dotyczący zamówionych ilości
```

Aby usunąć obiekty lub przenieść je do nowego właściciela, należy użyć opcji na tym ekranie. Gdy wszystkie obiekty zostaną usunięte z tego ekranu, można usunąć profil.

Uwagi:

1. Aby usunąć wszystkie obiekty posiadane przez profil użytkownika, można użyć klawisza F13.
2. Na ekranie Praca z obiektami wg właścicieli (Work with Objects by Owner) zbiory buforowe nie są wyświetlane. Profil użytkownika można usunąć nawet jeśli nadal posiada zbiory buforowe. Po usunięciu profilu użytkownika, należy użyć komendy Praca ze zbiorami buforowymi (Work with Spooled Files - WRKSPLF) i odszukać oraz usunąć zbiory buforowe, których właścicielem jest profil, jeśli nie są już potrzebne.
3. Wszystkie obiekty, dla których usunięty profil użytkownika był grupą podstawową, będą miały grupę podstawową o wartości *NONE.

Praca z obiektami według grupy podstawowej

Aby wyświetlić i pracować z obiektami, dla których profil jest grupą podstawową, można użyć komendy Praca z obiektami według grupy podstawowej (Work with Objects by Primary Group - WRKOBJPGP). Ten ekran może być wykorzystany do zmiany grupy podstawowej dla obiektu lub ustawienia jej na wartość *NONE.

```
         Praca z obiektami wg grupy podstawowej
          (Work with Objects by Primary Group)
Grupa podstawowa . . . . . :   DPTAR

Wpisz opcje i naciśnij klawisz Enter.
  2=Edytuj uprawnienia    4=Usuń   5=Wyświetl uprawnienia
  8=Wyświetlenie opisu    9=Zmiana grupy podstawowej
                                                Urządzenie
Opc    Obiekt     Biblioteka  Typ     Atrybut   ASP
       CUSTMAST   CUSTLIB     *FILE             *SYSBAS
       CUSTWRK    CUSTLIB     *FILE             *SYSBAS
       CUSTLIB    QSYS        *LIB              *SYSBAS
```

Włączanie profilu użytkownika

Jeśli w systemie wartości systemowe QMAXSIGN i QMAXSGNACN skonfigurowane są na wyłączanie profilu użytkownika po zbyt dużej ilości prób wpisania się, użytkownik może żądać od operatora systemu włączenia profilu przez zmianę jego statusu na *ENABLE. Jednak aby włączyć profil użytkownika, wymagane są uprawnienia specjalne *SECADM oraz uprawnienia *OBJMGT i *USE do profilu użytkownika. Zazwyczaj operator systemu nie ma uprawnień specjalnych *SECADM.

Rozwiązaniem tej sytuacji jest użycie prostego programu, który adoptuje uprawnienia:

1. Utwórz program CL posiadany przez użytkownika, który ma uprawnienia specjalne *SECADM oraz uprawnienia *OBJMGT i *USE do profili użytkowników w systemie. Adoptuj uprawnienia właściciela podczas tworzenia programu, korzystając z opcji USRPRF(*OWNER).
2. Za pomocą komendy EDTOBJAUT nadaj uprawnienia publiczne *EXCLUDE do programu, a operatorom systemu uprawnienia *USE.
3. Operator włącza profil wpisując:

   ```
   CALL ENABLEPGM nazwa_profilu
   ```

4. Główna część programu ENABLEPGM wygląda w następujący sposób:

   ```
   PGM &PROFILE
   DCL VAR(&PROFILE) TYPE(*CHAR) LEN(10)
   CHGUSRPRF USRPRF(&PROFILE) STATUS(*ENABLED)
   ENDPGM
   ```

Listing profili użytkowników

Użytkownik może wyświetlać i drukować informacje dotyczące profili użytkowników w różnych formatach.

Wyświetlanie pojedynczego profilu

Aby wyświetlić wartości pojedynczego profilu użytkownika, należy użyć opcji 5 (Wyświetl) na ekranie Praca z rejestrowaniem użytkowników (Work with Objects by Owner) lub Praca z profilami użytkowników (Work with User Profiles). Można także użyć komendy Wyświetlenie profilu użytkownika (Display User Profile - DSPUSRPRF).

Listing wszystkich profili

Za pomocą komendy Wyświetlanie uprawnionych użytkowników (Display Authorized Users - DSPAUTUSR) można wydrukować lub wyświetlić wszystkie profile użytkowników w systemie. Parametr sekwencji (SEQ) w komendzie umożliwia sortowanie według nazwy profilu lub profilu grupowego.

```
                  Wyświetlenie uprawnionych użytkowników
                        (Display Authorized Users)

                       Hasło -
Profil      Profil     Ostatnia    Brak
grupowy     użytkownika zmiana     Hasła   Tekst
DPTSM
            ANDERSR    08/04/0x            Anders, Roger
            VINCENT    09/15/0x            Vincent, Mark
DPTWH
            ANDERSR    08/04/0x            Anders, Roger
            HOGANR     09/06/0x            Hogan, Richard
            QUINN      09/06/0x            Quinn, Rose
QSECOFR
            JONESS     09/20/0x            Jones, Sharon
            HARRISON   08/29/0x            Harrison, Ken
*NO GROUP
            DPTSM      09/05/0x     X      Sprzedaż i marketing
            DPTWH      09/18/0x     X      Hurtownia
```

Naciskając klawisz F11 można zobaczyć, które profile użytkowników mają zdefiniowane hasła do użycia na różnych poziomach haseł.

```
                    Wyświetlenie uprawnionych użytkowników
                          (Display Authorized Users)

                    Ostatnia  Hasło      Hasło        Hasło
Profil    Profil    zmiana   dla poziomu dla poziomu   dla
użytkow. grupowy   hasła     0 lub 1     2 lub 3    NetServer
ANGELA              04/21/0x    *YES        *NO         *YES
ARTHUR              07/07/0x    *YES        *YES        *YES
CAROL1              05/15/0x    *YES        *YES        *YES
CAROL2              05/15/0x    *NO         *NO         *NO
CHUCKE              05/18/0x    *YES        *NO         *YES
DENNISS             04/20/0x    *YES        *NO         *YES
DPORTER             03/30/0x    *YES        *NO         *YES
GARRY               08/04/0x    *YES        *YES        *YES
JANNY               03/16/0x    *YES        *NO         *YES
```

Typy ekranów profilu użytkownika

Komenda Wyświetlenie profilu użytkownika (Display User Profile - DSPUSRPRF) udostępnia kilka typów ekranów i listingów:

- Niektóre ekrany i listingi dostępne są tylko dla pojedynczych profili. Inne mogą być drukowane dla wszystkich profili lub ogólnego zestawu profili. Szczegółowe informacje na temat dostępnych typów zawierają informacje elektroniczne.
- Podając parametr output(*OUTFILE), z niektórych ekranów można utworzyć zbiór wyjściowy. Aby utworzyć własne raporty ze zbiorów wyjściowych, należy użyć narzędzia do tworzenia zapytań. Temat “Analizowanie profili użytkowników” na stronie 269 zawiera sugestie dotyczące raportów.

Rodzaje raportów o profilach użytkowników

Przedstawione poniżej komendy udostępniają raporty o profilach użytkowników.

- Drukowanie profilu użytkownika (Print User Profile - PRTUSRPRF)

  Ta komenda umożliwia drukowanie raportu zawierającego informacje o profilach użytkowników w systemie. Można wydrukować cztery różne raporty. Raport zawierający informacje o uprawnieniach, raport zawierający informacje o środowiskach, raport zawierający informacje o rodzajach haseł oraz raport zawierający informacje o poziomach haseł.
- Analiza domyślnych haseł (Analyze Default Password - ANZDFTPWD)

  Ta komenda umożliwia drukowanie raportu o wszystkich profilach użytkowników w systemie, które mają hasło domyślne oraz umożliwia podjęcie działania względem tych profili. Profil ma domyślne hasło, gdy jest ono takie samo, jak nazwa profilu.

  Profile użytkowników z domyślnymi hasłami mogą być wyłączone, a ich hasła ustawione na wygaśnięcie.

Zmiana nazwy profilu użytkownika

System nie udostępnia bezpośredniej metody zmiany nazwy profilu użytkownika.

Dla użytkownika z nową nazwą można utworzyć profil z tymi samymi uprawnieniami. Jednak niektóre informacje nie mogą być przeniesione do nowego profilu. Poniżej przedstawiono przykłady informacji, które nie mogą być przeniesione:

- zbiory buforowe,
- wewnętrzne obiekty zawierające preferencje użytkownika oraz pozostałe informacje o użytkowniku,
- certyfikaty cyfrowe, które zawierają nazwę użytkownika,
- Informacje uid i gid zachowane przez zintegrowany system plików nie mogą być zmieniane.

- użytkownik nie może zmienić informacji, które przechowywane są przez aplikacje, a które zawierają nazwę użytkownika.

Aplikacje uruchamiane przez użytkownika mogą mieć ″profile aplikacji″. Tworzenie nowego profilu użytkownika systemu iSeries w celu zmiany nazwy nie zmienia nazw profili aplikacji, które może posiadać użytkownik. Przykładem profilu aplikacji jest profil programu Lotus Notes.

Przedstawiony poniżej przykład opisuje sposób tworzenia nowego profilu dla użytkownika z nową nazwą i takimi samymi uprawnieniami. Poprzednia nazwa profilu to SMITHM. Nowa nazwa to JONESM:

1. Skopiuj poprzedni profil (SMITHM) do nowego profilu (JONESM) korzystając z opcji kopiowania na ekranie Praca z rejestrowaniem użytkowników (Work with User Enrollment).
2. Nadaj użytkownikowi JONESM wszystkie uprawnienia prywatne użytkownika SMITHM korzystając z komendy Nadanie uprawnień użytkownika (Grant User Authority - GRTUSRAUT):

   ```
   GRTUSRAUT JONESM REFUSER(SMITHM)
   ```

3. Za pomocą komendy Praca z obiektami według grupy podstawowej (Work with Objects by Primary Group - WRKOBJPGP) zmień grupę podstawową dla wszystkich obiektów, dla których grupą podstawową jest użytkownik SMITHM:

   ```
   WRKOBJPGP PGP(SMITHM)
   ```

   Dla wszystkich obiektów, które muszą mieć zmienioną grupę podstawową, wpisz opcję 9 i w wierszu komend wpisz NEWPGP (JONESM).

   Uwaga: Użytkownik JONESM, za pomocą parametru GID w komendach Tworzenie lub zmiana profilu użytkownika (Create lub Change User Profile - CRTUSRPRF lub CHGUSRPRF) musi mieć przypisany identyfikator gid.
4. Za pomocą komendy Wyświetlenie profilu użytkownika (Display User Profile - DSPUSRPRF) wyświetl profil użytkownika SMITHM:

   ```
   DSPUSRPRF USRPRF(SMITHM)
   ```

   Zapisz jego identyfikatory uid i gid.
5. Przenieś prawo własności do wszystkich posiadanych obiektów na użytkownika JONESM i usuń profil SMITHM korzystając z opcji 4 (Usunięcie) ekranu Praca z rejestrowaniem użytkowników (Work with User Enrollment).
6. Za pomocą komendy Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF) zmień identyfikatory uid i gid użytkownika JONESM podając identyfikatory uid i gid, które należały do użytkownika SMITHM:

   ```
   CHGUSRPRF USRPRF(JONESM) UID(uid użytkownika SMITHM)
             GID(gid użytkownika SMITHM)
   ```

   Jeśli użytkownik JONESM posiada obiekty w katalogu, do zmiany identyfikatorów uid i gid nie można użyć komendy CHGUSRPRF. Zamiast tego należy użyć funkcji API QSYCHGID.

Praca z kontrolą użytkownika

Aby ustawić charakterystyki kontroli dla użytkowników, należy użyć komendy Zmiana kontroli użytkownika (Change User Auditing - CHGUSRAUD). Aby używać tej komendy, użytkownik musi mieć uprawnienia *AUDIT.

```
            Zmiana kontroli użytkownika
          (Change User Audit - CHGUSRAUD)

Wpisz i naciśnij Enter.
Profil użytkownika . . . . . . . HOGANR
                                   JONESS
Wartość kontroli obiektu . . . . *SAME
Kontrola działań użytkownika . . *CMD
                                   *SERVICE
```

Charakterystyki kontroli można podać dla więcej niż jednego użytkownika, podając listę nazw profili użytkowników.

Parametr AUDLVL (kontrola działań użytkownika) może mieć więcej niż jedną wartość. Wartości podawane w tej komendzie zastępują bieżące wartości parametru AUDLVL dla użytkowników. Podane wartości nie są dodawane do bieżących wartości parametru AUDLVL.

Za pomocą komendy Wyświetlenie profilu użytkownika (Display User Profile - DSPUSRPRF) można wyświetlić charakterystyki kontroli użytkownika.

Praca z profilami w programach CL

Informacje o profilu użytkownika można odtwarzać w programie CL. W programie CL można użyć komendy Odtwarzanie profilu użytkownika (Retrieve User Profile - RTVUSRPRF). Komenda zwraca żądane atrybuty profilu do zmiennych, które zostały powiązane z nazwami pól profilu użytkownika. Opisy pól profilu użytkownika zaprezentowane w tym rozdziale zawierają długości pól oczekiwane przez komendę RTVUSRPRF. W niektórych przypadkach pole dziesiętne może mieć wartość, która nie jest numeryczna. Na przykład pole pamięci maksymalnej (MAXSTG) jest polem dziesiętnym, ale może mieć wartość *NOMAX. W informacjach elektronicznych dotyczących komendy RVTUSRPRF opisano wartości, które zwracane są w polach dziesiętnych, a które nie są numeryczne.

Przedstawiony w sekcji “Używanie programu zatwierdzającego hasło” na stronie 45 przykładowy program opisuje przykład użycia komendy RTVUSRPRF.

W programach CL można używać także komend CRTUSRPRF lub CHGUSRPRF. Jeśli dla parametrów tych komend użyte zostaną zmienne, należy zdefiniować je jako pola znakowe, aby były zgodne z podpowiedzią ekranu Tworzenie profilu użytkownika (Create User Profile). Wielkości zmiennych nie muszą być dopasowane do wielkości pól.

Nie ma możliwości odtworzenia hasła użytkownika, ponieważ hasło przechowywane jest z jednokierunkowym szyfrowaniem. Jeśli użytkownik ma ponownie wprowadzić hasło do dostępu do informacji krytycznych, w programie można użyć komendy Sprawdzenie hasła (Check Password - CHKPWD). System porównuje wprowadzone hasło z hasłem użytkownika i jeśli hasło nie jest poprawne, wysyła do programu komunikat o przedwczesnym zakończeniu.

Punkty wyjścia profilu użytkownika

Punkty wyjścia udostępnione są w celu tworzenia, zmieniania, usuwania lub odtwarzania profili użytkowników. Aby wykonywać określone funkcje związane z profilem użytkownika, można napisać własny program obsługi wyjścia. Podczas rejestrowania programu obsługi wyjścia za pomocą punktu wyjścia profilu użytkownika, podczas tworzenia, zmiany, usuwania lub odtwarzania profilu użytkownika następuje powiadomienie o wykonanej funkcji. W momencie powiadomienia, program obsługi wyjścia może wykonać następujące czynności:

- odtworzyć informacje o profilu użytkownika,
- zarejestrować w katalogu systemowym profil, który właśnie został utworzony,
- utworzyć dla profilu użytkownika wymagane obiekty.

Uwaga: Przed wywołaniem programu obsługi wyjścia, wszystkie uprawnienia adoptowane są wstrzymywane. Oznacza to, że program może nie mieć uprawnień do dostępu do obiektu profilu użytkownika.

Więcej informacji na temat programów obsługi wyjścia związanych z ochroną zawiera temat Funkcje API w Centrum informacyjnym (patrz sekcja “Informacje wstępne i pokrewne” na stronie xvi).

Profile użytkowników IBM

Razem z oprogramowaniem systemu dostarczana jest pewna liczba profili użytkowników. Te profile użytkowników IBM używane są jako właściciele obiektów przez różne funkcje systemowe. Niektóre funkcje systemowe działają także tylko pod kontrolą profili użytkowników IBM.

Profile użytkowników IBM, z wyjątkiem QSECOFR, dostarczane są z hasłem *NONE i nie są przeznaczone do wpisywania się. Aby umożliwić zainstalowanie systemu, hasło dla profilu szefa ochrony (QSECOFR) zawsze jest takie samo dla każdego dostarczanego systemu. Jednak jest ono ustawione jako wygasłe. W przypadku nowych systemów, należy zmienić hasło podczas pierwszego wpisywania się za pomocą profilu QSECOFR.

Podczas instalowania nowego wydania systemu operacyjnego, hasła dla profili użytkowników IBM nie są zmieniane. Jeśli profile takie jak QPGMR i QSYSOPR mają hasła, to nie są one automatycznie ustawiane na wartość *NONE.

Dodatek B, “Profile użytkowników dostarczane przez IBM”, na stronie 281 zawiera pełną listę wszystkich profili użytkowników IBM oraz wartości pól dla każdego profilu.

Uwaga: Profile użytkowników IBM są dostępne, ale używane są przez system operacyjny IBM Operating System/400. Dlatego wpisywanie się za pomocą tych profili lub używanie ich do posiadania obiektów użytkownika (nie dostarczonych przez IBM) **nie** jest zalecane.

Zmienianie haseł dla profili użytkowników IBM

Jeśli istnieje potrzeba wpisania się za pomocą jednego z profili użytkowników IBM, za pomocą komendy CHGUSRPRF można zmienić jego hasło. Takie hasła można zmienić także za pomocą opcji z menu SETUP. Aby zabezpieczyć system, wszystkie profile użytkowników IBM oprócz QSECOFR powinny mieć hasło o wartości *NONE. Hasło dla profilu QSECOFR nie powinno być trywialne.

```
          Zmiana haseł użytkowników IBM
       (Change Passwords for IBM-Supplied)

Wpisz nowe hasło dla standardowego użytkownika
systemowego,
wpisz hasło ponownie w celu weryfikacji,
naciśnij Enter.

Nowe hasło szefa ochrony (QSECOFR) . . . . . .
  Nowe hasło (dla sprawdzenia) . . . . . .

Nowe hasło operatora systemu (QSYSOPR) . . . . . .
  Nowe hasło (dla sprawdzenia) . . . . . .

Nowe hasło programisty (QPGMR) . . . . . .
  Nowe hasło (dla sprawdzenia) . . . . . .

Nowe hasło użytkownika (QUSER) . . . . . .
  Nowe hasło (dla sprawdzenia) . . . . . .

Nowe hasło serwisanta (QSRV) . . . . . .
  Nowe hasło (dla sprawdzenia) . . . . . .
```

Aby zmienić dodatkowe hasła, należy przejść do następnej strony:

```
         Zmiana haseł użytkowników IBM
       (Change Passwords for IBM-Supplied)

Wpisz nowe hasło dla standardowego
użytkownika systemowego, wpisz
zmianę, naciśnij Enter.

Nowe hasło podstawowego serwisanta (QSRVBAS) . . . .
  Nowe hasło (dla sprawdzenia) . . . . . .
```

Praca z identyfikatorami użytkowników narzędzi serwisowych

W tym wydaniu wprowadzono kilka ulepszeń do narzędzi serwisowych, które ułatwiają ich używanie oraz zrozumienie.

- **Systemowe narzędzia serwisowe (System service tools - SST)**

  Teraz można zarządzać i tworzyć identyfikatory użytkowników narzędzi serwisowych z poziomu narzędzi SST, wybierając opcję 8 (Praca z identyfikatorami użytkowników narzędzi serwisowych) z głównego menu narzędzi SST. Aby zresetować hasło, nadać lub odwołać uprawnienia lub tworzyć identyfikatory użytkowników narzędzi serwisowych, nie trzeba już przechodzić do narzędzi DST. **Uwaga**: Informacje dotyczące narzędzi serwisowych zostały przeniesione do Centrum informacyjnego.

- **Ulepszenie wprowadzone w zarządzaniu hasłami**

  Serwer dostarczany jest z ograniczoną możliwością zmiany domyślnych oraz wygasłych haseł. Oznacza to, że użytkownik nie może zmienić za pomocą funkcji API Change Service Tools User ID (QSYCHGDS) identyfikatorów użytkowników narzędzi serwisowych, które mają domyślne i wygasłe hasła. Nie może zrobić tego także za pośrednictwem narzędzi SST. Identyfikator użytkownika narzędzi serwisowych z takimi hasłami można zmienić jedynie za pomocą narzędzi DST. Za pomocą tych narzędzi można także zmienić ustawienie umożliwiające zmianę domyślnych i wygasłych haseł. Nowych uprawnień do uruchamiania narzędzi serwisowych (STRSST) można użyć także do utworzenia identyfikatora użytkownika narzędzi serwisowych, który ma dostęp do narzędzi DST, ale nie ma dostępu do narzędzi SST.

- **Zmiany w terminologii**

  Dane tekstowe oraz pozostała dokumentacja została zmieniona, aby odzwierciedlać nową terminologię narzędzi serwisowych. Szczególnie termin identyfikatory użytkowników narzędzi serwisowych zastępuje poprzednie terminy, takie jak profile użytkowników DST, identyfikatory użytkowników DST, profile użytkowników narzędzi serwisowych lub odmiany tych nazw.

Informacje dotyczące pracy z narzędziami serwisowymi znajdują się w temacie dotyczącym narzędzi serwisowych w Centrum informacyjnym (**Ochrona—>Narzędzia serwisowe**). Więcej informacji na temat sposobu dostępu do Centrum informacyjnego zawiera sekcja “Informacje wstępne i pokrewne” na stronie xvi.

Hasło systemowe

Hasło systemowe używane jest do autoryzowania zmian modelu systemu, pewnych warunków serwisowych oraz zmian prawa własności. Jeśli w systemie wystąpią takie zmiany, podczas przeprowadzania IPL użytkownik zostanie poproszony o podanie hasła systemowego.

Rozdział 5. Ochrona zasobów

Ochrona zasobów definiuje, jacy użytkownicy uprawnieni są do korzystania z obiektów w systemie oraz jakie operacje na tych obiektach mogą wykonywać.

Ten rozdział zawiera opis komponentów ochrony zasobów oraz informacje dotyczące ich działania w celu ochrony informacji o systemie. Wyjaśnia także, jak używać komend CL oraz ekranów do konfigurowania ochrony zasobów.

Rozdział 7 omawia techniki projektowania ochrony zasobów, a także jej wpływ na projektowanie aplikacji oraz wydajność systemu.

Temat “Sposób sprawdzania uprawnień” na stronie 149 opisuje schematy blokowe oraz uwagi dotyczące sprawdzania uprawnień. Mogą to być informacje pomocne podczas czytania wyjaśnień znajdujących się poniżej.

Definiowanie, kto może mieć dostęp do informacji

Uprawnienia można nadać pojedynczym użytkownikom, grupom użytkowników lub wszystkim użytkownikom systemu.

Uwaga: W niektórych środowiskach uprawnienia nazywane są **przywilejami**.

Użytkownik może określić, kto może korzystać z obiektu na kilka sposobów:

Uprawnienia publiczne:

Użytkownicy publiczni to wszyscy, którzy mają uprawnienia do wpisywania się do systemu. Uprawnienia publiczne zdefiniowane są dla każdego obiektu w systemie, chociaż mogą być ustawione na *EXCLUDE. Uprawnienia publiczne do obiektu są używane, jeśli nie zostały podane żadne specyficzne uprawnienia do obiektu.

Uprawnienia prywatne:

Użytkownik może definiować określone uprawnienia do używania (lub nie) obiektu. Uprawnienia mogą być nadane pojedynczemu profilowi użytkownika lub profilowi grupowemu. Obiekt ma **uprawnienia prywatne**, jeśli zdefiniowano dla niego dowolne uprawnienia inne niż uprawnienia publiczne, prawo własności do obiektu lub uprawnienia grupy podstawowej.

Uprawnienia użytkownika:

Pojedyncze profile użytkowników mogą otrzymać uprawnienia do używania obiektów w systemie. To jeden z typów uprawnień prywatnych.

Uprawnienia grupowe:

Profile grupowe mogą otrzymać uprawnienia do używania obiektów w systemie. Członek grupy otrzymuje uprawnienia grupy, chyba że jego uprawnienia zostały zdefiniowane osobno. Uprawnienia grupowe są także uprawnieniami prywatnymi.

Prawo własności do obiektu:

Każdy obiekt w systemie ma właściciela. Właściciel domyślnie ma uprawnienia *ALL do tego obiektu. Jednak uprawnienia właściciela mogą być zmienione lub usunięte. Uprawnienia właściciela do obiektu nie są uprawnieniami prywatnymi.

Uprawnienia grupy podstawowej:

Użytkownik może określić dla obiektu grupę podstawową oraz uprawnienia, jakie ta grupa ma do obiektu. Uprawnienia grupy podstawowej zapisywane są razem z obiektem. Zapewnia to uzyskanie lepszej wydajności w porównaniu z nadaniem uprawnienia dla profilu grupowego. Jedynie profil użytkownika z numerem identyfikacyjnym grupy (gid) może być grupą podstawową dla obiektu. Uprawnienia grupy podstawowej nie są uprawnieniami prywatnymi.

Definiowanie sposobu dostępu do informacji

Uprawnienie oznacza rodzaj dozwolonego dostępu do obiektu. Różne rodzaje operacji wymagają różnego rodzaju uprawnień.

Uwaga: W niektórych środowiskach uprawnienia związane z obiektem nazywane są **trybem dostępu** do obiektu.

Uprawnienia do obiektu podzielone są na trzy kategorie: 1) **uprawnienia do obiektu** definiują, jakie operacje mogą być przeprowadzane na obiekcie jako całości. 2) **Uprawnienia do danych** definiują, jakie operacje mogą być przeprowadzane na zawartości obiektu. **Uprawnienia do pól** definiują, jakie operacje mogą być przeprowadzane na polach danych.

Tabela 111 opisuje typy dostępnych uprawnień oraz przykłady użycia tych uprawnień. W większości przypadków dostęp do obiektu wymaga kombinacji uprawnień do obiektu, do danych i do pól. Dodatek D udostępnia informacje dotyczące uprawnień, które wymagane są do wykonywania określonych funkcji.

Tabela 111. Opis typów uprawnień

Uprawnienie	Nazwa	Dozwolone funkcje
Uprawnienia do obiektu:		
*OBJOPR	Operacyjne do obiektu	Przeglądanie opisu obiektu. Używanie obiektu zgodnie z uprawnieniami użytkownika do danych.
*OBJMGT	Zarządzanie obiektami	Określanie ochrony obiektu. Przenoszenie lub zmiana nazwy obiektu. Wszystkie funkcje zdefiniowane dla uprawnień *OBJALTER i *OBJREF.
*OBJEXIST	Istnienie obiektu	Usunięcie obiektu. Zwalnianie pamięci obiektu. Wykonywanie operacji składowania i odtwarzania obiektu [1]. Przenoszenie prawa własności.
*OBJALTER	Zmiana obiektu	Dodawanie, usuwanie zawartości, inicjowanie i reorganizowanie podzbiorów zbiorów bazy danych. Zmiana i dodawanie atrybutów zbiorów bazy danych: dodawanie i usuwanie wyzwalaczy. Zmiana atrybutów pakietów SQL.
*OBJREF	Odniesienie do obiektu	Określanie zbioru bazy danych jako nadrzędnego w ograniczeniu referencyjnym. Na przykład można zdefiniować regułę, że rekord klienta musi istnieć w zbiorze CUSMAS, zanim zamówienie klienta będzie można dodać do zbioru CUSORD. Aby zdefiniować tę regułę, użytkownik musi mieć uprawnienia *OBJREF do zbioru CUSMAS.
*AUTLMGT	Zarządzanie listą autoryzacji	Dodawanie i usuwanie użytkowników oraz ich uprawnień z listy autoryzacji [2].
Uprawnienia do danych:		
*READ	Odczyt	Wyświetlanie zawartości obiektu - przeglądanie rekordów w zbiorze.
*ADD	Dodanie	Dodawanie pozycji do obiektu - dodawanie komunikatów do kolejki komunikatów lub rekordów do zbioru.

Tabela 111. Opis typów uprawnień (kontynuacja)

Uprawnienie	Nazwa	Dozwolone funkcje
*UPD	Aktualizacja	Zmienianie pozycji w obiekcie - zmienianie rekordów w zbiorze.
*DLT	Usunięcie (Delete)	Usuwanie pozycji z obiektu - usuwanie komunikatów z kolejki komunikatów lub usuwanie rekordów ze zbioru.
*EXECUTE	Wykonywanie	Uruchamianie programu, programu usługowego lub pakietu SQL. Odszukiwanie obiektu w bibliotece lub katalogu.
Uprawnienia do pól:		
*Mgt	Zarządzanie	Określanie ochrony pola.
*Alter	Zmienianie	Zmiana atrybutów pola.
*Ref	Odniesienie	Podanie pola jako części klucza nadrzędnego w ograniczeniu referencyjnym.
*Read	Odczyt	Dostęp do zawartości pola. Na przykład wyświetlenie zawartości pola.
*Add	Dodanie	Dodanie pozycji do danych, na przykład dodanie informacji do określonego pola.
*Update	Aktualizacja	Zmiana zawartości istniejących pozycji w polu.

[1] Jeśli użytkownik ma uprawnienia specjalne do składowania systemu (*SAVSYS), do wykonywania operacji składowania i odtwarzania obiektu uprawnienia do istnienia obiektu nie są wymagane.

[2] Więcej informacji zawiera temat “Zarządzanie listą autoryzacji” na stronie 120.

Najczęściej używane uprawnienia

Do wykonywania operacji na obiektach zwykle wymagane są pewne zestawy uprawnień do obiektu i do danych. Zamiast pojedynczo definiować uprawnienia potrzebne do obiektu, można określić zestawy uprawnień zdefiniowane systemowo (*ALL, *CHANGE, *USE). Uprawnienie *EXCLUDE to coś innego niż brak uprawnień. Uprawnienie *EXCLUDE szczególnie odmawia dostępu do obiektu. Brak uprawnień oznacza, że do obiektu można używać uprawnień publicznych. Tabela 112 opisuje uprawnienia zdefiniowane systemowo, które dostępne są podczas używania komend oraz ekranów uprawnień do obiektu.

Tabela 112. Uprawnienia zdefiniowane systemowo

Uprawnienie	*ALL	*CHANGE	*USE	*EXCLUDE
Uprawnienia do obiektu				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
Uprawnienia do danych				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X		
*DLT	X	X		
*EXECUTE	X	X	X	

Tabela 113 na stronie 116 zawiera uprawnienia zdefiniowane systemowo, które są dostępne podczas używania komend WRKAUT i CHGAUT:

Tabela 113. Uprawnienia zdefiniowane systemowo

Uprawnienie	*RWX	*RW	*RX	*R	*WX	*W	*X
Uprawnienia do obiektu							
*OBJOPR	X	X	X	X	X	X	X
*OBJMGT							
*OBJEXIST							
*OBJALTER							
*OBJREF							
Uprawnienia do danych							
*READ	X	X	X	X			
*ADD	X	X			X	X	
*UPD	X	X			X	X	
*DLT	X	X			X	X	
*EXECUTE	X		X		X		X

Program licencjonowany LAN Server do zarządzania uprawnieniami korzysta z list kontroli dostępu. Uprawnienia użytkownika nazywane są **zezwoleniami**. Tabela 114 pokazuje, w jaki sposób zezwolenia programu LAN Server odwzorowują uprawnienia do obiektu i do danych:

Tabela 114. Zezwolenia programu LAN Server

Uprawnienie	Zezwolenia programu LAN Server
*EXCLUDE	Brak
Uprawnienia do obiektu	
*OBJOPR	Patrz uwaga 1
*OBJMGT	Zezwolenie
*OBJEXIST	Tworzenie, usuwanie
*OBJALTER	Atrybut
*OBJREF	Brak odpowiednika
Uprawnienia do danych	
*READ	Odczyt
*ADD	Tworzenie
*UPD	Zapis
*DLT	Usunięcie (Delete)
*EXECUTE	Wykonywanie

1 Dopóki na liście kontroli dostępu dla użytkownika nie określona zostanie wartość NONE, użytkownik domyślnie ma uprawnienia *OBJOPR.

Definiowanie informacji, do których można uzyskać dostęp

Użytkownik może zdefiniować ochronę zasobów dla pojedynczych obiektów w systemie. Może także zdefiniować ochronę dla grup obiektów korzystając z ochrony biblioteki lub listy autoryzacji:

Ochrona biblioteki

Większość obiektów w systemie znajduje się w bibliotekach. Aby uzyskać dostęp do obiektu, użytkownik musi mieć uprawnienia zarówno do samego obiektu, jak i do biblioteki, w której znajduje się obiekt. Dla większości operacji, łącznie z usuwaniem obiektu, wystarczające są uprawnienia *USE do biblioteki obiektu (oprócz uprawnień wymaganych do obiektu). Tworzenie nowego obiektu wymaga uprawnień *ADD do biblioteki obiektu. Dodatek D pokazuje, jakie uprawnienia wymagane są przez komendy CL do obiektów oraz bibliotek obiektów.

Podczas obsługiwania prostego schematu ochrony, jedną z technik zabezpieczania informacji jest korzystanie z ochrony biblioteki. Aby ochronić na przykład poufne informacje dla zbioru aplikacji, można:

- dla danej grupy aplikacji skorzystać z biblioteki, w celu przechowywania wszystkich poufnych zbiorów;
- sprawdzić, czy uprawnienia prywatne do wszystkich obiektów (w bibliotece) używane przez aplikacje, są wystarczające (*USE lub *CHANGE);
- ograniczyć uprawnienia publiczne do samej biblioteki (*EXCLUDE);
- nadać wybranym grupom lub pojedynczym użytkownikom uprawnienia do biblioteki (*USE lub *ADD, jeśli aplikacje tego wymagają).

Chociaż ochrona biblioteki jest prostą i efektywną metodą zabezpieczania informacji, może nie być wystarczająca dla danych w środowiskach z wysokimi wymaganiami ochrony. Bardzo wrażliwe obiekty powinny być zabezpieczane pojedynczo lub za pomocą list autoryzacji, nie należy polegać na ochronie biblioteki.

Ochrona biblioteki i listy bibliotek

Gdy do listy bibliotek użytkownika dodawana jest biblioteka, uprawnienia, które użytkownik ma do biblioteki, przechowywane są razem z informacjami listy bibliotek. Uprawnienia użytkownika do biblioteki pozostają dla całego zadania, nawet jeśli zostaną odebrane, gdy zadanie będzie aktywne.

Po zgłoszeniu żądania dostępu do obiektu, dla ktorego podano parametr *LIBL, do sprawdzenia uprawnień do biblioteki używana jest lista bibliotek. Jeśli podana jest nazwa kwalifikowana, uprawnienia do biblioteki są sprawdzane osobno, nawet jeśli biblioteka znajduje się na liście bibliotek użytkownika.

Uwaga: Jeśli podczas dodawania biblioteki do listy użytkownik pracuje z uprawnieniami adoptowanymi, to po zakończeniu pracy z tymi uprawnieniami jest on nadal uprawniony do tej biblioteki. Powoduje to powstanie potencjalnego ryzyka naruszenia ochrony. Przed zakończeniem działania programu adoptującego uprawnienia wszystkie pozycje dodane do listy bibliotek użytkownika przez program powinny być usunięte.

Aplikacje używające listy bibliotek zamiast kwalifikowanych nazw bibliotek powodują powstanie potencjalnego ryzyka naruszenia ochrony. Użytkownik z uprawnieniami do komend umożliwiających pracę z listami bibliotek może potencjalnie uruchomić inną wersję programu. Więcej informacji na ten temat zawiera sekcja “Listy bibliotek” na stronie 187.

Uprawnienia do pól

Uprawnienia do pól są teraz obsługiwane dla zbiorów bazy danych. Obsługiwane uprawnienia to odniesienie i aktualizacja. Tymi uprawnieniami można zarządzać tylko za pomocą instrukcji SQL GRANT i REVOKE. Można je wyświetlać za pomocą komend Wyświetlenie uprawnień dla obiektu (Display Object Authority - DSPOBJAUT) i Edycja uprawnień dla obiektu (Edit Object Authority - EDTOBJAUT). Uprawnienia do pól można za pomocą komendy EDTOBJAUT tylko wyświetlać; nie można ich edytować.

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   PLMITXT     Właściciel . . . . . :   PGMR1
  Biblioteka . . :   RLN         Grupa podstawowa . . :   DPTAR
Typ obiektu  . . :   *FILE       Urządzenie ASP . . . :   *SYSBAS

Obiekt chroniony listą autoryzacji  . . . . . :   *NONE
                       Upr. do    ---------------Dane---------------
Użytkownik  Grupa      obiektu   Odczyt Dod. Aktual. Usuw. Wykonyw.
*PUBLIC                *CHANGE     X     X     X       X       X
PGMR1                  *ALL        X     X     X       X       X
USER1                  *USE        X                             X
USER2                  USER DEF    X           X                 X
USER3                  USER DEF    X                             X



Aby kontynuować, naciśnij Enter


F3=Wyjście F11=Bez szczegółów F12=Anuluj F16=Uprawnienia do pól
```

Rysunek 4. Ekran Wyświetlenie uprawnień dla obiektu (Display Object Authority) z opcją F16=Uprawnienia do pól. Ten klawisz funkcyjny jest wyświetlany, gdy zbiór bazy danych ma uprawnienia do pól.

```
                    Wyświetlenie uprawnień do pól
                      (Display Field Authority)
Obiekt . . . . . :   PLMITXT         Właściciel . . . . . :   PGMR1
  Biblioteka . . . . :     RLN       Grupa podstawowa . . :   *NONE
Typ obiektu  . . . . :   *FILE

                       Uprawn.   -----Uprawnienia do pól----------
Pole         Użytk.   do obiektu Zarz.Zmian.Odn. Odcz. Dod. Aktualiz.
Pole3        PGMR1      *ALL        X      X   X    X     X      X
             USER1      *Use                        X
             USER2      USER DEF                    X            X
             USER3      USER DEF                X   X
             *PUBLIC    *CHANGE                     X     X      X
Pole4        PGMR1      *ALL        X      X        X     X      X
             USER1      *Use                        X
             USER2      USER DEF                    X
             USER3      USER DEF                    X
             *PUBLIC    *CHANGE                     X     X      X
                                                            Więcej
Aby kontynuować, naciśnij Enter.

F3=Wyjście F5=Odśwież F12=Anuluj F16=Powtórz ustawienie na F17=Ustaw na
```

Rysunek 5. Ekran Wyświetlenie uprawnień do pól (Display Field Authority). Gdy zostanie naciśnięty klawisz F17=Ustaw na, wyświetlona zostanie podpowiedź Pozycja na liście. Jeśli naciśnięty zostanie klawisz F16, powtórzona zostanie poprzednia pozycja dla operacji

Zmiany uprawnień do pól obejmują następujące elementy:

- komenda Drukowanie uprawnień prywatnych (Print Private Authority - PRTPVTAUT) ma nowe pole wskazujące, że zbiór ma uprawnienia do pól,

- komenda Wyświetlenie uprawnień dla obiektu (Display Object Authority - DSPOBJAUT) ma teraz nowy parametr Typ uprawnień, umożliwiający wyświetlenie uprawnień do obiektu, uprawnień do pól lub wszystkich uprawnień; jeśli typem obiektu nie jest *FILE, można wyświetlić jedynie uprawnienia do obiektu,
- informacje udostępniane przez funkcje API List Users Authorized to Object (QSYLUSRA) teraz wskazują, czy zbiór ma uprawnienia do pól,
- komenda Nadanie uprawnień użytkownika (Grant User Authority - GRTUSRAUT) nie nada uprawnień użytkownika do pól,
- gdy za pomocą komendy GRTOBJAUT przeprowadzane jest nadawanie z użyciem obiektu odniesienia, a oba obiekty (ten, dla którego nadawane są uprawnienia i ten, który jest obiektem odniesienia) są zbiorami bazy danych, wszystkie uprawnienia do pól zostaną nadane, gdy nazwy pól będą zgodne,
- jeśli uprawnienia użytkownika do zbioru bazy danych są usuwane, wszystkie uprawnienia do pól dla tego użytkownika także są usuwane.

Ochrona a środowisko System/38

Środowisko System/38 oraz programy CL typu CLP38 stanowią potencjalne ryzyko naruszenia ochrony. Gdy z poziomu ekranu Wprowadzanie komendy System/38 (System/38 Command Entry) lub programu CL CLP38 wywoływana lub wprowadzana jest komenda nie kwalifikowana biblioteką, najpierw przeszukiwana jest biblioteka QUSER38 (jeśli istnieje) dla tej komendy. Drugą przeszukiwaną biblioteką jest QSYS38. Programista lub inny doświadczony użytkownik może umieścić inną komendę CL w jednej z tych bibliotek i spowodować, że zamiast komendy z biblioteki na liście bibliotek użyta zostanie właśnie ta komenda.

Biblioteka QUSER38 nie jest dostarczana razem z systemem operacyjnym. Jednak może być utworzona przez kogokolwiek z uprawnieniami wystarczającymi do tworzenia biblioteki.

Więcej informacji dotyczących środowiska System/38 zawiera podręcznik *System/38 Environment Programming*.

Zalecenia dla środowiska System/38

Poniższe działania należy wykorzystać w celu zabezpieczenia systemu przed środowiskiem System/38 oraz programami CL typu CLP38:

- należy sprawdzić uprawnienia publiczne do biblioteki QSYS38 i jeśli są to uprawnienia *ALL lub *CHANGE, należy zmienić je na *USE,
- należy sprawdzić uprawnienia publiczne do biblioteki QUSER38 i jeśli są to uprawnienia *ALL lub *CHANGE, należy zmienić je na *USE,
- jeśli biblioteki QUSER38 i QSYS38 nie istnieją, należy je utworzyć i ustawić ich uprawnienia publiczne na *USE; zapobiegnie to utworzeniu ich w późniejszym czasie i nadaniu im zbyt dużych uprawnień publicznych.

Ochrona katalogu

Podczas uzyskiwania dostępu do obiektu w katalogu, użytkownik musi mieć uprawnienia do wszystkich katalogów w ścieżce zawierającej obiekt. W celu przeprowadzenia żądanej operacji musi mieć także odpowiednie uprawnienia do obiektu.

Ochrony katalogu można używać w taki sam sposób, jak ochrony biblioteki. Należy ograniczyć dostęp do katalogów oraz użyć uprawnień publicznych do obiektów w katalogu. Ograniczenie liczby uprawnień prywatnych dla obiektów zwiększa wydajność procesu sprawdzania uprawnień.

Ochrona za pomocą listy autoryzacji

Obiekty z podobnymi wymaganiami ochrony można pogrupować za pomogą listy autoryzacji. Lista autoryzacji zawiera listę użytkowników oraz ich uprawnienia do obiektów chronionych przez tę listę. Każdy użytkownik może mieć inne uprawnienia do zestawu obiektów, które chroni lista. Nadanie użytkownikowi uprawnień do listy autoryzacji powoduje, że system operacyjny nadaje **temu użytkownikowi uprawnienia prywatne** do listy autoryzacji.

Listę autoryzacji można wykorzystać także do zdefiniowania uprawnień publicznych dla obiektów znajdujących się na liście. Jeśli uprawnienia publiczne do obiektu ustawione są na *AUTL, obiekt pobiera swoje uprawnienia publiczne ze swojej listy autoryzacji.

Obiekt listy autoryzacji używany jest przez system jako narzędzie zarządzania. Zazwyczaj zawiera ona listę wszystkich obiektów, które są chronione przez listę autoryzacji. Te informacje używane są do generowania ekranów do wyświetlania lub edytowania obiektów listy autoryzacji.

Listy autoryzacji nie można wykorzystać do zabezpieczania profilu użytkownika lub innej listy autoryzacji. Obiekt może mieć określoną tylko jedną listę autoryzacji.

Tylko właściciel obiektu, użytkownik z uprawnieniami specjalnymi do wszystkich obiektów (*ALLOBJ) lub użytkownik z uprawnieniami *ALL do obiektu może dodać lub usunąć listę autoryzacji dla obiektu.

Obiekty znajdujące się w bibliotece systemowej (QSYS) mogą być chronione za pomocą listy autoryzacji. Jednak nazwa listy autoryzacji, która chroni obiekt, przechowywana jest razem z obiektem. W niektórych przypadkach podczas instalowania nowego wydania systemu operacyjnego, zastępowane są wszystkie obiekty znajdujące się w bibliotece QSYS. Powiązania między obiektami i listą autoryzacji mogą być utracone.

Przykłady użycia list autoryzacji opisuje temat “Planowanie list autoryzacji” na stronie 217.

Zarządzanie listą autoryzacji

Do list autoryzacji można nadać specjalne uprawnienia operacyjne nazywane zarządzaniem listą autoryzacji (*AUTLMGT). Użytkownicy z uprawnieniami *AUTLMGT mają możliwość dodawania i usuwania uprawnień użytkownika z listy autoryzacji oraz zmieniania uprawnień dla tych użytkowników. Same uprawnienia *AUTLMGT nie dają uprawnień do zabezpieczania za pomocą listy nowych obiektów lub usuwania ich z listy.

Użytkownik z uprawnieniami *AUTLMGT może nadać tylko takie same uprawnienia lub mniejsze. Na przykład przyjmijmy, że UŻYTKOWNIK_A ma do listy autoryzacji CPLIST1 uprawnienia *CHANGE oraz *AUTLMGT. UŻYTKOWNIK_A może dodać do listy CPLIST1 UŻYTKOWNIKA_B i nadać mu uprawnienia *CHANGE lub mniejsze. UŻYTKOWNIK_A nie może nadać UŻYTKOWNIKOWI_B uprawnień *ALL, ponieważ ich nie posiada.

Użytkownik z uprawnieniami *AUTLMGT może usunąć uprawnienia użytkownika, jeśli użytkownik *AUTLMGT ma uprawnienia równe lub większe niż profil usuwanego użytkownika. Jeśli UŻYTKOWNIK_C ma do listy CPLIST1 uprawnienia *ALL, to UŻYTKOWNIK_A nie może usunąć go z listy, ponieważ ma jedynie uprawnienia *CHANGE i *AUTLMGT.

Używanie list autoryzacji do zabezpieczania obiektów IBM

Listę autoryzacji można wykorzystać do zabezpieczenia obiektów IBM. Na przykład używanie grupy komend można ograniczyć do kilku użytkowników.

Obiekty znajdujące się w bibliotekach IBM, innych niż QUSRSYS i QGPL, zastępowane są za każdym razem, gdy instalowane jest nowe wydanie systemu operacyjnego. Dlatego powiązania między obiektami znajdującymi się w bibliotekach IBM, a listami autoryzacji mogą zostać utracone. Podobnie jeśli lista autoryzacji zabezpiecza obiekt w bibliotece QSYS i przeprowadzane jest pełne odtwarzanie systemu, tracone jest powiązanie między obiektami znajdującymi się w bibliotece QSYS a listą autoryzacji. Po zainstalowaniu nowego wydania lub odtworzenia systemu należy użyć komendy EDTOBJAUT lub GRTOBJAUT w celu ponownego ustanowienia powiązania między obiektami IBM a listą autoryzacji.

Dokumentacja techniczna (redbook) *Implementation Guide for AS/400 Security and Auditing* zawiera przykładowe programy, takie jak ALLAUTL i FIXAUTL, które mogą zostać użyte do podłączania list autoryzacji do obiektów po odtworzeniu tych list.

Uprawnienia dla nowych obiektów w bibliotece

Każda biblioteka ma parametr CRTAUT (uprawnienia do tworzenia). Ten parametr określa domyślne uprawnienia publiczne dla każdego nowego obiektu, który jest tworzony w tej bibliotece. Podczas tworzenia obiektu parametr AUT komendy tworzącej określa uprawnienia publiczne dla obiektu. Jeśli wartość parametru AUT ustawiona jest na *LIBCRTAUT, która jest wartością domyślną, uprawnienia publiczne dla obiektu ustawiane są na wartość CRTAUT dla biblioteki.

Na przykład biblioteka CUSTLIB dla parametru CRTAUT ma wartość *USE. Obie wymienione poniżej komendy utworzą obszar danych nazwany DTA1 z uprawnieniami publicznymi *USE:

- Podawanie parametru AUT:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1) +
   TYPE(*CHAR) AUT(*LIBCRTAUT)
```

- Pozostawianie wartości domyślnej parametru AUT. Wartością domyślną jest *LIBCRTAUT:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1) +
   TYPE(*CHAR)
```

Wartością domyślną parametru CRTAUT dla biblioteki jest wartość *SYSVAL. Wszystkie nowe obiekty, tworzone w bibliotece z wykorzystaniem parametru AUT(*LIBCRTAUT), mają uprawnienia publiczne ustawiane na wartość podaną dla wartości systemowej QCRTAUT. Wartość systemowa QCRTAUT domyślnie ustawiona jest na *CHANGE. Na przykład parametr CRTAUT dla biblioteki ITEMLIB ma wartość *SYSVAL. Przedstawiona poniżej komenda tworzy obszar danych DTA2 z uprawnieniami publicznymi do zmiany:

```
CRTDTAARA DTAARA(ITEMLIB/DTA2) +
   TYPE(*CHAR) AUT(*LIBCRTAUT)
```

Sekcja “Przypisywanie uprawnień i prawa własności nowym obiektom” na stronie 124 zawiera więcej przykładów przypisywania przez system prawa własności oraz uprawnień do nowych obiektów.

Uwaga: Niektóre biblioteki IBM, w tym biblioteka QSYS, mają wartość systemową CRTAUT ustawioną na *SYSVAL. Jeśli wartość systemowa QCRTAUT zostanie zmieniona na inną niż *CHANGE, mogą wystąpić problemy. Na przykład urządzenia tworzone są w bibliotece QSYS. Wartością domyślną podczas tworzenia urządzeń jest wartość AUT(*LIBCRTAUT). Wartością parametru CRTAUT dla biblioteki QSYS jest *SYSVAL. Jeśli wartość systemowa QCRTAUT ustawiona jest na *USE lub *EXCLUDE, uprawnienia publiczne nie będą wystarczające do dodawania nowych urządzeń.

Jako wartość parametru CRTAUT dla biblioteki może być podana także nazwa listy autoryzacji. Nowy obiekt tworzony w bibliotece z parametrem AUT(*LIBCRTAUT) zabezpieczany jest przez listę autoryzacji. Uprawnienia publiczne do obiektu ustawiane są na *AUTL.

Wartość parametru CRTAUT dla biblioteki nie jest wykorzystywana podczas przenoszenia (MOVOBJ), tworzenia duplikatu (CRTDUPOBJ) lub odtwarzania obiektu w bibliotece. W tym celu wykorzystywane są uprawnienia publiczne istniejącego obiektu.

Jeśli w komendzie tworzenia podano parametr REPLACE (*YES), wtedy zamiast wartości parametru CRTAUT dla biblioteki, używane są uprawnienia istniejącego obiektu.

Ryzyko związane z Uprawnieniem do tworzenia (CRTAUT)

Jeśli aplikacje do tworzenia nowych obiektów wykorzystują uprawnienia domyślne, należy kontrolować uprawnienia do zmiany opisów bibliotek. Zmiana uprawnienia CRTAUT do biblioteki aplikacji może umożliwić dostęp bez uprawnień do nowych obiektów tworzonych w tej bibliotece.

Uprawnienia do nowych obiektów w katalogu

Podczas tworzenia nowego obiektu w katalogu za pomocą komend CRTDIR, MD lub MKDIR, należy podać publiczne uprawnienia do danych oraz do obiektu. Jeśli użyta zostanie opcja *INDIR, uprawnienia do tworzonego katalogu zostaną określone na podstawie uprawnień katalogu, w którym tworzony jest nowy katalog. W przeciwnym przypadku użytkownik podaje żądane uprawnienia.

Prawo własności do obiektu

Każdy obiekt podczas tworzenia otrzymuje właściciela. Właścicielem jest użytkownik, który tworzy obiekt lub profil grupowy, jeśli w profilu użytkownika określono, że to profil grupowy powinien być właścicielem obiektu. Podczas tworzenia obiektu, właściciel otrzymuje wszystkie uprawnienia do obiektu oraz do danych. W sekcji “Przypisywanie uprawnień i prawa własności nowym obiektom” na stronie 124 pokazano przykłady przypisywania przez system prawa własności do nowych obiektów.

Właściciel obiektu zawsze ma wszystkie uprawnienia do tego obiektu, chyba że jakieś lub wszystkie uprawnienia zostaną usunięte. Właściciel obiektu może usunąć niektóre uprawnienia w celach zapobiegawczych. Na przykład jeśli zbiór zawiera informacje krytyczne, użytkownik może usunąć uprawnienia do istnienia, w celu zapobiegnięcia przypadkowemu usunięciu tego zbioru. Jednak, jako właściciel obiektu, użytkownik w dowolnym momencie może nadać sobie dowolne uprawnienia.

Prawo własności do obiektu może być przeniesione z jednego użytkownika na innego. Prawo własności może być przeniesione na pojedynczy profil lub na profil grupowy. Profil grupowy może być właścicielem obiektów, gdy grupa ma członków.

Podczas zmiany właściciela obiektu można zachować lub odebrać uprawnienia poprzedniemu właścicielowi. Prawo własności może przenieść użytkownik z uprawnieniami *ALLOBJ, a także każdy inny użytkownik spełniający następujące warunki:

- mający uprawnienia do istnienia obiektu (z wyjątkiem uprawnień do listy autoryzacji),
- mający prawo własności do obiektu, jeśli obiekt znajduje się na liście autoryzacji,
- mający uprawnienie do dodawania do nowego profilu użytkownika właściciela,
- uprawnienia do usuwania do obecnego profilu właściciela.

Nie można usunąć profilu, który posiada obiekty. Przed usunięciem profilu najpierw należy przenieść prawo własności do obiektu na innego właściciela lub usunąć obiekt. Komenda Usunięcie profilu użytkownika (Delete User Profile - DLTUSRPRF) umożliwia obsługę posiadanych obiektów podczas usuwania profilu.

Prawo własności do obiektu system wykorzystuje jako narzędzie do zarządzania. Profil właściciela obiektu zawiera listę wszystkich użytkowników, którzy mają uprawnienia prywatne do obiektu. Te informacje używane są do tworzenia ekranów edycyjnych lub przeglądania uprawnień do obiektu.

Profile, do których należy wiele obiektów z wieloma uprawnieniami prywatnymi, mogą być bardzo duże. Wielkość profilu, który ma wiele obiektów, wpływa na szybkość wyświetlania uprawnień do obiektów i pracy z tymi uprawnieniami, a także składowania i odzyskiwania profili. Może to mieć także wpływ na wydajność całego systemu. Aby temu zapobiec, nie należy przypisywać obiektów tylko do jednego profilu właściciela w całym systemie iSeries. Każda aplikacja oraz obiekty aplikacji powinny być w posiadaniu oddzielnych profili. Także profile użytkowników IBM nie powinny posiadać danych lub obiektów użytkowników.

Właściciel obiektu wymaga także wystarczającej pamięci dla obiektu. Więcej informacji na ten temat zawiera sekcja “Pamięć maksymalna” na stronie 77.

Grupowe prawo własności do obiektów

Podczas tworzenia obiektu system sprawdza profil użytkownika tworzącego obiekt, aby określić prawa własności do tego obiektu. Jeśli użytkownik jest członkiem profilu grupowego, pole OWNER w jego profilu określa, czy to użytkownik, czy też grupa powinna być właścicielem nowego obiektu.

Jeśli grupa posiada obiekt (parametr OWNER ma wartość *GRPPRF), użytkownik tworzący obiekt nie otrzymuje automatycznie uprawnień szczegółowych do tego obiektu. Użytkownik dostaje uprawnienia do obiektu za pośrednictwem grupy. Jeśli użytkownik posiada obiekt (parametr OWNER ma wartość *USRPRF), uprawnienia grupowe do obiektu określane są przez pole GRPAUT tego profilu użytkownika.

Pole *Typ uprawnień grupowych* (GRPAUTTYP) w profilu użytkownika określa, czy grupa 1) staje się grupą podstawową dla obiektu, czy 2) ma nadane uprawnienia prywatne do tego obiektu. W sekcji “Przypisywanie uprawnień i prawa własności nowym obiektom” na stronie 124 przedstawiono kilka przykładów.

Jeśli użytkownik, który posiada obiekt, zmieni swoją grupę, początkowy profil grupowy nadal zachowuje uprawnienia do utworzonych obiektów.

Nawet jeśli pole *Właściciel* w profilu użytkownika ma wartość *GRPPRF, użytkownik nadal musi mieć wystarczającą pamięć, aby przechowywać nowe obiekty podczas ich tworzenia. Po ich utworzeniu prawo własności przenoszone jest na profil grupowy. Parametr MAXSTG w profilu użytkownika określa, ile użytkownik ma dostępnej pamięci dyskowej.

Podczas wybierania między prawem własności dla grupy i dla pojedynczego użytkownika, należy przeanalizować obiekty, które użytkownik może tworzyć, takie jak programy zapytania:

- Jeśli użytkownik przechodzi do innego wydziału lub innej grupy użytkowników, to czy powinien nadal posiadać dane obiekty?
- Czy ważne jest, kto tworzy obiekty? Na ekranach uprawnień do obiektu wyświetlany jest właściciel obiektu, a nie użytkownik, który go utworzył.

  Uwaga: Na ekranie Wyświetlenie opisu obiektu (Display Object Description) wyświetlany jest twórca obiektu.

  Jeśli funkcja kroniki kontroli jest aktywna, podczas tworzenia obiektu w kronice kontroli QAUDJRN zapisywana jest pozycja tworzenia obiektu (CO). Ta pozycja identyfikuje profil użytkownika tworzącego obiekt. Pozycja zapisywana jest tylko wtedy, gdy wartość systemowa QAUDLVL jest równa *CREATE, a wartość systemowa QAUDCTL zawiera wartość *AUDLVL.

Grupa podstawowa dla obiektu

Dla obiektu można określić grupę podstawową. Nazwa profilu grupy podstawowej oraz uprawnień grupy podstawowej do obiektu przechowywane są razem z obiektem. Korzystanie z uprawnień grupy podstawowej może zapewnić lepszą wydajność podczas sprawdzania uprawnień niż prywatne uprawnienia grupowe.

Aby profil mógł być przypisany jako grupa podstawowa, musi być profilem grupowym (musi mieć identyfikator gid). Ten sam profil nie może być równocześnie właścicielem i grupą podstawową obiektu.

Gdy użytkownik tworzy nowy obiekt, parametry jego profilu określają, czy grupa użytkownika otrzymuje uprawnienia do obiektu oraz jakie to są uprawnienia. Parametr *Typ uprawnień grupowych* (GRPAUTTYP) profilu użytkownika może być użyty do utworzenia grupy użytkownika jako grupy podstawowej dla obiektu. Sekcja “Przypisywanie uprawnień i prawa własności nowym obiektom” na stronie 124 zawiera przykłady sposobu przypisywania uprawnień podczas tworzenia nowych obiektów.

Aby określić grupę podstawową dla obiektu, należy użyć komendy Zmiana grupy podstawowej obiektu (Change Object Primary Group - CHGOBJPGP) lub Praca z obiektami wg grupy podstawowej (Work with Objects by Primary Group - WRKOBJPGP). Za pomocą ekranu Edycja uprawnień dla obiektu (Edit Object Authority) lub komend nadawania i odbierania uprawnień można zmienić uprawnienia grupy podstawowej.

Profil użytkownika domyślnego właściciela (QDFTOWN)

Profil użytkownika domyślnego właściciela (QDFTOWN) jest profilem użytkownika IBM, który jest używany, gdy obiekt nie ma właściciela lub gdy prawo własności może spowodować ryzyko naruszenia ochrony. Poniżej przedstawiono sytuacje mogące powodować przypisanie prawa własności do obiektu profilowi QDFTOWN:

- jeśli profil właściciela zostanie uszkodzony lub usunięty, jego obiekty nie będą miały już właściciela; użycie komendy Odzyskiwanie pamięci (Reclaim Storage - RCLSTG) przypisuje prawo własności do tych obiektów profilowi użytkownika domyślnego właściciela (QDFTOWN),
- jeśli obiekt jest odtwarzany, a profil właściciela nie istnieje,
- jeśli odtwarzany jest program wymagający ponownego utworzenia, ale jego utworzenie nie powiedzie się; więcej informacji na temat warunków powodujących przypisanie prawa własności do profilu QDFTOWN zawiera temat “Sprawdzanie odtwarzanych programów” na stronie 15,
- jeśli dla profilu użytkownika, który jest właścicielem magazynu uprawnień, który ma taką samą nazwę jak przenoszony zbiór, zmieniana nazwa zbioru lub zmieniana nazwa biblioteki tego zbioru lub przekroczony zostanie limit pamięci.

Profil użytkownika QDFTOWN znajduje się w systemie dlatego, że każdy obiekt musi mieć właściciela. Gdy system jest dostarczany, tylko użytkownik z uprawnieniami specjalnymi *ALLOBJ może wyświetlić i uzyskać dostęp do tego profilu oraz przenieść prawa własności do obiektów związanych z profilem użytkownika QDFTOWN. Profilowi QDFTOWN można nadać również inne uprawnienia użytkownika. Profil użytkownika QDFTOWN przeznaczony jest tylko do użytku systemowego. Nie należy projektować ochrony tak, żeby profil QDFTOWN posiadał obiekty.

Przypisywanie uprawnień i prawa własności nowym obiektom

Do przypisywania uprawnień oraz prawa własności podczas tworzenia nowego obiektu, system korzysta z kilku wartości:

parametrów komendy CRTxxx,

wartości systemowej QCRTAUT,

wartości CRTAUT biblioteki,

wartości w profilu użytkownika tworzącego.

Rysunki od Rys. 6 do Rys. 9 prezentują kilka przykładów używania tych wartości:

Wartość systemowa QCRTAUT:
*CHANGE

Parametr CRTAUT biblioteki:
*USE

Wartości w profilu USERA (tworzącego):

GRPPRF:
DPT806

OWNER:
*USRPRF

GRPAUT:
*CHANGE

GRPAUTTYP:
*PRIVATE

Komenda użyta do tworzenia obiektu:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
        TYPE(*CHAR) AUT(*LIBCRTAUT)
```

albo

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
   TYPE(*CHAR)
```

Wartości dla nowego obiektu:

Uprawnienia publiczne:
*USE

Uprawnienia właściciela:
USERA *ALL

Uprawnienia grupy podstawowej:
Brak

Uprawnienia prywatne:
DPT806 *CHANGE

Uwaga:

Wartość *LIBCRTAUT jest wartością domyślną parametru AUT dla większości komend CRTxxx.

Rysunek 6. Przykład nowego obiektu: uprawnienia publiczne z biblioteki, grupa ma nadane uprawnienia prywatne

Wartość systemowa QCRTAUT:
*CHANGE

Parametr CRTAUT biblioteki:
*SYSVAL

Wartości w profilu USERA (tworzącego):

GRPPRF:
DPT806

OWNER:
*USRPRF

GRPAUT:
*CHANGE

GRPAUTTYP:
*PRIVATE

Komenda użyta do tworzenia obiektu:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
        TYPE(*CHAR) AUT(*LIBCRTAUT)
```

Wartości dla nowego obiektu:

Uprawnienia publiczne:
*CHANGE

Uprawnienia właściciela:
USERA *ALL

Uprawnienia grupy podstawowej:
Brak

Uprawnienia prywatne:
DPT806 *CHANGE

Rysunek 7. Przykład nowego obiektu: uprawnienia publiczne z wartości systemowej, grupa ma nadane uprawnienia prywatne

Wartość systemowa QCRTAUT:
*CHANGE

Parametr CRTAUT biblioteki:
*USE

Wartości w profilu USERA (tworzącego):

GRPPRF:
DPT806

OWNER:
*USRPRF

GRPAUT:
*CHANGE

GRPAUTTYP:
*PGP

Komenda użyta do tworzenia obiektu:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
        TYPE(*CHAR) AUT(*LIBCRTAUT)
```

Wartości dla nowego obiektu:

Uprawnienia publiczne:
*USE

Uprawnienia właściciela:
USERA *ALL

Uprawnienia grupy podstawowej:
DPT806 *CHANGE

Uprawnienia prywatne:
Brak

Rysunek 8. Przykład nowego obiektu: uprawnienia publiczne z biblioteki, grupa ma nadane uprawnienia grupy podstawowej

Wartość systemowa QCRTAUT:
*CHANGE

Parametr CRTAUT biblioteki:
*USE

Wartości w profilu USERA (tworzącego):

GRPPRF:
DPT806

OWNER:
*GRPPRF

GRPAUT:

GRPAUTTYP:

Komenda użyta do tworzenia obiektu:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
        TYPE(*CHAR) AUT(*CHANGE)
```

Wartości dla nowego obiektu:

Uprawnienia publiczne:
*CHANGE

Uprawnienia właściciela:
DPT806 *ALL

Uprawnienia grupy podstawowej:
Brak

Uprawnienia prywatne:
Brak

Rysunek 9. Przykład nowego obiektu: uprawnienia publiczne są podane, grupa posiada obiekt

Obiekty, które adoptują uprawnienia właściciela

W zależności od sytuacji, czasami użytkownik potrzebuje różnych uprawnień do obiektu lub do aplikacji. Na przykład może być uprawniony do zmiany informacji w zbiorze klienta podczas korzystania z aplikacji udostępniających tę funkcję. Jednak ten sam użytkownik podczas korzystania z narzędzia wspomagającego decyzje, takiego jak SQL, może tylko przeglądać, a nie zmieniać informacje o kliencie.

Rozwiązaniem tej sytuacji jest 1) nadanie użytkownikowi uprawnień *USE do informacji o kliencie, aby umożliwić tworzenie zapytań i 2) użycie uprawnień adoptowanych w programach obsługi klienta, aby umożliwić użytkownikowi zmianę zbiorów.

Gdy obiekt korzysta z uprawnień właściciela, jest to nazywane **adoptowaniem uprawnień**. Uprawnienia mogą adoptować obiekty typu *PGM, *SRVPGM, *SQLPKG i programy Java.

Podczas tworzenia programu, w komendzie CRTxxxPGM należy podać parametr profil użytkownika (USRPRF). Ten parametr określa, czy oprócz uprawnień użytkownika uruchamiającego program, korzysta on z uprawnień właściciela.

W Centrum informacyjnym znajdują się uwagi dotyczące ochrony oraz uprawnień adoptowanych podczas korzystania z pakietów SQL (patrz sekcja “Informacje wstępne i pokrewne” na stronie xvi).

Do uprawnień adoptowanych mają zastosowanie następujące reguły:

- uprawnienia adoptowane dodawane są do pozostałych uprawnień użytkownika,
- uprawnienia adoptowane są sprawdzane tylko jeśli uprawnienia, które ma użytkownik, grupa użytkowników lub użytkownicy publiczni nie są wystarczające dla żądanej operacji,
- uprawnienia specjalne (takie jak *ALLOBJ) profilu użytkownika są używane,
- jeśli profil właściciela jest członkiem profilu grupowego, uprawnienia grupowe *nie* są używane jako uprawnienia adoptowane,
- uprawnienia publiczne *nie* są używane dla uprawnień adoptowanych; na przykład UŻYTKOWNIK1 uruchamia program LSTCUST, który wymaga uprawnień *USE do zbioru CUSTMST:
  - uprawnienia publiczne do zbioru CUSTMST to *USE,
  - uprawnienia UŻYTKOWNIKA1 to *EXCLUDE,
  - program LSTCUST, który adoptuje uprawnienia właściciela, należy do UŻYTKOWNIKA1,
  - UŻYTKOWNIK2 nie posiada zbioru CUSTMST i nie ma do niego uprawnień prywatnych,
  - chociaż uprawnienia publiczne są wystarczające, aby UŻYTKOWNIK2 uzyskał dostęp do zbioru CUSTMST, UŻYTKOWNIK1 nie uzyska takiego dostępu; uprawnienia właściciela, grupy podstawowej oraz uprawnienia prywatne używane są jako uprawnienia adoptowane,
  - adoptowane są tylko uprawnienia; inne atrybuty profilu użytkownika nie są adoptowane; na przykład nie są adoptowane atrybuty ograniczonych możliwości.
- uprawnienia adoptowane są aktywne tak długo, jak długo program korzystający z tych uprawnień pozostaje na stosie programów; na przykład program PGMA korzysta z uprawnień adoptowanych:
  - jeśli program PGMA uruchamia program PGMB korzystając z komendy CALL, stosy przed i po wywołaniu komendy CALL, wyglądają następująco:

Stos programów przed wywołaniem komendy CALL:	**Stos programów po wywołaniu komendy CALL:**
QCMD : : PGMA	QCMD : : PGMA PGMB

Rysunek 10. Uprawnienia adoptowane i komenda CALL

    ponieważ program PGMA pozostaje na stosie po wywołaniu programu PGMB, to program PGMB korzysta z uprawnień adoptowanych programu PGMA; (wykorzystanie parametru użycia uprawnień adoptowanych (USEADPAUT) może to przesłonić; więcej informacji na temat parametru USEADPAUT zawiera sekcja “Programy, które ignorują uprawnienia adoptowane” na stronie 131),
  - jeśli program PGMA uruchamia program PGMB za pomocą komendy Kontrola transferu (Transfer Control - TFRCTL), stos programów wygląda następująco:

Stos programów przed wywołaniem komendy TFRCTL:	**Stos programów po wywołaniu komendy TFRCTL:**
QCMD : : PGMA	QCMD : : PGMB

Rysunek 11. Uprawnienia adoptowane i komenda TFRCTL

    program PGMB nie korzysta z uprawnień adoptowanych programu PGMA, ponieważ program PGMA został zdjęty ze stosu.
- jeśli progam uruchamiany z uprawnieniami adoptowanymi zostanie przerwany, użycie tych uprawnień zostanie zawieszone; przedstawione poniżej funkcje nie korzystają z uprawnień adoptowanych:
  - żądanie systemowe,

– klawisz ATTN (jeśli uruchomiona jest komenda Transfer do zadania grupowego (Transfer to Group Job - TFRGRPJOB), uprawnienia adoptowane nie są przekazywane do zadania grupowego),
– program obsługi komunikatu przerywającego,
– funkcje debugowania.

Uwaga: Uprawnienia adoptowane są natychmiast przerywane przez klawisz ATTN lub żądanie zadania grupowego. Użytkownik musi mieć uprawnienia do programu obsługi klawisza ATTN lub programu początkowego zadania grupowego, w przeciwnym przypadku próba nie powiedzie się.

na przykład UŻYTKOWNIK_A uruchamia program PGM1, który adoptuje uprawnienia UŻYTKOWNIKA_B; program PGM1 korzysta z komendy SETATNPGM i podaje program PGM2; UŻYTKOWNIK_B do programu PGM2 ma uprawnienia *USE; natomiast UŻYTKOWNIK_A ma uprawnienia *EXCLUDE; funkcja SETATNPGM zostanie wykonana pomyślnie, ponieważ uruchamiana jest z wykorzystaniem uprawnień adoptowanych; podczas próby użycia przez UŻYTKOWNIKA_A klawisza ATTN otrzyma on błąd uprawnień, ponieważ uprawnienia UŻYTKOWNIKA_B nie będą już aktywne.

- jeśli program korzystający z uprawnień adoptowanych wprowadza zadanie, to takie zadanie nie ma uprawnień adoptowanych,
- gdy wywoływany jest program wyzwalany lub program obsługi wyjścia, uprawnienia adoptowane z poprzedniego programu ze stosu wywołań nie będą używane jako źródło uprawnień dla programu wyzwalanego lub programu obsługi wyjścia,
- podczas używania komendy Zmiana zadania (Change Job - CHGJOB) w celu zmiany kolejki wyjściowej dla zadania, funkcja adoptowania programu nie jest używana; profil użytkownika dokonującego zmiany musi mieć uprawnienia do nowej kolejki wyjściowej,
- każdy tworzony obiekt, także zbiory buforowe, które mogą zawierać poufne dane, należą do użytkownika programu lub profilu grupowego, a nie do właściciela programu,
- uprawnienia adoptowane mogą być określone w komendzie, która tworzy program (CRTxxxPGM) lub komendzie Zmiana programu (Change Program - CHGPGM),
- jeśli program tworzony jest z wykorzystaniem parametru REPLACE(*YES) w komendzie CRTxxxPGM, nowa kopia programu ma takie same wartości parametrów USRPRF, USEADPAUT i AUT, jakie miał zastępowany program; parametry USRPRF i AUT podane w komendzie CRTxxxPGM są ignorowane,
- gdy w początkowym programem podany jest parametr USRPRF(*OWNER), tylko właściciel programu może podać parametr REPLACE(*YES) w komendzie CRTxxxPGM,
- tylko użytkownik, który posiada program lub ma uprawnienia specjalne *ALLOBJ i *SECADM, może zmienić wartość parametru USRPRF,
- aby przenieść prawo własności do obiektu, który adoptuje uprawnienia, użytkownik musi być wpisany jako użytkownik z uprawnieniami specjalnymi *ALLOBJ i *SECADM,
- jeśli program adoptujący uprawnienia odtwarzany jest przez użytkownika, który nie jest właścicielem programu lub nie ma uprawnień specjalnych *ALLOBJ i *SECADM, wszystkie uprawnienia prywatne i publiczne do programu są odbierane, w celu zabezpieczenia przed potencjalnym ryzykiem naruszenia ochrony.

Komendy Wyświetlenie programu (Display Program - DSPPGM) oraz Wyświetlenie programu usługowego (Display Service Program - DSPSRVPGM) pokazują, czy program adoptuje uprawnienia (pole *Profil użytkownika*) i czy używają uprawnień adoptowanych z poprzedniego programu na stosie programów (pole *Użycie uprawnień adoptowanych*). Komenda Wyświetlenie adopcji programu (Display Program Adopt - DSPPGMADP) wyświetla wszystkie obiekty, które adoptują uprawnienia danego profilu użytkownika. Komenda Drukowanie obiektów adoptujących (Print Adopting Objects - PRTADPOBJ) udostępnia raport zawierający więcej informacji dotyczących obiektów, które adoptują uprawnienia. Ta komenda udostępnia także opcję drukowania raportu dla obiektów, które zmieniły się od czasu poprzedniego uruchomienia.

“Schemat blokowy 8: Jak sprawdzane są uprawnienia adoptowane” na stronie 162 udostępnia więcej informacji dotyczących uprawnień adoptowanych. Temat “Używanie uprawnień adoptowanych w projekcie menu” na stronie 208 pokazuje przykład sposobu użycia uprawnień adoptowanych w aplikacji.

Uprawnienia adoptowane a programy skonsolidowane:

Program ILE* (*PGM) jest obiektem, który zawiera jeden lub więcej modułów. Tworzony jest przez kompilator ILE*. Program ILE może być skonsolidowany z jednym lub większą ilością programów usługowych (*SRVPGM).

Aby pomyślnie aktywować program ILE, użytkownik musi mieć uprawnienia *EXECUTE do programu ILE oraz wszystkich programów usługowych, z którym program jest skonsolidowany. Jeśli program ILE korzysta z uprawnień adoptowanych od programu znajdującego się wyżej na stosie wywołań programu, te uprawnienia **są** używane do sprawdzenia uprawnień do wszystkich programów usługowych, z którymi skonsolidowany jest program ILE. Jeśli program ILE adoptuje uprawnienia, to te uprawnienia nie będą sprawdzane podczas sprawdzania przez system uprawnień użytkownika do programów usługowych podczas ich aktywacji.

Ryzyko związane z uprawnieniami adoptowanymi i zalecenia

Umożliwienie uruchamiania programu z uprawnieniami adoptowanymi jest zamierzonym pozbawieniem kontroli. Umożliwia to użytkownikowi uzyskanie uprawnień do obiektów oraz możliwe uzyskanie uprawnień specjalnych, których użytkownik zwykle może nie mieć. Uprawnienia adoptowane udostępniają ważne narzędzie do spełnienia różnych wymagań dotyczących uprawnień, ale musi być ono używane ze szczególną ostrożnością:

- należy adoptować minimalne uprawnienia, tak aby spełnić wymagania aplikacji; zamiast adoptowania uprawnień użytkownika QSECOFR lub użytkownika z uprawnieniami specjalnymi *ALLOBJ preferowane jest adoptowanie uprawnień właściciela aplikacji,
- należy uważnie moniotorwać funkcje udostępniane przez programy, które adoptują uprawnienia; należy upewnić się, że te programy nie udostępniają użytkownikom sposobów na dostęp do obiektów poza kontrolą programu, takiego jak możliwość wprowadzenia komendy,
- programy, które adoptują uprawnienia oraz pozostałe wywoływane programy muszą wykonać kwalifikowane wywoływanie biblioteki; w tym celu nie należy używać listy bibliotek (*LIBL),
- należy kontrolować, którzy użytkownicy mają pozwolenie na wywoływanie programów adoptujących uprawnienia; aby zapobiec wywoływaniu tych programów bez wystarczającej kontroli, należy użyć interfejsów menu oraz ochrony biblioteki.

Programy, które ignorują uprawnienia adoptowane

Użytkownik może nie chcieć, aby niektóre programy używały uprawnień adoptowanych poprzednich programów ze stosu programów. Na przykład jeśli używany jest program menu początkowego, który adoptuje uprawnienia właściciela, użytkownik może nie chcieć, aby niektóre programy wywoływane z menu programu używały tych uprawnień.

Użycie parametru adoptowania uprawnień (USEADPAUT) programu określa, czy system podczas sprawdzania uprawnień do obiektów używa uprawnień adoptowanych poprzedniego programu ze stosu.

Podczas tworzenia programu domyślną wartością jest używanie uprawnień adoptowanych z poprzedniego programu ze stosu. Jeśli użytkownik nie chce, aby używane były uprawnienia adoptowane, może zmienić program korzystając z komendy Zmiana programu (Change Program - CHGPGM) lub Zmiana programu usługowego (Change Service Program - CHGSRVPGM), w celu ustawienia parametru USEADPAUT na *NO. Jeśli program tworzony jest z wykorzystaniem parametru REPLACE(*YES) w komendzie CRTxxxPGM, nowa kopia programu ma takie same wartości parametrów USRPRF, USEADPAUT i AUT, jakie miał zastępowany program.

Temat “Ignorowanie uprawnień adoptowanych” na stronie 210 zawiera przykład sposobu użycia tego parametru w projekcie menu. Więcej informacji na temat wartości systemowej QUSEADPAUT znajduje się w temacie “Użycie uprawnień adoptowanych (QUSEADPAUT)” na stronie 30.

Uwaga: W niektórych sytuacjach, aby zapobiec przekazywaniu uprawnień adoptowanych do wywoływanych funkcji, można użyć instrukcji MI MODINVAU. Instrukcja MODINVAU może być użyta do zabezpieczenia przed przekazywaniem uprawnień adoptowanych z programów C i C++ do wywoływanych funkcji w innym programie lub programie usługowym. Może to być użyteczne gdy nie jest znane ustawienie parametru USEADPAUT dla wywoływanej funkcji.

Magazyny uprawnień

Magazyn uprawnień jest narzędziem do przechowywania uprawnień do zbiorów bazy danych opisanych przez program, które aktualnie nie istnieją w systemie. Jego podstawowym przeznaczeniem jest użycie w aplikacjach środowiska System/36, które często usuwa zbiory opisane przez program, a następnie tworzy je ponownie.

Magazyn uprawnień może być utworzony za pomocą komendy Tworzenie magazynu uprawnień (Create Authority Holder - CRTAUTHLR) dla zbioru, który już istnieje lub dla zbioru, który jeszcze nie istnieje. Dla magazynów uprawnień mają zastosowanie następujące reguły:

- magazyny uprawnień mogą zabezpieczać tylko zbiory w systemowej puli pamięci dyskowej (ASP) lub podstawowej puli ASP użytkownika; nie mogą zabezpieczać zbiorów z niezależnej puli ASP,
- magazyn uprawnień powiązany jest z określonym zbiorem i biblioteką; ma taką samą nazwę, jak zbiór,
- magazyny uprawnień mogą być użyte tylko dla zbiorów bazy danych opisanych przez program oraz zbiorów logicznych tworzonych w środowisku S/36,
- po utworzeniu magazynu uprawnień można do niego dodawać uprawnienia w taki sam sposób, jak do zbioru; w tym celu należy używać komend do nadawania odbierania i wyświetlania uprawnień do obiektów oraz podawać typ obiektu *FILE; na ekranach uprawnień do obiektu magazyn uprawnień nie jest odróżnialny od samego zbioru; ekrany nie wskazują, czy zbiór istnieje ani czy dany zbiór ma magazyn uprawnień,
- jeśli zbiór związany jest z magazynem uprawnień, podczas sprawdzania uprawnień użyte będą uprawnienia zdefiniowane dla magazynu uprawnień; wszystkie uprawnienia prywatne zdefiniowane dla zbioru są ignorowane,
- do wyświetlenia lub drukowania wszystkich magazynów uprawnień w systemie, należy użyć komendy Wyświetlenie magazynu uprawnień (Display Authority Holder - DSPAUTHLR); można jej użyć także do utworzenia zbioru wyjściowego (Outfile) do przetwarzania,
- jeśli magazyn uprawnień tworzony jest dla zbioru, który już istnieje:
  - użytkownik tworzący magazyn uprawnień musi mieć uprawnienia *ALL do zbioru,
  - właściciel zbioru staje się właścicielem magazynu uprawnień, bez względu na to, kto tworzy magazyn uprawnień,
  - uprawnienia publiczne do magazynu uprawnień pochodzą ze zbioru; parametr uprawnień publicznych (AUT) komendy CRTAUTHLR jest ignorowany,
  - istniejące uprawnienia do zbioru kopiowane są do magazynu uprawnień.
- jeśli zbiór jest tworzony, a magazyn uprawnień do tego zbioru już istnieje:
  - użytkownik tworzący zbiór musi mieć uprawnienia *ALL do magazynu uprawnień,
  - właściciel magazynu uprawnień staje się właścicielem zbioru, bez względu na to, kto tworzy zbiór,
  - uprawnienia publiczne do zbioru pochodzą z magazynu uprawnień; parametr uprawnień publicznych (AUT) komendy CRTPF lub CRTLF jest ignorowany,
  - magazyn uprawnień jest dowiązywany do zbioru; uprawnienia podane dla magazynu uprawnień używane są do zabezpieczania zbioru.
- jeśli magazyn uprawnień jest usuwany, informacje o uprawnieniach przekazywane są do samego zbioru,
- jeśli zmieniana jest nazwa zbioru, a nowa nazwa jest taka sama, jak nazwa istniejącego magazynu uprawnień, uprawnienia i prawo własności do zbioru zmieniane są tak, aby były zgodne z magazynem uprawnień; użytkownik zmieniający nazwę zbioru musi mieć uprawnienia *ALL do magazynu uprawnień,
- jeśli zbiór jest przenoszony do innej biblioteki, a dla takiej nazwy zbioru oraz biblioteki docelowej istnieje magazyn uprawnień, uprawnienia oraz prawo własności do zbioru zmieniane są tak, aby były zgodne z magazynem uprawnień; użytkownik przenoszący zbiór musi mieć uprawnienia *ALL do magazynu uprawnień,
- prawo własności magazynu uprawnień oraz zbioru zawsze są zgodne; jeśli zmieniane jest prawo własności do zbioru, zmieniane jest także prawo własności do magazynu uprawnień,
- gdy zbiór jest odtwarzany, a dla takiej nazwy zbioru oraz biblioteki, w której jest odtwarzany, istnieje magazyn uprawnień, zbiór jest dowiązywany do tego magazynu uprawnień,
- magazyny uprawnień nie mogą być tworzone dla zbiorów w następujących bibliotekach: QSYS, QRCL, QRECOVERY, QSPL, QTEMP i QSPL0002 – QSPL0032.

Magazyny uprawnień i migrowanie z System/36

Funkcja Migration Aid systemu System/36 tworzy magazyn uprawnień dla każdego zbioru, który jest przenoszony. Tworzy także magazyn uprawnień dla pozycji zbioru ochrony zasobów System/36, jeśli w systemie System/36 nie istnieje odpowiadający mu zbiór.

Magazyn uprawnień wymagany jest jedynie dla zbiorów, które są usuwane i tworzone ponownie przez aplikacje użytkownika. Aby usunąć niepotrzebne magazyny uprawnień, należy użyć komendy Usunięcie magazynu uprawnień (Delete Authority Holder - DLTAUTHLR).

Ryzyko związane z magazynem uprawnień

Magazyn uprawnień udostępnia możliwość definiowania uprawnień do zbioru, zanim on jeszcze powstanie. W określonych okolicznościach może to umożliwić dostęp do tych informacji użytkownikowi bez uprawnień. Jeśli użytkownik wie, że aplikacja może utworzyć, przenieść lub zmienić nazwę zbioru, to może utworzyć magazyn uprawnień dla nowego zbioru. A zatem użytkownik uzyska dostęp do zbioru.

Aby ograniczyć to ryzyko, komenda CRTAUTHLR dostarczana jest z uprawnieniami *EXCLUDE. Tylko użytkownicy z uprawnieniami *ALLOBJ mogą korzystać z tej komendy, chyba że zostanie nadane do niej uprawnienie.

Praca z uprawnieniami

Ten fragment rozdziału opisuje najczęściej używane metody konfigurowania, obsługiwania i wyświetlania informacji o uprawnieniach dotyczących systemu. Dodatek A, “Komendy ochrony”, na stronie 273 udostępnia pełną listę komend dostępnych do pracy z uprawnieniami. Poniższe opisy nie omawiają wszystkich parametrów komend lub pól na ekranach. Wszystkie szczegóły zawierają informacje elektroniczne.

Ekrany uprawnień

Uprawnienia do obiektów pokazują cztery ekrany:

- Wyświetlenie uprawnień dla obiektu, ekran
- Edycja uprawnień dla obiektu, ekran
- Ekran Wyświetlenie uprawnień (Display Authority),
- Ekran Praca z uprawnieniami (Work with Authority).

Ta sekcja opisuje niektóre parametry tych ekranów. Rys. 12 na stronie 134 pokazuje podstawową wersję ekranu Wyświetlenie uprawnień dla obiektu (Display Object Authority):

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   CUSTNO    Właściciel . . . . . :   PGMR1
  Biblioteka . . . :   CUSTLIB   Grupa podstawowa . . :   DPTAR
Typ obiektu  . . . :   *DTAARA   Urządzenie ASP . . . :   *SYSBAS

Obiekt chroniony listą autoryzacji  . . . . . :   *NONE

                       Uprawnienia
Użytkownik  Grupa      do obiektu
*PUBLIC                *EXCLUDE
PGMR1                  *ALL
DPTAR                  *CHANGE
DPTSM                  *USE
F3=Wyjście F11=Szczegółowe uprawnienia do obiektu F12=Anuluj
F17=Początek
```

Rysunek 12. Ekran Wyświetlenie uprawnień dla obiektu (Display Object Authority)

Na tym ekranie prezentowane są nazwy systemowe uprawnień. Klawisz F11 działa jako przełącznik między tym, a dwoma innymi wersjami ekranu. Jedna z nich opisuje szczegółowe uprawnienia do obiektu:

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   CUSTNO       Właściciel . . . . . :   PGMR1
  Biblioteka . . . :   CUSTLIB      Grupa podstawowa . . :   DPTAR
Typ obiektu  . . . :   *DTAARA        Urządzenie ASP . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji . . . . . :   *NONE

                       Upr. do   ----------Obiekt-----------
Użytkownik  Grupa      obiektu    Oper Zarz.Istn. Zmian. Odn.
*PUBLIC                *EXCLUDE    X
PGMR1                  *ALL        X    X     X      X     X
DPTAR                  *CHANGE     X
DPTSM                  *USE        X
   :
F3=Wyjście F11=Uprawnienia do danych F12=Anuluj  F17=Początek
F18=Koniec
```

Pozostały ekran opisuje uprawnienia do danych:

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   CUSTNO      Właściciel . . . . . :   PGMR1
  Biblioteka . . . :   CUSTLIB     Grupa podstawowa . . :   DPTAR
Typ obiektu  . . . :   *DTAARA     Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji . . . . . :   *NONE

                       Upr. do    ---------------Dane---------------
Użytkownik  Grupa      obiektu   Odczyt Dod. Aktual. Usuw.  Wykonyw.
*PUBLIC                *EXCLUDE
PGMR1                  *ALL        X     X     X       X       X
DPTAR                  *CHANGE     X     X     X       X       X
DPTSM                  *USE        X                           X
```

Jeśli użytkownik ma do obiektu uprawnienia *OBJMGT, widzi wszystkie uprawnienia prywatne do tego obiektu. Jeśli nie ma uprawnień *OBJMGT, widzi tylko własne źródła uprawnień do obiektu.

Na przykład jeśli UŻYTKOWNIK_A wyświetla uprawnienia do obszaru danych CUSTNO, prezentowane są jedynie uprawnienia publiczne.

Jeśli UŻYTKOWNIK_B, który jest członkiem profilu grupowego DPTAR, wyświetla uprawnienia do obszaru danych CUSTNO, ekran będzie wyglądał następująco:

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   CUSTNO      Właściciel . . . . . :   PGMR1
  Biblioteka . . . :   CUSTLIB     Grupa podstawowa . . :   DPTAR
Typ obiektu  . . . :   *DTAARA     Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji . . . . . :   *NONE

                       Uprawnienia
Użytkownik  Grupa      do obiektu
*GROUP      DPTAR      *CHANGE
```

Jeśli UŻYTKOWNIK_B uruchamia program, który adoptuje uprawnienia programu PGMR1 i wyświetla uprawnienia dla obszaru danych CUSTNO, ekran wygląda następująco:

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt  . . . . . :   CUSTNO      Właściciel . . . . . :   PGMR1
  Biblioteka  . . . :   CUSTLIB     Grupa podstawowa . . :   DPTAR
Typ obiektu . . . . :   *DTAARA     Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji  . . . . . :   *NONE

                       Uprawnienia
Użytkownik  Grupa      do obiektu
*ADOPTED               USER DEF
*PUBLIC                *EXCLUDE
PGMR1                  *ALL
*GROUP      DPTAR      *CHANGE
DPTSM                  *USE
```

Uprawnienia *ADOPTED oznaczają tylko dodatkowe uprawnienia otrzymane od właściciela programu. UŻYTKOWNIK_B z programu PGMR1 otrzymuje wszystkie uprawnienia, które nie są zawarte w uprawnieniach *CHANGE. Ekran pokazuje wszystkie uprawnienia prywatne, ponieważ UŻYTKOWNIK_B adoptuje *OBJMGT. Ekran szczegółowy wygląda następująco:

```
                   Wyświetlenie uprawnień dla obiektu
                      (Display Object Authority)
Obiekt . . . . . :   CUSTNO       Właściciel . . . . . :   PGMR1
  Biblioteka . . . :   CUSTLIB      Grupa podstawowa . . :   DPTAR
Typ obiektu . . . . :   *DTAARA     Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji  . . . . . :   *NONE

                        Upr. do    -----------Obiekt-----------
Użytkownik  Grupa       obiektu    Oper Zarz.Istn. Zmian. Odn.
*ADOPTED                USER DEF         X     X      X     X
*PUBLIC                 *EXCLUDEPGMR1
                        *ALL        X    X     X      X     X
*GROUP     DPTAR        *CHANGE     X
DPTSM                   *USE        X
F3=Wyjście F11=Uprawnienia do danych F12=Anuluj  F17=Początek
F18=Koniec
```

Jeśli pole opcji użytkownika (USROPT) w profilu użytkownika UŻYTKOWNIK_B ma wartość *EXPERT, ekran wygląda następująco:

```
                    Wyświetlenie uprawnień dla obiektu
                       (Display Object Authority)
Obiekt . . . . . :   CUSTNO     Właściciel . . . . . :   PGMR1
  Biblioteka . . . :   CUSTLIB    Grupa podstawowa . . :   DPTAR
Typ obiektu  . . . :   *DTAARA    Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji  . . . . :   *NONE

                 Opr. do    -----Obiekt------   ------Dane--------
Użytk. Grupa    obiektu     O   M   E   A   R   R   A   U   D   E
*ADOPTED         USER DEF        X   X   X   X
*PUBLIC          *EXCLUDE
PGMR1            *ALL         X   X   X   X   X   X   X   X   X   X
*GROUP  DPTAR    *CHANGE      X                   X   X   X   X   X
DPTSM            *USE         X                   X               X
```

Raporty o uprawnieniach

Do monitorowania implementacji ochrony dostępnych jest kilka raportów. Na przykład, za pomocą wymienionych poniżej komend można monitorować obiekty z uprawnieniami *PUBLIC innymi niż *EXCLUDE oraz obiekty z uprawnieniami prywatnymi:

- Drukowanie uprawnień publicznych (Print Public Authority - PRTPUBAUT),
- Drukowanie uprawnień prywatnych (Print Private Authority - PRTPVTAUT).

Więcej informacji dotyczących narzędzi ochrony zawiera podręcznik *Wskazówki i narzędzia dotyczące ochrony iSeries*.

Praca z bibliotekami

Na uprawnienia mają wpływ dwa parametry komendy Tworzenie biblioteki (Create Library - CRTLIB):

Uprawnienia (AUT): Parametr AUT może być użyty do podania:

- uprawnień publicznych do biblioteki,
- listy autoryzacji, która zabezpiecza bibliotekę.

Parametr AUT dotyczy samej biblioteki, a nie obiektów w bibliotece. Jeśli podana zostanie nazwa listy autoryzacji, uprawnienia publiczne do biblioteki będą miały wartość *AUTL.

Jeśli podczas tworzenia biblioteki nie zostanie podany parametr AUT, użyta zostanie wartość domyślna *LIBCRTAUT. System korzysta z wartości CRTAUT z biblioteki QSYS, która ma wartość *SYSVAL.

Uprawnienie do tworzenia (CRTAUT): Parametr CRTAUT określa domyślne uprawnienia do wszystkich nowych obiektów, które są tworzone w bibliotece. Parametr CRTAUT może być ustawiony na jedno z uprawnień systemowych (*ALL, *CHANGE, *USE lub *EXCLUDE), może mieć wartość *SYSVAL (wartość systemowa QCRTAUT) lub zawierać nazwę listy autoryzacji.

Uwaga: Parametr CRTAUT dla biblioteki można zmienić za pomocą komendy Zmiana biblioteki (Change Library - CHGLIB).

Jeśli użytkownik PGMR1 wpisuje następującą komendę:

```
CRTLIB TESTLIB AUT(LIBLST) CRTAUT(OBJLST)
```

uprawnienia dla biblioteki wyglądają następująco:

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   TESTLIB       Właściciel . . . . . :   PGMR1
  Biblioteka . . . :     QSYS        Grupa podstawowa . . :   *NONE
Typ obiektu  . . . :   *LIB          Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji . . . . . :   LIBLST

                       Uprawnienia
Użytkownik  Grupa      do obiektu
*PUBLIC                 *AUTL
PGMR1                   *ALL
```

- Ponieważ dla parametru AUT podana została lista autoryzacji, uprawnienia publiczne zostały ustawione na *AUTL.
- Użytkownik wprowadzający komendę CRTLIB jest właścicielem biblioteki, chyba że profil użytkownika ma parametr OWNER(GRPPRF). Użytkownik automatycznie otrzymuje uprawnienia *ALL.
- Na ekranach uprawnień do obiektu wartość CRTAUT nie jest pokazywana. Aby sprawdzić wartość CRTAUT dla biblioteki, należy użyć komendy Wyświetlenie opisu biblioteki (Display Library Description - DSPLIBD).

```
            Wyświetlenie opisu biblioteki
            (Display Library Description)
Biblioteka . . . . . . . . . . . . . . . . . :   CUSTLIB

Typ  . . . . . . . . . . . . . . . . . . . . :   PROD
Numer ASP  . . . . . . . . . . . . . . . . . :   1
Urządzenie ASP . . . . . . . . . . . . . . . :   *SYSBAS
Uprawnienie do tworzenia . . . . . . . . . . :   *OBJLST
Kontrola tworzonego obiektu  . . . . . . . . :   *SYSVAL
Tekst opisu  . . . . . . . . . . . . . . . . :   Customer Rec
```

Tworzenie obiektów

Gdy użytkownik tworzy nowy obiekt, może podać uprawnienia (AUT) lub skorzystać z wartości domyślnej *LIBCRTAUT. Jeśli PGMR1 wprowadza następującą komendę:

```
CRTDTAARA (TESTLIB/DTA1) +
   TYPE(*CHAR)
```

uprawnienia dla obszaru do danych wyglądają następująco:

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   DTA1          Właściciel . . . . . :   PGRM1
  Biblioteka . . . :   TESTLIB     Grupa podstawowa . . :   *NONE
Typ obiektu  . . . :   *DTAARA     Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji . . . . . :   OBJLST

                       Uprawnienia
Użytkownik  Grupa      do obiektu
*PUBLIC                 *AUTL
PGMR1                   *ALL
```

Lista autoryzacji (OBJLST) pochodzi z parametru CRTAUT, który został podany, gdy tworzona była biblioteka TESTLIB.

Jeśli PGMR1 wprowadza następującą komendę:

```
CRTDTAARA (TESTLIB/DTA2) AUT(*CHANGE) +
   TYPE(*CHAR)
```

uprawnienia dla obszaru do danych wyglądają następująco:

```
                   Wyświetlenie uprawnień dla obiektu
                      (Display Object Authority)
Obiekt . . . . . :   DTA2       Właściciel . . . . . :   PGRM1
  Biblioteka . . . :   TESTLIB    Grupa podstawowa . . :   *NONE
Typ obiektu  . . . :   *DTAARA    Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji  . . . . :   *NONE

                        Uprawnienia
Użytkownik  Grupa       do obiektu
*PUBLIC                 *CHANGE
PGMR1                   *ALL
```

Praca z uprawnieniami do pojedynczego obiektu

Aby zmienić uprawnienia do obiektu, użytkownik musi spełniać jeden z poniższych warunków:

- musi mieć uprawnienia *ALLOBJ lub być członkiem profilu grupowego, który ma uprawnienia specjalne *ALLOBJ,

  Uwaga: Jeśli użytkownik ma uprawnienia prywatne do obiektu, uprawnienia grupowe nie zostaną użyte.
- musi mieć prawo własności do obiektu; jeśli profil grupowy jest właścicielem obiektu, każdy członek grupy może działać jako właściciel obiektu, chyba że ma nadane określone uprawnienia, które nie spełniają wymagań potrzebnych do zmiany obiektu,
- musi mieć uprawnienia *OBJMGT do obiektu oraz dowolne inne uprawnienia - nadane lub odwołane - (z wyjątkiem *EXCLUDE); każdy użytkownik, który może pracować z uprawnieniami obiektu, może nadawać lub odwoływać uprawnienia *EXCLUDE.

Najprostszym sposobem zmiany uprawnień do pojedynczego obiektu jest skorzystanie z ekranu Edycja uprawnień dla obiektu (Edit Object Authority). Ten ekran można wywołać bezpośrednio za pomocą komendy Edycja uprawnień dla obiektu (Edit Object Authority - EDTOBJAUT) lub wybierając jako opcję na ekranie Praca z obiektami wg właścicieli (Work with Objects by Owner - WRKOBJOWN) lub WRKOBJ (Praca z obiektami - Work with Objects).

```
                    Edycja uprawnień dla obiektu
                     (Edit Object Authority)

Obiekt  . . . . . :   DTA1       Właściciel . . . . . :   PGMR1
 Biblioteka . . . :   TESTLIB    Grupa podstawowa . . :   *NONE
Typ obiektu . . . :   *DTAARA    Urządzenie ASP . . . :   *SYSBAS

Wpisz zmiany obecnych uprawnień i naciśnij Enter.

    Obiekt jest chroniony przez listę autoryzacji . . :   OBJLST

                         Uprawnienia
Użytkownik  Grupa        do obiektu
*PUBLIC                  *AUTL
PGMR1                    *ALL
```

Aby zmienić uprawnienia do obiektu, można użyć także następujących komend:

Zmiana uprawnień (Change Authority - CHGAUT),

Praca z uprawnieniami (Work with Authority - WRKAUT)

Nadanie uprawnień dla obiektu (Grant Object Authority - GRTOBJAUT),

Odwołanie uprawnień dla obiektu (Revoke Object Authority - RVKOBJAUT)

Aby podać ogólne podzbiory uprawnień, takie jak odczyt/zapis (*RX) lub zapis/wykonanie (*WX), użytkownik musi użyć komend CHGAUT lub WRKAUT.

Określanie uprawnień zdefiniowanych przez użytkownika

Kolumna Uprawnienia do obiektu na ekranie Edycja uprawnień dla obiektu (Edit Object Authority) umożliwia podanie dowolnych zestawów uprawnień zdefiniowanych systemowo (*ALL, *CHANGE, *USE, *EXCLUDE). Jeśli użytkownik chce podać uprawnienia, które nie są zdefiniowane systemowo, musi użyć klawisza F11 (Wyświetl szczegóły).

Uwaga: Jeśli pole *Opcje użytkownika* (USROPT) w profilu użytkownika ma wartość *EXPERT, użytkownik zawsze będzie widział ekran w wersji z szczegółami, bez konieczności naciskania klawisza F11.

Na przykład użytkownik PGMR1 usuwa uprawnienia *OBJEXIST do zbioru CONTRACTS, aby zapobiec przypadkowemu usunięciu tego zbioru. Ponieważ użytkownik PGMR1 ma kombinację uprawnień, która nie jest zestawem zdefiniowanym systemowo, w kolumnie Uprawnienia do obiektu system wstawi wartość *USER DEF* (zdefiniowane przez użytkownika):

```
                  Edycja uprawnień dla obiektu
                   (Edit Object Authority)

Obiekt . . . . . :   CONTRACTS   Właściciel . . . . . :   PGMR1
  Biblioteka . . . :   TESTLIB     Grupa podstawowa . . :   *NONE
Typ obiektu  . . . :   *FILE       Urządzenie ASP . . . :   *SYSBAS

Wpisz zmiany obecnych uprawnień i naciśnij Enter.

  Obiekt jest chroniony przez listę autoryzacji . . . . . :   LIST2

                       Upr. do   ----------Obiekt-----------
Użytkownik  Grupa      obiektu  Oper Zarz.Istn. Zmian. Odn.
*PUBLIC                *AUTL
PGMR1                  USER DEF    X    X            X     X
```

Aby przeglądać lub zmieniać uprawnienia do danych, należy nacisnąć klawisz F11 (Uprawnienia do danych):

```
                  Edycja uprawnień dla obiektu
                   (Edit Object Authority)

 Obiekt . . . . . :   CONTRACTS   Właściciel . . . . . :   PGMR1
  Biblioteka  . . . :   TESTLIB     Grupa podstawowa . . :   *NONE
 Typ obiektu  . . . :   *FIL        Urządzenie ASP . . . :   *SYSBAS

Wpisz zmiany obecnych uprawnień i naciśnij Enter.

  Obiekt jest chroniony przez listę autoryzacji . . . . . :   LIST2

                       Uprawn.  ---------------Dane---------------
Użytk      Grupa       do obiektu Odcz. Dod. Aktual. Usuw.  Wykon.
*PUBLIC                *AUTL
PGMR1                  USER DEF    X     X     X       X        X
```

Nadawanie uprawnień nowym użytkownikom

Aby nadać uprawnienia dodatkowym użytkownikom, na ekranie Edycja uprawnień dla obiektu (Edit Object Authority) należy nacisnąć klawisz F6 (Dodaj użytkowników). Pojawi się ekran Dodawanie nowych użytkowników (Add New Users), który umożliwia zdefiniowane uprawnień dla wielu użytkowników:

```
             Dodawanie nowych użytkowników
                  (Add New Users)
Obiekt . . . . . :   DTA1
  Biblioteka . . . :     TESTLIB

Wpisz nowych użytkowników i naciśnij Enter.

            Uprawnienia
Użytkownik  do obiektu
USER1       *USE
USER2       *CHANGE
PGMR2       *ALL
```

Usuwanie uprawnień użytkownika

Usuwanie uprawnień użytkownika do obiektu to inna sytuacja niż nadawanie mu uprawnień *EXCLUDE. Uprawnienia *EXCLUDE oznaczają, że użytkownik wyraźnie ma zabroniony dostęp do danego obiektu. Tylko uprawnienia specjalne *ALLOBJ oraz adoptowane mogą przesłonić uprawnienia *EXCLUDE. Usuwanie uprawnień użytkownika oznacza, że użytkownik nie ma konkretnych uprawnień do obiektu. Może uzyskać dostęp za pośrednictwem profilu grupowego, listy autoryzacji, uprawnień publicznych, uprawnień specjalnych *ALLOBJ lub uprawnień adoptowanych.

Uprawnienia użytkownika można usunąć za pomocą ekranu Edycja uprawnień dla obiektu (Edit Object Authority). W tym celu pole Uprawnienia do obiektu, dla danego użytkownika należy pozostawić puste i nacisnąć klawisz Enter. Użytkownik zostanie usunięty z ekranu. Można także użyć komendy Odwołanie uprawnień dla obiektu (Revoke Object Authority - RVKOBJAUT). Można odwołać konkretne uprawnienia lub odwołać wszystkie (*ALL).

Uwaga: Komenda RVKOBJAUT odwołuje tylko uprawnienia podane przez użytkownika. Na przykład UŻYTKOWNIK_B ma uprawnienia *ALL do zbioru ZBIÓR_B w bibliotece BIB_B. Odwołane mają być uprawnienia *CHANGE:

```
RVKOBJAUT OBJ(BIB_B/ZBIÓR_B) OBJTYPE(*FILE) +
USER(*UŻYTKOWNIK_BUSERB) AUT(*CHANGE)
```

Po wywołaniu tej komendy, uprawnienia UŻYTKOWNIKA_B do ZBIORU_B wyglądają następująco:

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   ZBIÓR_B   Właściciel . . . . . :   PGMR1
  Biblioteka . . . :   BIB_B     Grupa podstawowa . . :   *NONE
Typ obiektu . . . :   *FILE      Urządzenie ASP . . . :   *SYSBAS

  Obiekt jest chroniony przez listę autoryzacji . . . :   *NONE

                       Uprawn.  ------------Dane---------------
Użytk      Grupa       do obiektu Odcz. Dod. Aktual. Usuw.  Wykon.
USERB            USER DEF         X    X       X       X
```

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   ZBIÓR_B   Właściciel . . . . . :   PGMR1
  Biblioteka . . . :   BIB_B     Grupa podstawowa . . :   *NONE
Typ obiektu. . . . :   *FILE     Urządzenie ASP . . . :   *SYSBAS

  Obiekt jest chroniony przez listę autoryzacji . . . :   *NONE

                       Upr. do    ---------------Dane---------------
Użytkownik  Grupa      obiektu   Odczyt Dod. Aktual. Usuw. Wykonyw.
PGMR1                  USER DEF
```

Praca z uprawnieniami dla wielu obiektów

Ekran Edycja uprawnień dla obiektu (Edit Object Authority) umożliwia interaktywną pracę z uprawnieniami do jednego obiektu. Komenda Nadanie uprawnień dla obiektu (Grant Object Authority - GRTOBJAUT) umożliwia dokonywanie zmian uprawnień do więcej niż jednego obiektu w tym samym czasie. Komendy GRTOBJAUT można używać interaktywnie lub wsadowo. Można ją także wywołać z programu.

Poniżej przedstawiono przykłady użycia komendy GRTOBJAUT, prezentując ekrany. Gdy komenda jest uruchomiona, dla każdego obiektu użytkownik otrzymuje komunikat informujący, czy zmiana została dokonana. Zmiany uprawnień

wymagają blokady obiektu na wyłączność i nie mogą być przeprowadzane, gdy obiekt jest używany. Aby sprawdzić rekordy zmian, które próbowano wprowadzić i które zostały wprowadzone, należy wydrukować protokół zadania.

- Aby wszystkim obiektom w bibliotece TESTLIB nadać uprawnienia publiczne *USE:

```
               Nadanie uprawnień dla obiektu
             (Grant Object Authority - GRTOBJAUT)

Wpisz i naciśnij Enter.  Obiekt . . . . . . . . . . . . .   *ALL
Biblioteka  . . . . . . . . . . . . TESTLIB
Typ obiektu  . . . . . . . . . . . *ALL
Urządzenie ASP  . . . . . . . . . . *
Użytkownicy. . . . . . . . . . .  *PUBLIC
+ więcej wartości
Uprawnienie  . . . . . . . . . . .  *USE
```

  Ten przykład komendy GRTOBJAUT nadaje podane przez użytkownika uprawnienia, ale nie usuwa uprawnień, które są większe niż te podane przez użytkownika. Jeśli jakieś obiekty w bibliotece TESTLIB mają uprawnienia publiczne *CHANGE, przedstawiona komenda nie zmniejszy ich uprawnień publicznych do uprawnień *USE. Aby upewnić się, że wszystkie obiekty w bibliotece TESTLIB mają uprawnienia *USE, należy użyć komendy GRTOBJAUT z parametrem REPLACE.

  ```
  GRTOBJAUT OBJ(TESTLIB/*ALL) OBJTYPE(*ALL) +
            USER(*PUBLIC) REPLACE(*YES)
  ```

  Parametr REPLACE określa, czy podane uprawnienia zastępują istniejące. Wartość domyślna REPLACE(*NO) nadaje podane uprawnienia, ale nie usuwa uprawnień, które są większe niż te podawane przez użytkownika, chyba że użytkownik nadaje uprawnienia *EXCLUDE.

  Te komendy ustawiają uprawnienia publiczne do obiektów, które aktualnie znajdują się w bibliotece. Aby ustawić uprawnienia publiczne dla nowych obiektów, które zostaną utworzone później, w opisie biblioteki należy wykorzystać parametr CRTAUT.

- Aby użytkownikom AMES i SMITHR nadać uprawnienia *ALL do zbiorów roboczych biblioteki TESTLIB. W tym przykładzie nazwy wszystkich zbiorów roboczych rozpoczynają się od znaków WRK:

```
               Nadanie uprawnień dla obiektu
             (Grant Object Authority - GRTOBJAUT)

Wpisz i naciśnij Enter.
Obiekt . . . . . . . . . . . . .  WRK*
  Biblioteka . . . . . . . . . .  TESTLIB
Typ obiektu  . . . . . . . . . .  *FILE
Urządzenie ASP  . . . . . . . . . *
Użytkownicy  . . . . . . . . . .  AMES
               + więcej wartości   SMITHR
Uprawnienie  . . . . . . . . . .  *ALL
```

  Ta komenda do określenia zbiorów korzysta z nazwy ogólnej. Nazwę ogólną podaje się wpisując znaki, po których następuje gwiazdka (*). Omówienie parametrów komendy umożliwiających podanie nazw ogólnych zawierają informacje elektroniczne.

- Aby zabezpieczyć wszystkie zbiory rozpoczynające się od znaków AR* korzystając z listy autoryzacji ARLST1 oraz nadać im uprawnienia publiczne z listy, należy użyć następującej komendy:

  1. Ochrona zbiorów z wykorzystaniem listy autoryzacji za pomocą komendy GRTOBJAUT:

```
             Nadanie uprawnień dla obiektu
              (Grant Object Authority)

Wpisz i naciśnij Enter.
Obiekt . . . . . . . . . . . . . .  AR*
  Biblioteka . . . . . . . . . . .  TESTLIB
Typ obiektu  . . . . . . . . . . .  *FILE
Urządzenie ASP  . . . . . . . . . . *
  :
Lista autoryzacji . . . . . . . .  ARLST1
```

2. Za pomocą komendy GRTOBJAUT należy ustawić uprawnienia publiczne do zbiorów na uprawnienia *AUTL:

```
             Nadanie uprawnień dla obiektu
              (Grant Object Authority)

Wpisz i naciśnij Enter.
Obiekt . . . . . . . . . . . . . .  AR*
  Biblioteka . . . . . . . . . . .  TESTLIB
Typ obiektu  . . . . . . . . . . .  *FILE
Urządzenie ASP  . . . . . . . . . . *
Użytkownicy. . . . . . . . . . .  *PUBLIC
               + więcej wartości
Uprawnienie  . . . . . . . . . . .  *AUTL
```

Praca z prawem własności do obiektu

Aby zmienić prawo własności do obiektu, należy użyć jednej z następujących komend:

Zmiana właściciela obiektu (Change Object Owner - CHGOBJOWN),

Praca z obiektami wg właścicieli (Work with Objects by Owner - WRKOBJOWN),

Zmiana właściciela (Change Owner - CHGOWN).

Na ekranie Praca z obiektami wg właścicieli (Work with Objects by Owner) wyświetlane są wszystkie obiekty posiadane przez profil. Pojedyncze obiekty można przypisać do nowego właściciela. Można także zmienić prawo własności do więcej niż jednego obiektu - korzystając z parametru NEWOWN (nowy właściciel) znajdującego się u dołu ekranu:

```
              Praca z obiekt. wg właścicieli
               (Work with Objects by Owner)

Profil użytkownika . . . . :   OLDOWNER

Wpisz opcje i naciśnij klawisz Enter.
  2=Edytuj uprawnienia    4=Usuń   5=Wyświetl uprawnienia
  8=Wyświetlenie opisu    9=Zmiana właściciela
                                                          Urządzenie
Opc    Obiekt      Biblioteka    Typ     Atrybut          ASP
     COPGMMSG      COPGMLIB      *MSGQ                    *SYSBAS
9    CUSTMAS       CUSTLIB       *FILE                    *SYSBAS
9    CUSTMSGQ      CUSTLIB       *MSGQ                    *SYSBAS
     ITEMMSGQ      ITEMLIB       *MSGQ                    *SYSBAS

Parametry lub komenda
===> NEWOWN(OWNIC)
F3=Wyjście   F4=F4=Podpowiedź   F5=Odśwież   F9=Poprzednie komendy
F18=Koniec
```

Podczas zmiany prawa własności za pomocą jednej z tych metod, można usunąć uprawnienia poprzedniego właściciela obiektu. Wartością domyślną parametru CUROWNAUT (uprawnienia bieżącego właściciela) jest wartość *REVOKE.

Aby przenieść prawo własności do obiektu, użytkownik musi mieć:

- uprawnienia do istnienia obiektu,
- jeśli obiekt znajduje się na liście autoryzacji, uprawnienia *ALL lub prawo własności,
- mający uprawnienie do dodawania do nowego profilu użytkownika właściciela,
- uprawnienia do usuwania do obecnego profilu właściciela.

Nie można usunąć profilu użytkownika, który posiada obiekty. Temat “Usuwanie profili użytkowników” na stronie 103 opisuje metody obsługi posiadanych obiektów podczas usuwania profilu.

Na ekranie Praca z obiektami wg właścicieli (Work with Objects by Owner) można obejrzeć obiekty zintegrowanego systemu plików. Dla tych obiektów kolumna *Obiekt* na ekranie zawiera pierwszych 18 znaków nazwy ścieżki. Jeśli nazwa ścieżki jest dłuższa niż 18 znaków, na jej końcu pojawia się znak większości (>). Aby zobaczyć bezwzględną nazwę ścieżki, w dowolnym miejscu nazwy ścieżki należy umieścić kursor i nacisnąć klawisz F22.

Praca z uprawnieniami grupy podstawowej

Aby zmienić grupę podstawową lub uprawnienia grupy podstawowej dla obiektu, należy użyć jednej z następujących komend:

Zmiana grupy podstawowej obiektu (Change Object Primary Group - CHGOBJPGP),

Praca z obiektami wg grupy podstawowej (Work with Objects by Primary Group - WRKOBJPGP)

Zmiana grupy podstawowej (Change Primary Group - CHGPGP).

Gdy zmieniana jest grupa podstawowa obiektu, użytkownik podaje, jakie uprawnienia ma nowa grupa podstawowa. Można także odwołać uprawnienia poprzedniej grupy podstawowej. Jeśli uprawnienia poprzedniej grupy podstawowej nie zostaną odwołane, stają się uprawnieniami prywatnymi.

Nowa grupa podstawowa nie może być właścicielem obiektu.

Aby zmienić grupę podstawową obiektu, użytkownik musi mieć:

- uprawnienia *OBJEXIST do obiektu,
- jeśli obiekt jest zbiorem, biblioteką lub opisem podsystemu, uprawnienia *OBJOPR i *OBJEXIST,

- jeśli obiekt jest listą autoryzacji, uprawnienia specjalne *ALLOBJ lub prawo własności do listy autoryzacji,
- w przypadku odwoływania uprawnień dla poprzedniej grupy podstawowej, uprawnienia *OBJMGT,
- jeśli podana została wartość inna niż *PRIVATE, uprawnienia *OBJMGT oraz wszystkie nadawane uprawnienia.

Używanie obiektu odniesienia

Zarówno ekran Edycja uprawnień dla obiektu (Edit Object Authority) jak i komenda GRTOBJAUT umożliwiają nadanie uprawnień do obiektu (lub grupy obiektów) w oparciu o uprawnienia obiektu odniesienia. Jest to przydatne narzędzie, ale aby spełnić stawiane wymagania, należy rozważyć użycie listy autoryzacji. Więcej informacji dotyczących korzyści z używania listy autoryzacji zawiera sekcja “Planowanie list autoryzacji” na stronie 217.

Kopiowanie uprawnień innego użytkownika

Za pomocą komendy Nadanie uprawnień użytkownika (Grant User Authority - GRTUSRAUT) można skopiować wszystkie uprawnienia prywatne jednego użytkownika do innego. Ta metoda może być przydatna w pewnych sytuacjach. Na przykład gdy system nie zezwala na zmianę nazwy profilu użytkownika. Tworzenie identycznego profilu z inną nazwą obejmuje kilka czynności, między innymi kopiowanie uprawnień oryginalnego profilu. Sekcja “Zmiana nazwy profilu użytkownika” na stronie 107 pokazuje przykład takiej operacji.

Komenda GRTUSRAUT kopiuje jedynie uprawnienia prywatne. Nie kopiuje uprawnień specjalnych, ani nie przenosi prawa własności do obiektu.

Komenda GRTUSRAUT nie powinna być używana zamiast tworzenia profili grupowych. Tworzy ona duplikat zestawu uprawnień prywatnych, który powoduje zwiększenie czasu składowania systemu i utrudnia zarządzanie uprawnieniami. Komenda GRTUSRAUT kopiuje uprawnienia, które istnieją w danym momencie. Jeśli w przyszłości wymagane będą uprawnienia do nowego obiektu, każdemu profilowi będą musiały być przydzielane oddzielnie. Profil grupowy udostępnia taką funkcję automatycznie.

Aby użyć komendy GRTUSRAUT, użytkownik musi mieć wszystkie kopiowane uprawnienia. Jeśli nie ma uprawnień, to dane uprawnienie nie zostanie nadane docelowemu profilowi. System wysyła komunikat dla każdego uprawnienia, które zostało nadane lub nie nadane docelowemu profilowi użytkownika. Wszystkie rekordy można zobaczyć po wydrukowaniu protokołu zadania. Aby uniknąć częściowego kopiowania zestawu uprawnień, komendę GRTUSRAUT powinien uruchamiać użytkownik z uprawnieniami specjalnymi *ALLOBJ.

Praca z listami autoryzacji

Skonfigurowanie listy autoryzacji wymaga trzech czynności:

1. utworzenie listy autoryzacji,
2. dodanie użytkowników do listy autoryzacji,
3. zabezpieczenie obiektów za pomocą listy autoryzacji.

Czynności 2 i 3 można wykonać w dowolnej kolejności.

Tworzenie listy autoryzacji

Aby utworzyć listę autoryzacji w bibliotece QSYS, nie są potrzebne żadne uprawnienia do tej biblioteki. W tym celu należy użyć komendy Tworzenie listy autoryzacji (Create Authorization List - CRTAUTL):

```
                Tworzenie listy autoryzacji
              (Create Authorization List - CRTAUTL)

Wpisz i naciśnij Enter.
Lista autoryzacji  . . . . . .  custlst1
Tekst opisu  . . . . . .  Zbiory czyszczone na koniec miesiąca

                          Dodatkowe parametry
                        (Additional Parameters)

Uprawnienie  . . . . . .  *use
```

Parametr AUT ustawia uprawnienia publiczne dla wszystkich obiektów zabezpieczanych przez listę. Uprawnienia publiczne pochodzące z listy autoryzacji używane są tylko wtedy, gdy uprawnienia publiczne dla obiektu zabezpieczanego przez daną listę mają wartość *AUTL.

Nadawanie użytkownikom uprawnień do listy autoryzacji

Do pracy z uprawnieniami użytkowników do listy autoryzacji jest niezbędne posiadanie uprawnień *AUTLMGT (zarządzanie listą autoryzacji) oraz tych, które są nadawane. Pełen opis zawiera temat “Zarządzanie listą autoryzacji” na stronie 120.

Aby zmienić uprawnienia użytkownika do listy autoryzacji lub dodać nowych użytkowników do tej listy, można użyć ekranu Edycja listy autoryzacji (Edit Authorization List):

```
                 Edycja listy autoryzacji
                (Edit Authorization List)
Obiekt . . . . . :   CUSTLST1       Właściciel . . . . . :   PGMR1
  Biblioteka . . . :   QSYS         Grupa podstawowa . . :   *NONE

Wpisz zmiany obecnych uprawnień i naciśnij Enter.

           Uprawnienia Zarząd.
Użytkownik  do obiektu  listą
*PUBLIC     *USE
PGMR1       *ALL        X
```

Aby nowym użytkownikom nadać uprawnienia do listy autoryzacji, należy nacisnąć klawisz F6 (Dodawanie nowych użytkowników):

```
            Dodawanie nowych użytkowników
                  (Add New Users)
Obiekt . . . . . :   CUSTLST1     Właściciel . . PGMR1
  Biblioteka . . . :     QSYS

Wpisz nowych użytkowników i naciśnij Enter.

           Uprawnienia Zarząd.
Użytkownik  do obiektu  listą
AMES        *CHANGE
SMITHR      *CHANGE
```

Wszystkie uprawnienia użytkownika do listy przechowywane są jako uprawnienia prywatne w jego profilu użytkownika. Do pracy z użytkownikami listy autoryzacji można także użyć komend - interaktywnie lub wsadowo:

- komenda Dodanie pozycji listy autoryzacji (Add Authorization List Entry - ADDAUTLE) do zdefiniowania uprawnień dla dodatkowych użytkowników,
- komenda Zmiana pozycji listy autoryzacji (Change Authorization List Entry - CHGAUTLE) do zmiany uprawnień dla użytkowników, którzy już są autoryzowani do listy,
- komenda Usunięcie pozycji listy autoryzacji (Remove Authorization List Entry - RMVAUTLE) do usunięcia uprawnień użytkownika z listy.

Ochrona obiektów za pomocą listy autoryzacji

Aby zabezpieczyć obiekt za pomocą listy autoryzacji, użytkownik musi być właścicielem obiektu oraz mieć do niego uprawnienia *ALL lub uprawnienia specjalne *ALLOBJ.

Aby zabezpieczyć obiekt za pomocą listy autoryzacji, należy użyć ekranu Edycja uprawnień dla obiektu (Edit Object Authority) lub komendy GRTOBJAUT:

```
                  Edycja uprawnień dla obiektu
                   (Edit Object Authority)

Obiekt . . . . . :   ZBIÓR_B      Właściciel . . . . . :   PGMR1
  Biblioteka . . . :   TESTLIB     Grupa podstawowa . . :   *NONE
Typ obiektu. . . . :   *FILE       Urządzenie ASP . . . :   *SYSBAS

Wpisz zmiany obecnych uprawnień i naciśnij Enter.

Obiekt jest chroniony przez listę autoryzacji . . . . . :   ARLST1

            Uprawnienia
Użytkownik  do obiektu
*PUBLIC     *AUTL
PGMR1       *ALL
```

Jeśli uprawnienia publiczne mają pochodzić z listy autoryzacji, to uprawnienia publiczne do obiektu muszą mieć wartość *AUTL.

Na ekranie Edycja listy autoryzacji (Edit Authorization List), aby pokazać listę wszystkich obiektów zabezpieczanych przez listę, można użyć klawisza F15 (Wyświetlenie obiektów listy autoryzacji):

```
                     Wyświetlenie obiektów listy autoryzacji
                       (Display Authorization List Objects)

Lista autoryzacji  . . . . . :   CUSTLST1
  Biblioteka . . . . . :   CUSTLIB
Właściciel . . . . . :   OWNAR
Grupa podstawowa . . . . . :   DPTAR

Grupa      Biblioteka     Typ    Właściciel
podstawowa                                  Tekst
CUSTMAS     CUSTLIB     *FILE     OWNAR
CUSTADDR    CUSTLIB     *FILE     OWNAR
```

To jest jedynie lista informacyjna. Nie można dodawać ani usuwać z niej obiektów. Do przeglądania lub drukowania listy wszystkich obiektów zabezpieczanych przez listę można także użyć komendy Wyświetlenie listy autoryzacji (Display Authorization List Objects - DSPAUTLOBJ).

Usunięcie listy autoryzacji

Jeśli lista autoryzacji używana jest do zabezpieczania jakichkolwiek obiektów, nie można jej usunąć. Aby wyświetlić wszystkie obiekty zabezpieczane przez listę, należy użyć komendy DSPAUTLOBJ. Aby zmienić uprawnienia do każdego obiektu, należy użyć ekranu Edycja uprawnień dla obiektu (Edit Object Authority) lub komendy Odwołanie uprawnień dla obiektu (Revoke Object Authority - RVKOBJAUT). Gdy lista autoryzacji nie będzie już zabezpieczała żadnego obiektu, należy użyć komendy Usunięcie listy autoryzacji (Delete Authorization List - DLTAUTL).

Sposób sprawdzania uprawnień

Gdy użytkownik próbuje wykonać na obiekcie operację, system sprawdza, czy dany użytkownik ma wystarczające uprawnienia. System najpierw sprawdza uprawnienia do biblioteki lub ścieżki katalogu, który zawiera obiekt. Jeśli uprawnienia do biblioteki lub ścieżki katalogu są wystarczające, system sprawdza uprawnienia do samego obiektu. W przypadku zbiorów bazy danych, sprawdzanie uprawnień przeprowadzane jest w momencie otwierania zbioru, a nie podczas każdej pojedynczej operacji wykonywanej na zbiorze.

Podczas procesu sprawdzania uprawnień, gdy odnalezione zostaną jakiekolwiek uprawnienia (nawet jeśli nie są wystarczające dla żądanej operacji), sprawdzanie uprawnień jest zatrzymywane i dostęp jest nadawany lub odmawiany. Wyjątkiem od tej reguły jest funkcja uprawnień adoptowanych. Uprawnienia adoptowane mogą przesłonić dowolne (i niewystarczające) znalezione uprawnienia. Więcej informacji dotyczących uprawnień adoptowanych zawiera temat “Obiekty, które adoptują uprawnienia właściciela” na stronie 128.

System sprawdza uprawnienia użytkownika do obiektu w następującej kolejności:

1. Uprawnienia do obiektu - krótka ścieżka.
2. Uprawnienia specjalne *ALLOBJ użytkownika.
3. Konkretne uprawnienia do obiektu.
4. Uprawnienia użytkownika do listy autoryzacji zabezpieczającej obiekt.
5. Uprawnienia specjalne *ALLOBJ grupy.
6. Uprawnienia grupy do obiektu.
7. Uprawnienia grupy do listy autoryzacji zabezpieczającej obiekt.
8. Uprawnienia publiczne podane dla obiektu lub dla listy autoryzacji zabezpieczającej obiekt.
9. Uprawnienia właściciela programu, jeśli używane są uprawnienia adoptowane.

Uwaga: Aby zapewnić wystarczające uprawnienia do obiektu, system może kumulować uprawnienia z jednej lub więcej grup użytkownika.

Schematy blokowe sprawdzania uprawnień

Poniżej przedstawione zostały schematy blokowe, ich opisy oraz przykłady sprawdzania uprawnień. Należy ich użyć do odpowiedzi na określone pytania dotyczące tego, czy dany schemat uprawnień będzie działał lub do zdiagnozowania problemów związanych z definicjami uprawnień. Schematy wskazują także typy uprawnień mających największy wpływ na wydajność.

Proces sprawdzania uprawnień podzielony jest na podstawowy schemat blokowy i kilka mniejszych schematów, przedstawiających poszczególne części procesu. W zależności od kombinacji uprawnień do obiektu, kroki dla niektórych schematów blokowych mogą być powtarzane po kilka razy.

Liczby w lewym górnym rogu bloków na schematach blokowych używane są w przykładach następujących po tych schematach.

Wymienione poniżej kroki reprezentują wyszukiwanie uprawnień prywatnych profilu:

krok 6 na Schemacie blokowym 3 na stronie 154,

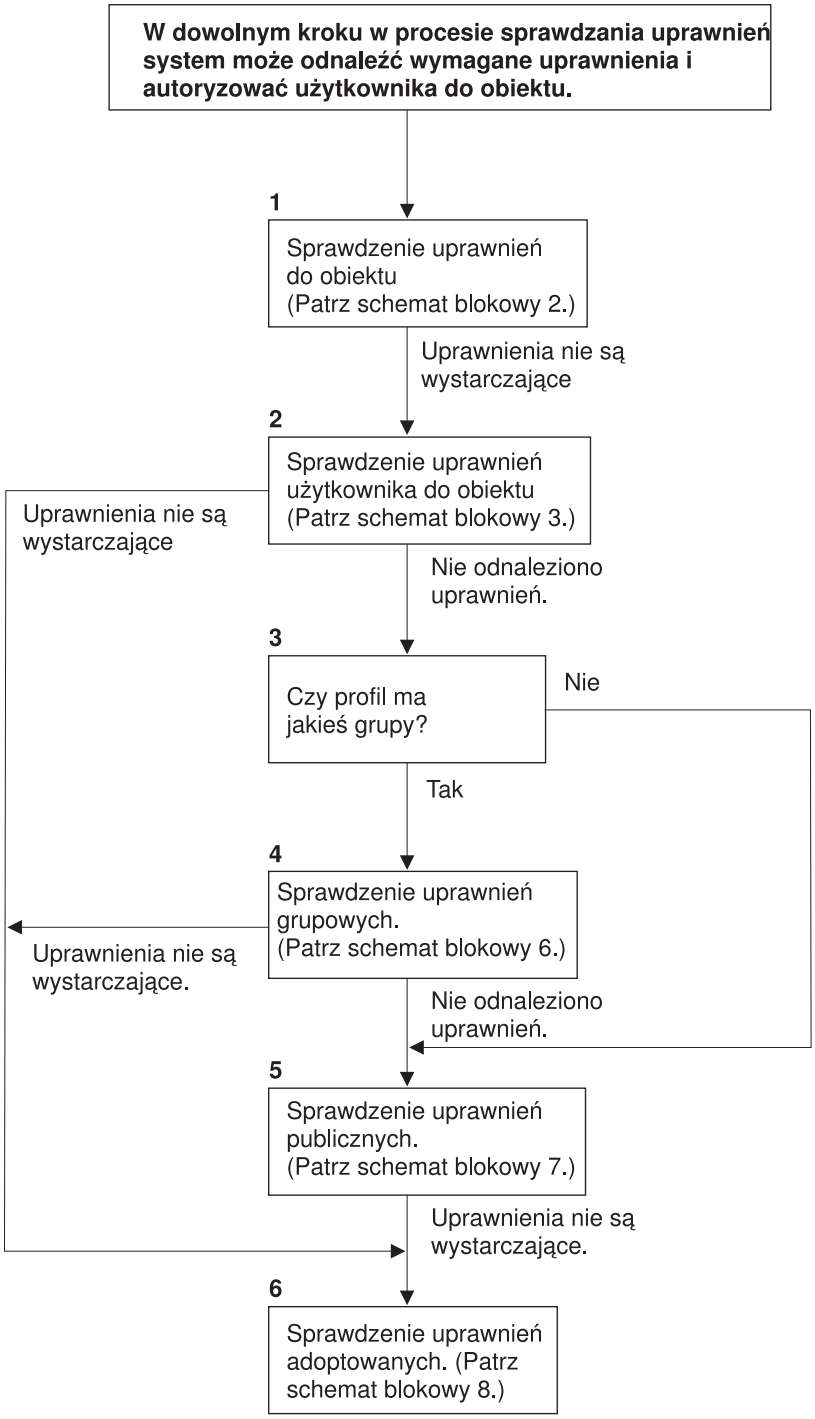
krok 6 na Schemacie blokowym 6 na stronie 160,

krok 2 na Schemacie blokowym 8B na stronie 165.

Powtarzanie tych kroków może spowodować problemy związane z wydajnością procesu sprawdzania uprawnień.

Schemat blokowy 1: Główny proces sprawdzania uprawnień

Kroki na Schemacie blokowym 1 prezentują główny proces, który przeprowadza system podczas sprawdzania uprawnień do obiektu.



Jeśli użytkownik nie jest uprawniony, wykonywane są następujące czynności:
1) Do użytkownika lub programu wysyłany jest komunikat;
2) Program nie powiódł się;
3)W kronice kontroli zapisywana jest pozycja AF.

RBAFW508-0

Rysunek 13. Schemat blokowy 1: Główny proces sprawdzania uprawnień

Opis Schematu blokowego 1: Główny proces sprawdzania uprawnień

Uwaga: W dowolnym kroku w procesie sprawdzania uprawnień system może odnaleźć wymagane uprawnienia i autoryzować użytkownika do obiektu.

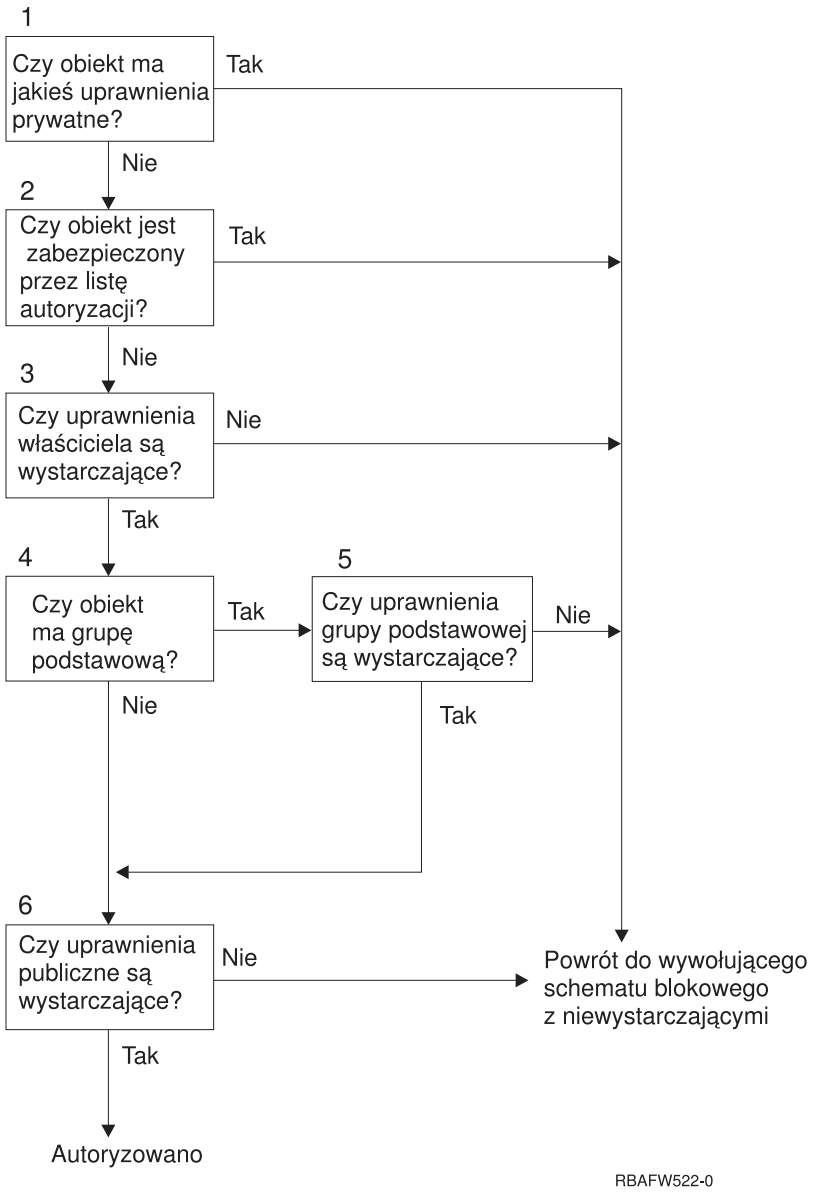
1. System sprawdza uprawnienia obiektu. (Patrz Schemat blokowy 2: Krótka ścieżka sprawdzania uprawnień do obiektu) Jeśli system sprawdzi, że uprawnienia nie są wystarczające, przechodzi do Kroku 2.
2. System sprawdza uprawnienia użytkownika do obiektu. (Patrz Schemat blokowy 3: Jak sprawdzane są uprawnienia użytkownika do obiektu.) Jeśli system stwierdzi, że użytkownik nie ma uprawnień do obiektu, przechodzi do Kroku 3. Jeśli system stwierdzi, że uprawnienia użytkownika są niewystarczające, przechodzi do Kroku 6.
3. System sprawdza, czy profil użytkownika należy do jakiejś grupy. Jeśli tak, to przechodzi do Kroku 4. Jeśli nie, system przechodzi do Kroku 5.
4. System określa uprawnienia grupowe. (Patrz Schemat blokowy 6). Jeśli system stwierdzi, że grupa nie ma uprawnień do obiektu, przechodzi do Kroku 5. Jeśli stwierdzi, że grupa ma niewystarczające uprawnienia do obiektu, przechodzi do Kroku 6.
5. System sprawdza uprawnienia publiczne do obiektu. (Patrz Schemat blokowy 7). Jeśli system stwierdzi, że uprawnienia publiczne są niewystarczające, przechodzi do Kroku 6.
6. System sprawdza uprawnienia adoptowane do obiektu. (Patrz Schemat blokowy 8).

Jeśli użytkownik nie jest uprawniony, wykonywane są następujące czynności:

- do użytkownika lub programu wysyłany jest komunikat,
- program kończy się niepowodzeniem,
- w kronice kontroli zapisywana jest pozycja AF.

Schemat blokowy 2: Krótka ścieżka sprawdzania uprawnień do obiektu

Czynności pokazane na Schemacie blokowym 2 wykonywane są przy wykorzystaniu informacji przechowywanych z obiektem. Jest to najszybsza metoda autoryzowania użytkownika do obiektu.



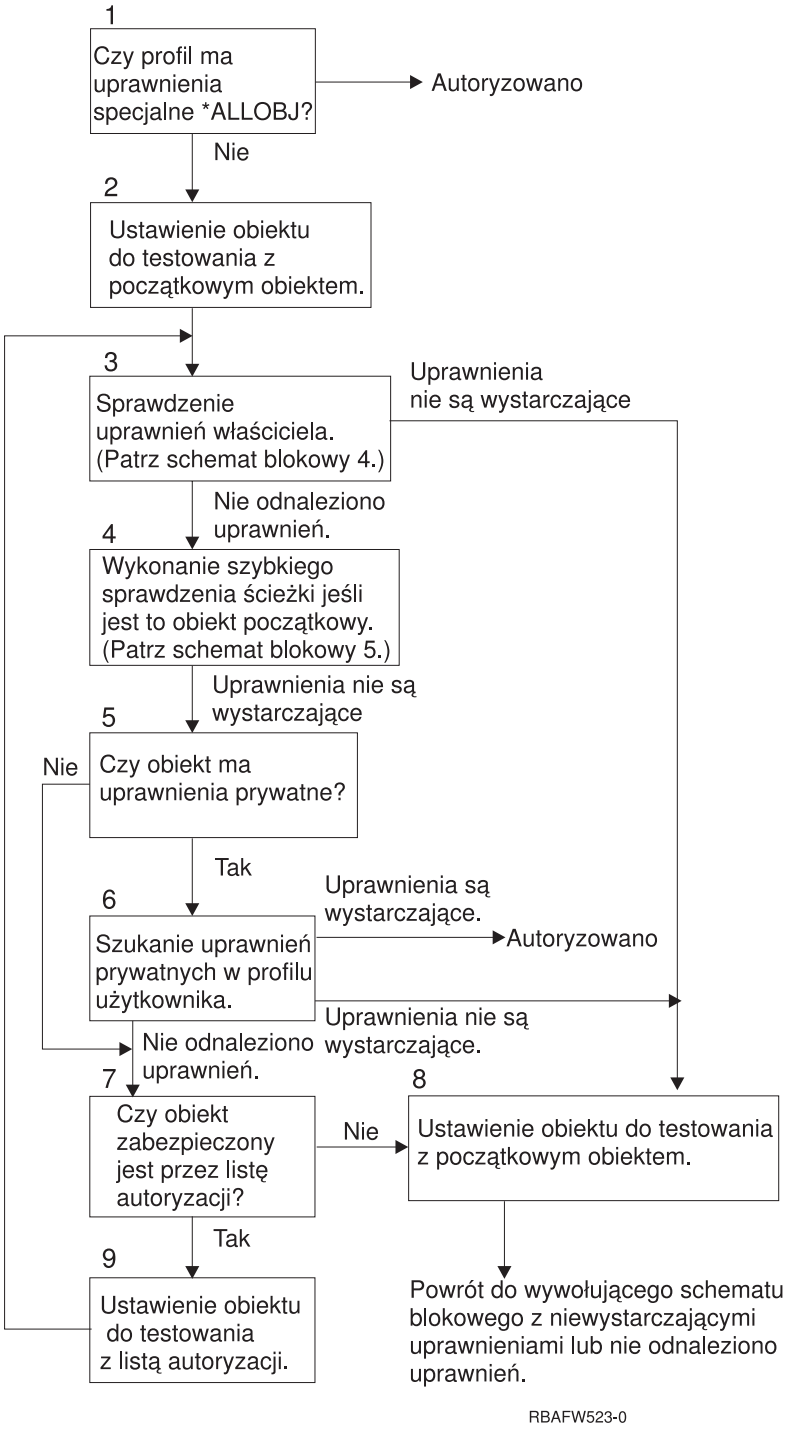
Rysunek 14. Schemat blokowy 2: Krótka ścieżka dla uprawnień do obiektu

Opis Schematu blokowego 2: Krótka ścieżka dla uprawnień do obiektu

1. System sprawdza, czy obiekt ma uprawnienia prywatne. Jeśli ma, system powraca do wywołującego schematu blokowego z niewystarczającymi uprawnieniami. Jeśli nie ma, system przechodzi do Kroku 2.
2. System sprawdza, czy obiekt jest chroniony przez listę autoryzacji. Jeśli jest, powraca do wywołującego schematu blokowego z niewystarczającymi uprawnieniami. Jeśli nie, przechodzi do Kroku 3.
3. System sprawdza, czy właściciel obiektu ma wystarczające uprawnienia. Jeśli ma, system powraca do wywołującego schematu blokowego z niewystarczającymi uprawnieniami. Jeśli nie ma, system przechodzi do Kroku 4.
4. System sprawdza, czy obiekt ma grupę podstawową. Jeśli tak, to przechodzi do Kroku 5. Jeśli nie, przechodzi do Kroku 6.
5. System sprawdza, czy grupa podstawowa obiektu ma wystarczające uprawnienia. Jeśli tak, to przechodzi do Kroku 6. Jeśli nie, system przechodzi do wywołującego schematu blokowego z niewystarczającymi uprawnieniami.
6. System sprawdza, czy uprawnienia publiczne są wystarczające. Jeśli są, obiekt jest autoryzowany. Jeśli nie, powraca do wywołującego schematu blokowego z niewystarczającymi uprawnieniami.

Schemat blokowy 3: Jak sprawdzane są uprawnienia użytkownika do obiektu

Kroki pokazane na Schemacie blokowym 3 wykonywane są dla pojedynczego profilu użytkownika.



Rysunek 15. Schemat blokowy 3: Sprawdzanie uprawnień użytkownika

Opis Schematu blokowego 3: Sprawdzanie uprawnień użytkownika

1. System sprawdza, czy profil użytkownika ma uprawnienia *ALLOBJ. Jeśli je ma, następuje autoryzowanie profilu. Jeśli profil nie ma uprawnień *ALLOBJ, proces sprawdzania uprawnień przechodzi do Kroku 2.
2. System ustawia uprawnienia obiektu na równe początkowemu obiektowi. Proces sprawdzania uprawnień przechodzi do kroku 3.

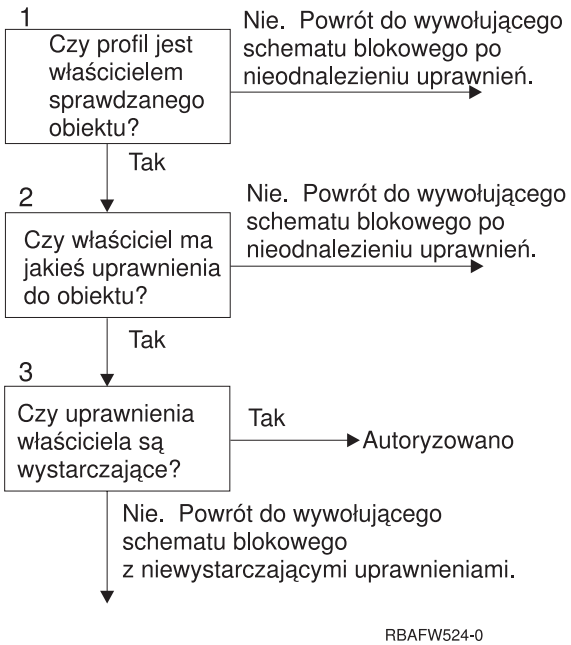
3. System sprawdza uprawnienia właściciela. Jeśli uprawnienia nie są wystarczające, wtedy przechodzi do Kroku 8. Jeśli nie zostaną odnalezione żadne uprawnienia, przechodzi do Kroku 4.
4. System kończy krotką ścieżkę sprawdzania uprawnień obiektu początkowego. (Patrz Schemat blokowy 5). Jeśli uprawnienia nie są wystarczające, proces sprawdzania uprawnień przechodzi do kroku 5.
5. System określa, czy obiekt ma uprawnienia prywatne. Jeśli tak, proces sprawdzania uprawnień przechodzi do Kroku 6. Jeśli nie, przechodzi do Kroku 7.
6. System sprawdza uprawnienia prywatne profilu użytkownika. Jeśli są wystarczające, użytkownik zostaje autoryzowany. Jeśli nie są wystarczające, proces sprawdzania uprawnień przechodzi do Kroku 8. Jeśli nie znaleziono żadnych uprawnień, proces sprawdzania przechodzi do Kroku 7.
7. System sprawdza, czy obiekt jest chroniony przez listę autoryzacji. Jeśli nie, przechodzi do Kroku 8. Jeśli jest chroniony przez listę autoryzacji, przechodzi do Kroku 9.
8. System ustawia obiekt na obiekt początkowy i powraca do wywołującego schematu blokowego z niewystarczającymi uprawnieniami lub brakiem uprawnień.
9. System ustawia obiekt na listę autoryzacji i powraca do Kroku 3.

Schemat blokowy 4: Jak sprawdzane są uprawnienia właściciela

Rys. 16 pokazuje proces sprawdzania uprawnień właściciela. Nazwa profilu właściciela oraz jego uprawnienia do obiektu przechowywane są razem z obiektem.

Podczas wykorzystywania uprawnień właściciela przy dostępie do obiektu, istnieje kilka możliwości:

- profil użytkownika jest właścicielem obiektu,
- profil użytkownika jest właścicielem listy autoryzacji,
- profil grupowy użytkownika jest właścicielem obiektu,
- profil grupowy użytkownika jest właścicielem listy autoryzacji,
- używane są uprawnienia adoptowane, a program właściciela jest właścicielem obiektu,
- używane są uprawnienia adoptowane, a program właściciela jest właścicielem listy autoryzacji.



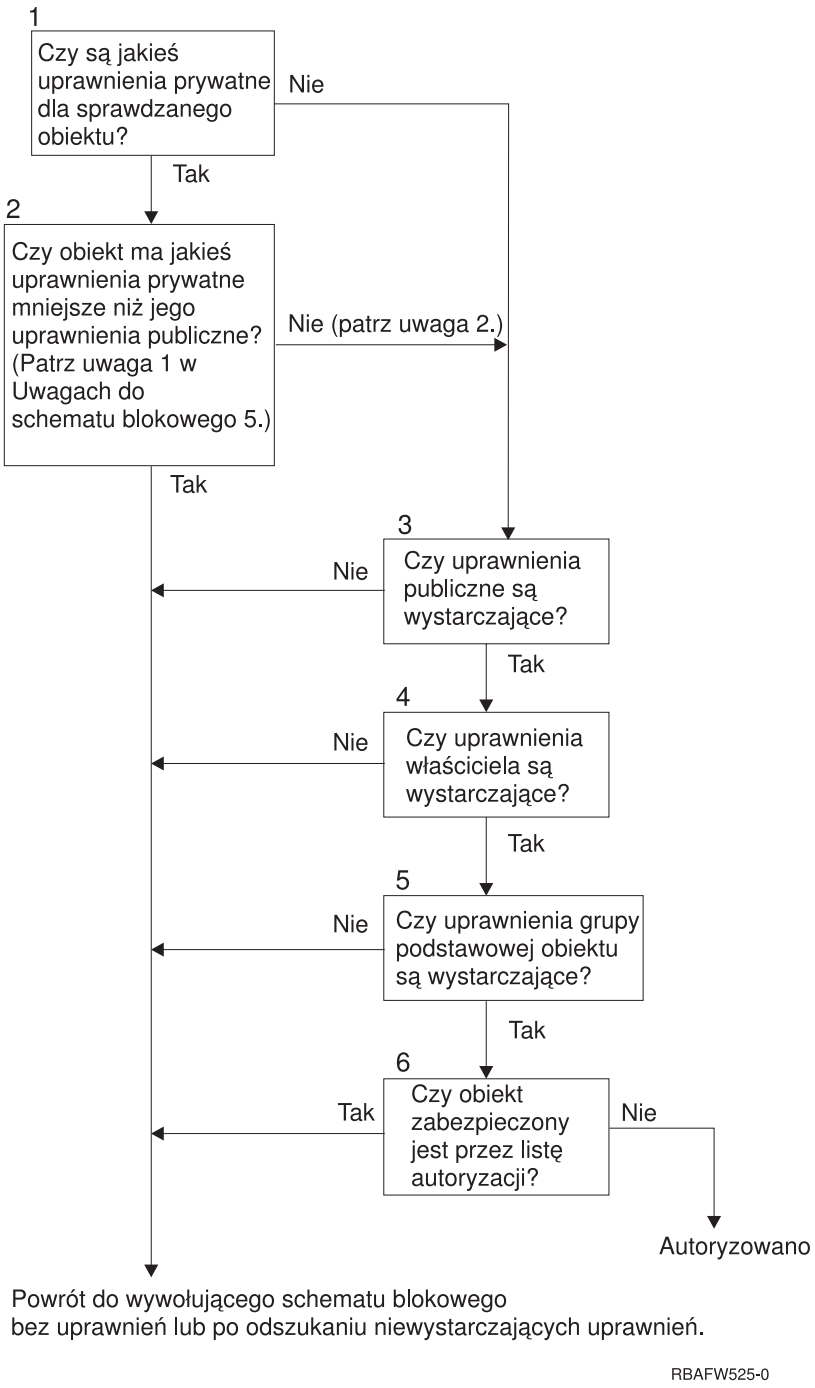
Rysunek 16. Schemat blokowy 4: Sprawdzanie uprawnień właściciela

Opis Schematu blokowego 4: Sprawdzanie uprawnień właściciela

1. System określa, czy profil użytkownika jest właścicielem sprawdzanego obiektu. Jeśli profil użytkownika jest właścicielem danego obiektu, system przechodzi do Kroku 2. Jeśli profil nie jest właścicielem danego obiektu, system powraca do wywołującego schematu blokowego bez odnalezienia uprawnień.
2. Jeśli profil użytkownika jest właścicielem obiektu, system określa czy, właściciel ma uprawnienia do obiektu. Jeśli użytkownik jest właścicielem, wtedy proces sprawdzania uprawnień przechodzi do Kroku 3. Jeśli system stwierdzi, że właściciel nie ma uprawnień do obiektu, wtedy przechodzi do wywołującego schematu blokowego bez odnalezienia uprawnień.
3. Jeśli właściciel nie ma uprawnień do obiektu, to system określa, czy to uprawnienie jest wystarczające, aby uzyskać dostęp do obiektu. Jeśli są, wtedy właściciel jest autoryzowany do danego obiektu. Jeśli nie są wystarczające, system powraca do wywołującego schematu blokowego z niewystarczającymi uprawnieniami.

Schemat blokowy 5: Krótka ścieżka sprawdzania uprawnień użytkownika

Rys. 17 na stronie 157 pokazuje krótką ścieżkę do testowania uprawnień użytkownika bez przeszukiwania uprawnień prywatnych.



Rysunek 17. Schemat blokowy 5: Krótka ścieżka dla uprawnień użytkownika

Uwagi dotyczące Schemat blokowy 5:

1. Uprawnienia są uważane za mniejsze niż publiczne, jeśli dowolne uprawnienia, które są obecne dla *PUBLIC, nie są obecne dla innego użytkownika. Tabela 115 ilustruje przykład, w którym użytkownicy publiczni mają do obiektu uprawnienia *OBJOPR, *READ i *EXECUTE. Użytkownik WILSONJ ma uprawnienia *EXCLUDE i nie ma żadnych uprawnień, które mają użytkownicy publiczni. Dlatego ten obiekt ma uprawnienia prywatne mniejsze niż jego uprawnienia publiczne. (Użytkownik OWNAR także ma uprawnienia mniejsze niż użytkownicy publiczni, ale uprawnienia właściciela nie są uważane za uprawnienia prywatne.)

Tabela 115. Uprawnienia publiczne a uprawnienia prywatne

	Użytkownicy			
Uprawnienie	**OWNAR**	**DPTMG**	**WILSONJ**	***PUBLIC**
Uprawnienia do obiektu:				
*OBJOPR		X		X
*OBJMGT	X			
*OBJEXIST				
*OBJALTER				
*OBJREF				
Uprawnienia do danych				
*READ		X		X
*ADD		X		
*UPD		X		
*DLT		X		
*EXECUTE		X		X
*EXCLUDE			X	

2. Ta ścieżka udostępnia metodę używania uprawnień publicznych, jeśli jest to możliwe, nawet jeśli dla obiektu istnieją uprawnienia prywatne. System sprawdza, czy napewno podczas procesu sprawdzania uprawnień nie zostanie odmówiony dostęp do obiektu. Jeśli wynik tych testów jest *wystarczający*, przeszukiwanie uprawnień prywatnych może być pominięte.

Opis Schematu blokowego 5: Krótka ścieżka dla uprawnień użytkownika

Ten schemat blokowy opisuje krótką ścieżkę testowania uprawnień użytkownika bez przeszukiwania uprawnień prywatnych.

1. System sprawdza, czy do sprawdzanego obiektu są jakieś uprawnienia prywatne. Jeśli są, proces sprawdzania uprawnień przechodzi do Kroku 2. Jeśli nie ma, przechodzi do Kroku 3.
2. Jeśli istnieją uprawnienia prywatne, system sprawdza, czy obiekt ma uprawnienia prywatne, które są mniejsze niż uprawnienia publiczne. (Patrz Uwaga 1.) Jeśli obiekt ma uprawnienia prywatne, które są mniejsze niż uprawnienia publiczne, system powraca do wywołującego schematu blokowego z brakiem uprawnień lub z niewystarczającymi uprawnieniami. Jeśli obiekt nie ma uprawnień prywatnych, które są mniejsze niż jego uprawnienia publiczne, (patrz Uwaga 2), wtedy proces sprawdzania uprawnień przechodzi do Kroku 3.
3. Jeśli obiekt nie ma uprawnień prywatnych, które są mniejsze niż jego uprawnienia publiczne, system sprawdza, czy uprawnienia publiczne są wystarczające. Jeśli uprawnienia publiczne są wystarczające, proces sprawdzania uprawnień przechodzi do Kroku 4. Jeśli uprawnienia publiczne nie są wystarczające, system powraca do wywołującego schematu blokowego z brakiem uprawnień lub niewystarczającymi uprawnieniami.
4. Jeśli uprawnienia publiczne są wystarczające, system sprawdza, czy wystarczające są uprawnienia właściciela obiektu. Jeśli są, proces sprawdzania uprawnień przechodzi do Kroku 5. Jeśli uprawnienia właściciela obiektu nie są wystarczające, system powraca do wywołującego schematu blokowego z brakiem uprawnień lub niewystarczającymi uprawnieniami.
5. Jeśli uprawnienia właściciela obiektu są wystarczające, system sprawdza, czy wystarczające są uprawnienia grupy podstawowej obiektu. Jeśli są wystarczające, proces sprawdzania uprawnień przechodzi do Kroku 6. Jeśli nie są wystarczające, system powraca do wywołującego schematu blokowego z brakiem uprawnień lub z niewystarczającymi uprawnieniami.
6. Jeśli uprawnienia grupy podstawowej obiektu są wystarczające, system określa, czy obiekt zabezpieczany jest listą autoryzacji. Jeśli jest zabezpieczany taką listą, system powraca do wywołującego schematu blokowego bez uprawnień lub z niewystarczającymi uprawnieniami. Jeśli obiekt nie jest zabezpieczany listą autoryzacji, użytkownik jest autoryzowany do używania obiektu.

Schemat blokowy 6: Jak sprawdzane są uprawnienia grupowe

Użytkownik może być członkiem nawet 16 grup. Grupa może mieć uprawnienia prywatne do obiektu lub może być grupą podstawową dla obiektu.

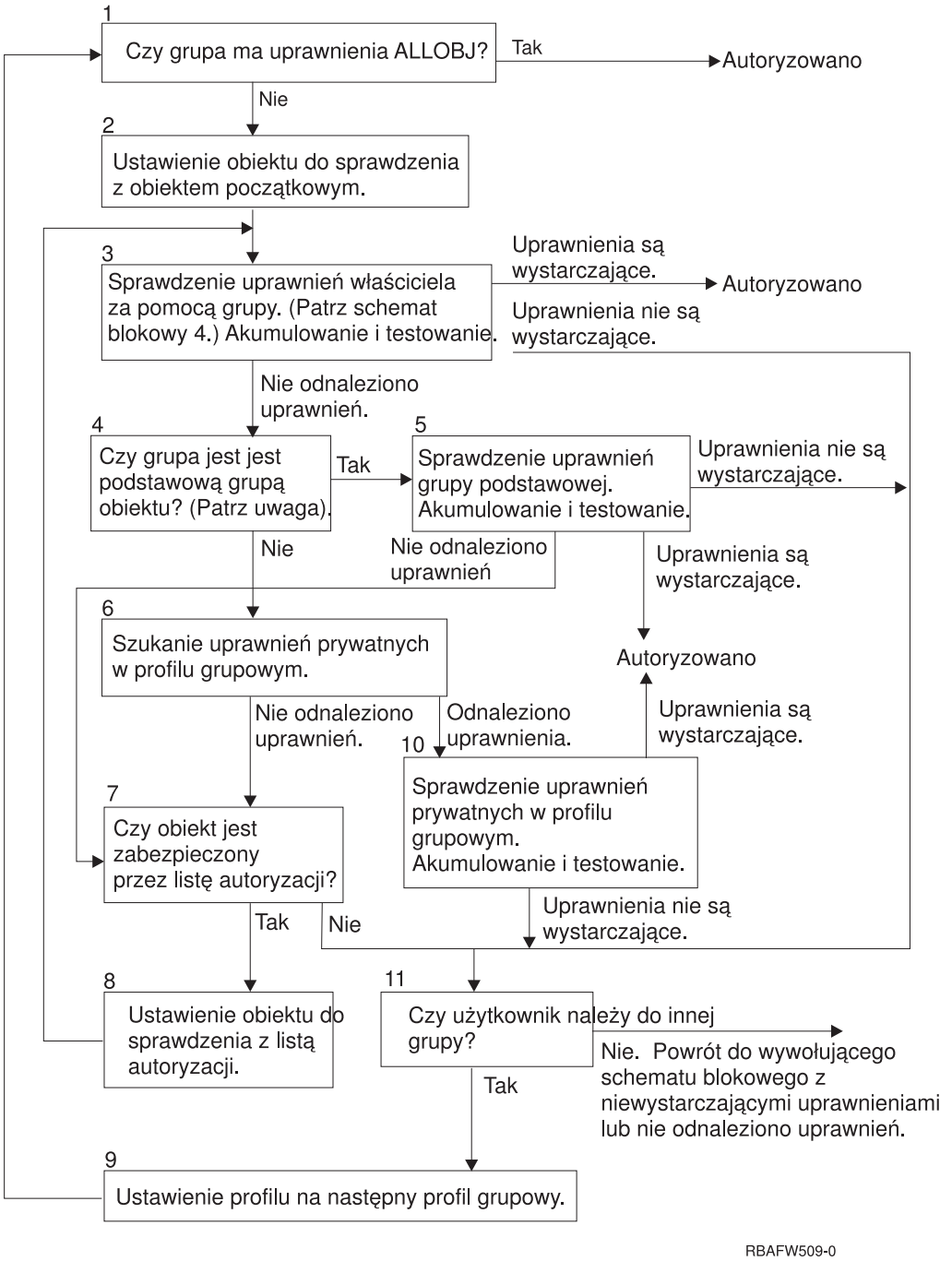
Aby odszukać wystarczające uprawnienia do obiektu, mogą być kumulowane uprawnienia z jednej lub więcej grup użytkownika. Na przykład użytkownik WAGNERB potrzebuje uprawnień *CHANGE do zbioru CRLIM. Uprawnienia *CHANGE obejmują uprawnienia *OBJOPR, *READ, *ADD, *UPD, *DLT i *EXECUTE. Tabela 116 pokazuje uprawnienia do zbioru CRLIM:

Tabela 116. Skumulowane uprawnienia grupowe

	Użytkownicy			
Uprawnienie	**OWNAR**	**DPT506**	**DPT702**	***PUBLIC**
Uprawnienia do obiektu:				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
Uprawnienia do danych				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X	X	
*DLT	X		X	
*EXECUTE	X	X	X	
*EXCLUDE				X

Użytkownik WAGNERB musi być zarówno członkiem grupy DPT506, jak i DPT702, aby uzyskać wystarczające uprawnienia do zbioru CRLIM. Grupa DPT506 nie ma uprawnień *DLT, a DPT702 uprawnień *ADD.

Schemat blokowy 6 na stronie 160 opisuje kroki w procesie sprawdzania uprawnień grupowych.



Rysunek 18. Schemat blokowy 6: Sprawdzanie uprawnień grupowych.

Uwaga: Jeśli użytkownik wpisany jest za pomocą profilu, który jest grupą podstawową dla obiektu, nie może uzyskać uprawnień do obiektu za pośrednictwem grupy podstawowej.

Opis Schematu blokowego 6: Sprawdzanie uprawnień grupowych

1. System sprawdza, czy grupa ma uprawnienia *ALLOBJ. Jeśli tak, to jest autoryzowana. Jeśli nie, proces sprawdzania uprawnień przechodzi do Kroku 2.
2. Jeśli grupa nie ma uprawnień ALLOBJ, system ustawia sprawdzany obiekt na obiekt początkowy.

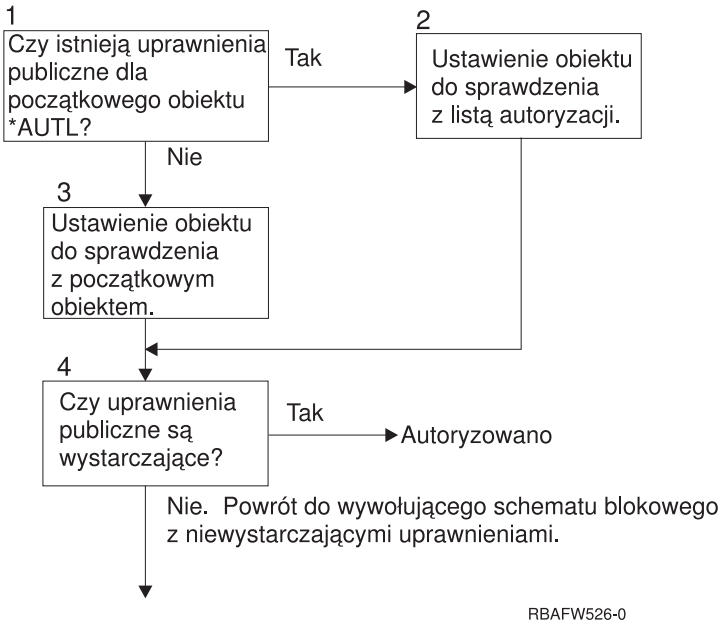
3. Po ustawieniu obiektu początkowego, system sprawdza uprawnienia właściciela (patrz Schemat blokowy 4). Jeśli uprawnienia są wystarczające, wtedy grupa jest autoryzowana. Jeśli uprawnienia nie są wystarczające, wtedy sprawdzanie uprawnień przechodzi do Kroku 7. Jeśli uprawnienia nie zostały odnalezione, sprawdzanie uprawnień przechodzi do Kroku 4.
4. Jeśli uprawnienia właściciela nie zostaną odnalezione, system sprawdza, czy grupa jest grupą podstawową obiektu.

   Uwaga: Jeśli użytkownik wpisany jest za pomocą profilu, który jest grupą podstawową dla obiektu, użytkownik nie może uzyskać uprawnień do obiektu za pośrednictwem grupy podstawowej.

   Jeśli grupa jest grupa podstawową obiektu, wtedy proces sprawdzania uprawnień przechodzi do Kroku 5. Jeśli grupa nie jest grupą podstawową obiektu, proces przechodzi do Kroku 6.
5. Jeśli grupa jest grupą podstawową obiektu, system sprawdza i testuje uprawnienia grupy podstawowej. Jeśli uprawnienia grupy podstawowej są wystarczające, grupa jest autoryzowana. Jeśli uprawnienia grupy podstawowej nie są wystarczające lub nie zostały odnalezione, sprawdzanie uprawnień przechodzi do Kroku 7.
6. Jeśli grupa nie jest grupą podstawową obiektu, system sprawdza uprawnienia prywatne w profilu grupowym. Jeśli uprawnienia zostaną odnalezione, proces sprawdzania uprawnień przechodzi do Kroku 10. Jeśli uprawnienia nie zostaną odnalezione, proces ten przechodzi do Kroku 7.
7. Jeśli dla profilu grupowego uprawnienia prywatne nie zostaną odnalezione, system sprawdza, czy obiekt jest chroniony przez listę autoryzacji. Jeśli jest, wtedy proces sprawdzania uprawnień przechodzi do Kroku 8. Jeśli nie, proces przechodzi do Kroku 11.
8. Jeśli obiekt jest chroniony przez listę autoryzacji, system ustawia obiekt na listę autoryzacji, a proces sprawdzania uprawnień powraca do Kroku 3.
9. Jeśli użytkownik należy do innego profilu grupowego, system ustawia ten profil jako następny profil grupowy i powraca do Kroku 1, aby ponownie rozpocząć proces sprawdzania uprawnień.
10. Jeśli uprawnienia prywatne zostaną odnalezione w profilu grupowym, wtedy uprawnienia te są sprawdzane i testowane w profilu grupowym. Jeśli uprawnienia są wystarczające, wtedy profil grupowy jest autoryzowany. Jeśli nie są wystarczające, wtedy proces sprawdzania uprawnień przechodzi do Kroku 7.
11. Jeśli obiekt nie jest jest chroniony przez listę autoryzacji, system sprawdza, czy użytkownicy powiązani są z innym profilem grupowym. Jeśli użytkownik nie należy do innego profilu grupowego, system przechodzi do Kroku 9. Jeśli użytkownik nie należy do innego profilu grupowego, system powraca do wywołującego schematu blokowego z niewystarczającymi uprawnieniami lub brakiem uprawnień.

Schemat blokowy 7: Jak sprawdzane są uprawnienia publiczne

Podczas sprawdzania uprawnień publicznych system musi określić, czy do obiektu lub listy autoryzacji mają być użyte uprawnienia publiczne. Proces ten pokazuje Schemat blokowy 7:



Rysunek 19. Schemat blokowy 7: Sprawdzanie uprawnień publicznych

Opis Schematu blokowego 7: Sprawdzanie uprawnień publicznych

Schemat blokowy 7 pokazuje, w jaki sposób system określa, czy do obiektu lub listy autoryzacji mają być użyte uprawnienia publiczne.

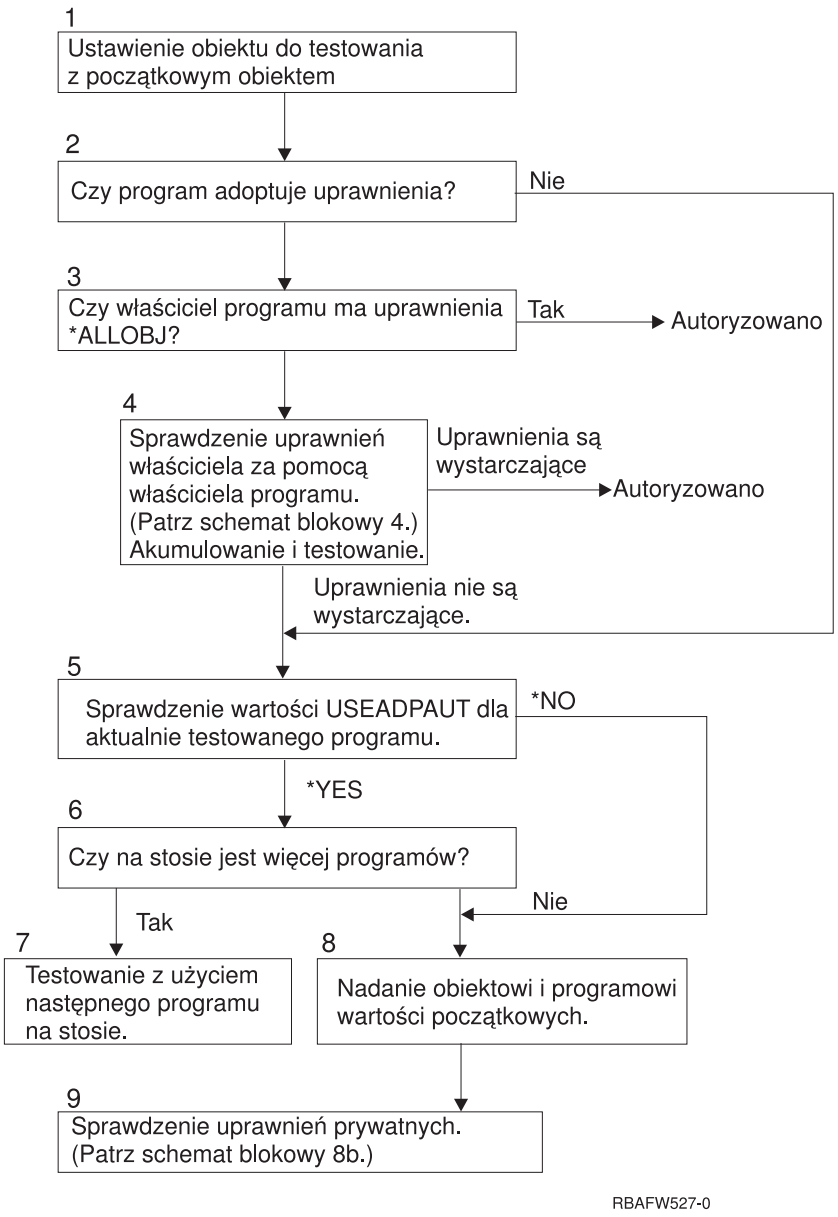
1. System określa, czy uprawnienia publiczne do obiektu początkowego to uprawnienia *AUTL. Jeśli uprawnienia publiczne do obiektu początkowego to *AUTL, system przechodzi do Kroku 2. Jeśli uprawnienia do tego obiektu nie są uprawnieniami *AUTL, system przechodzi do Kroku 3.
2. Jeśli uprawnienia publiczne do obiektu początkowego to uprawnienia *AUTL, system ustawia sprawdzany obiekt na listę autoryzacji i przechodzi do Kroku 4.
3. Jeśli nie są to uprawnienia *AUTL, system ustawia sprawdzany obiekt na początkowy i przechodzi do Kroku 4.
4. Jeśli sprawdzany obiekt został ustawiony na listę autoryzacji lub obiekt początkowy, system określa, czy uprawnienia publiczne są wystarczające. Jeśli są, wtedy użytkownik otrzymuje uprawnienia do danego obiektu. Jeśli nie są, system powraca do wywołującego schematu blokowego z niewystarczającymi uprawnieniami.

Schemat blokowy 8: Jak sprawdzane są uprawnienia adoptowane

Jeśli podczas sprawdzania uprawnień użytkownika uprawnienia będą niewystarczające, system sprawdza uprawnienia adoptowane. System może użyć uprawnień adoptowanych z programu, który wywołał użytkownik, lub z programu poprzedzającego go na stosie programów. Aby zapewnić najlepszą wydajność i zminimalizować liczbę przeszukiwań uprawnień prywatnych, proces sprawdzania uprawnień adoptowanych sprawdza, czy właściciel programu ma uprawnienia specjalne *ALLOBJ lub czy jest właścicielem testowanego obiektu. Operacja ta powtarzana jest dla każdego programu znajdującego się na stosie i używającego uprawnień adoptowanych.

Jeśli nie zostaną odnalezione wystarczające uprawnienia, system sprawdza, czy właściciel program ma uprawnienia prywatne do sprawdzanego obiektu. Powtarzane to jest dla każdego programu znajdującego się na stosie i używającego uprawnień adoptowanych.

Rys. 20 na stronie 163 i Rys. 21 na stronie 165 pokazują proces sprawdzania uprawnień adoptowanych.



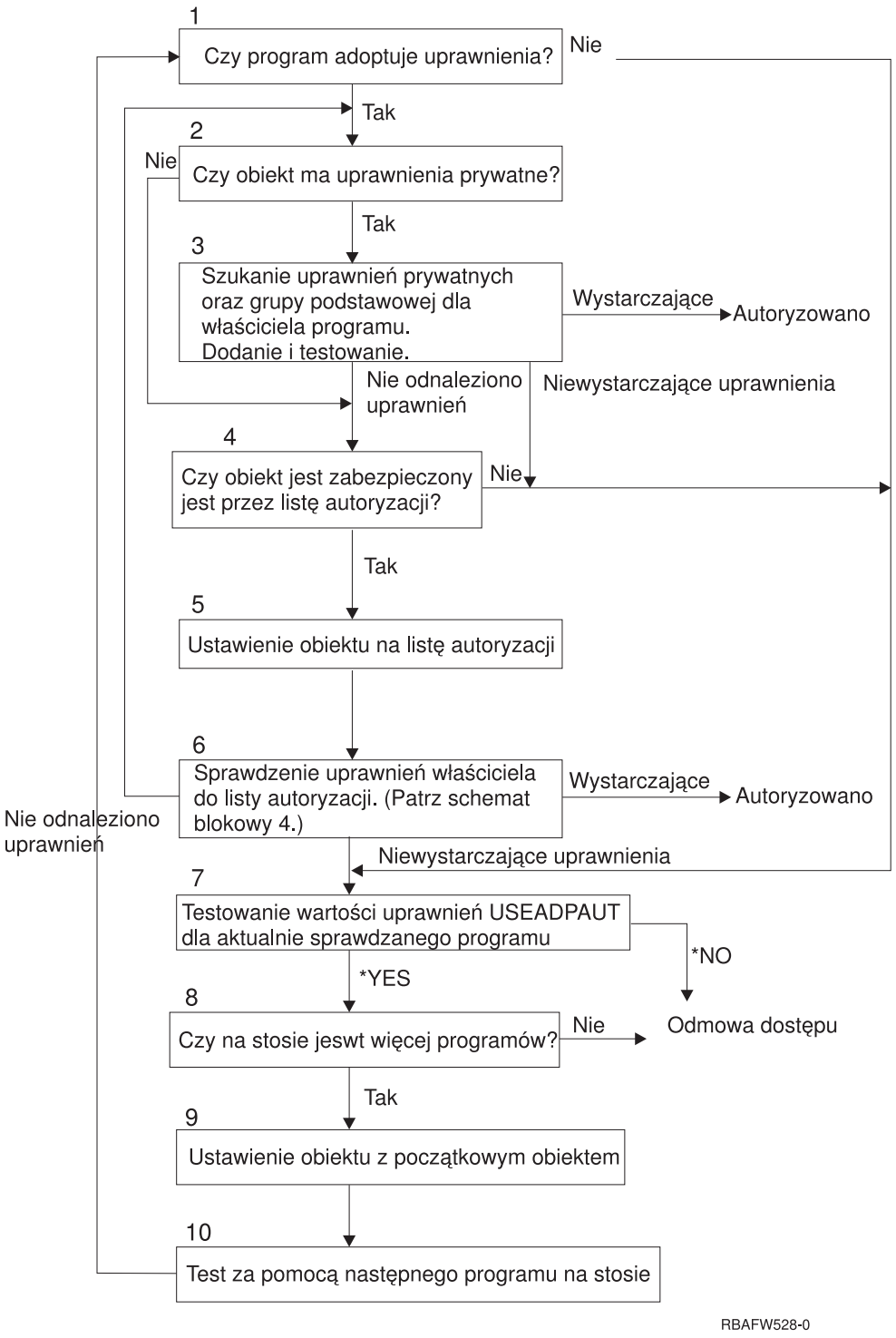
*Rysunek 20. Schemat blokowy 8A: Sprawdzanie uprawnień adoptowanych użytkownika: *ALLOBJ i właściciela*

Opis Schematu blokowego 8A: Sprawdzanie uprawnień adoptowanych użytkownika: *ALLOBJ i właściciela

Schemat blokowy 8A opisuje sposób sprawdzania przez system uprawnień adoptowanych, gdy podczas sprawdzania uprawnień użytkownika nie zostały odnalezione wystarczające uprawnienia.

1. System ustawia sprawdzany obiekt na obiekt początkowy i przechodzi do Kroku 2.
2. System określa, czy program adoptuje uprawnienia. Jeśli tak, wtedy proces sprawdzania uprawnień przechodzi do Kroku 3. Jeśli nie, a uprawnienia nie są wystarczające, wtedy sprawdzanie uprawnień przechodzi do Kroku 5.
3. Jeśli program adoptuje uprawnienia, system określa, czy właściciel programu ma uprawnienia *ALLOBJ. Jeśli właściciel programu ma uprawnienia *ALLOBJ, wtedy użytkownik jest autoryzowany. Jeśli właściciel programu nie ma uprawnień *ALLOBJ, wtedy proces sprawdzania uprawnień przechodzi do Kroku 4.
4. Jeśli właściciel programu nie ma uprawnień *ALLOBJ, system sprawdza i testuje uprawnienia właściciela. Jeśli są wystarczające, użytkownik zostaje autoryzowany. Jeśli uprawnienia nie są wystarczające, przechodzi do kroku 5.

5. System sprawdza wartość USEADPAUT dla aktualnie testowanego programu. Jeśli wartość jest równa *NO, wtedy proces sprawdzania uprawnień przechodzi do Kroku 8. Jeśli wartość jest równa *YES, proces sprawdzania przechodzi do Kroku 6.
6. Jeśli wartość USEADPAUT jest równa *YES, system określa, czy na stosie oczekuje więcej programów. Jeśli tak, proces sprawdzania uprawnień przechodzi do Kroku 7. Jeśli nie, proces przechodzi do Kroku 8.
7. Jeśli na stosie znajduje się więcej programów, system testuje następny program ze stosu.
8. Jeśli na stosie nie ma więcej programów lub wartość USEADPAUT jest równa *NO, system ustawia obiekt i program na wartości początkowe i przechodzi do Kroku 9.
9. System sprawdza uprawnienia prywatne. Opis procesu można znaleźć w sekcji Schemat blokowy 8B: Sprawdzanie uprawnień adoptowanych za pomocą uprawnień prywatnych.



Rysunek 21. Schemat blokowy 8B: Sprawdzanie uprawnień adoptowanych za pomocą uprawnień prywatnych

Opis Schematu blokowego 8B: Sprawdzanie uprawnień adoptowanych za pomocą uprawnień prywatnych

1. System sprawdza, czy program może adoptować uprawnienia. Jeśli tak, przechodzi do Kroku 2. Jeśli nie, przechodzi do Kroku 7.
2. System określa, czy obiekt ma uprawnienia prywatne. Jeśli tak, przechodzi do Kroku 3. Jeśli nie, przechodzi do Kroku 4.

3. System sprawdza uprawnienia prywatne oraz grupy podstawowej dla właściciela programu. Jeśli uprawnienia są wystarczające, program jest autoryzowany.Jeśli nie są wystarczające, przechodzi do Kroku 7. Jeśli nie odnaleziono żadnych uprawnień, przechodzi do Kroku 4.
4. System sprawdza, czy obiekt jest chroniony przez listę autoryzacji. Jeśli tak, przechodzi do Kroku 5. Jeśli nie, przechodzi do Kroku 7.
5. System ustawia obiekt na listę autoryzacji i przechodzi do Kroku 6.
6. System sprawdza uprawnienia właściciela do listy autoryzacji. (Patrz Schemat blokowy 4). Jeśli nie zostaną odnalezione żadne uprawnienia, wraca do Kroku 2. Jeśli odnalezione zostaną wystarczające uprawnienia, program jest autoryzowany.
7. System sprawdza wartość systemową USEADPAUT dla aktualnie sprawdzanego programu. Jeśli jest równa *YES, przechodzi do Kroku 8. Jeśli jest równa *NO, żądanie dostępu jest odrzucane.
8. System sprawdza, czy na stosie znajduje się więcej programów. Jeśli tak, przechodzi do Kroku 9. Jeśli nie, żądanie dostępu jest odrzucane.
9. System ustawia obiekt na obiekt początkowy i przechodzi do Kroku 10.
10. Test za pomocą następnego programu ze stosu i powrót do Kroku 1.

Przykłady sprawdzania uprawnień

Poniżej przedstawiono kilka przykładów sprawdzania uprawnień. Te przykłady demonstrują kroki podejmowane przez system w celu ustalenia, czy użytkownik może uzyskać dostęp do żądanego obiektu. Te przykłady demonstrują sposób działania sprawdzania uprawnień oraz pokazują, gdzie mogą wystąpić potencjalne problemy związane z wydajnością.

Rys. 22 pokazuje uprawnienia do zbioru PRICES. Poniżej pokazano kilka przykładów żądania dostępu do tego zbioru i proces sprawdzania uprawnień. W przykładach proces sprawdzania uprawnień prywatnych (Schemat blokowy 4, Krok 6) został wyróżniony, ponieważ jest tą częścią procesu sprawdzania uprawnień, która może powodować problemy związane z wydajnością, gdy jest powtarzany kilka razy.

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   PRICES          Właściciel . . . . . :   OWNCP
  Biblioteka . . . :   CONTRACTS     Grupa podstawowa . . :   *NONE
Typ obiektu  . . . :   *FILE         Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji . . . . . :   *NONE

                       Uprawnienia
Użytkownik  Grupa      do obiektu
OWNCP                  *ALL
DPTSM                  *CHANGE
DPTMG                  *CHANGE
WILSONJ                *USE
*PUBLIC                *USE
```

Rysunek 22. Uprawnienia do zbioru PRICES

Przypadek 1: Używanie prywatnych uprawnień grupowych

Użytkownik ROSSM chce uzyskać dostęp do zbioru PRICES korzystając z programu CPPGM01. Program CPPGM01 wymaga uprawnień *CHANGE do zbioru. Użytkownik ROSSM jest członkiem profilu grupowego DPTSM. Ani użytkownik ROSSM, ani profil DPTSM nie mają uprawnień specjalnych *ALLOBJ. W celu określenia, czy umożliwić użytkownikowi ROSSM dostęp do zbioru PRICES, system wykonuje następujące kroki:

1. Schemat blokowy 1, krok 1.
   a. Schemat blokowy 2, krok 1.
2. Schemat blokowy 1, krok 2.

a. Schemat blokowy 3, kroki 1 i 2. Obiekt do sprawdzenia = CONTRACTS/PRICES *FILE.
b. Schemat blokowy 3, krok 3.
   1) Schemat blokowy 4, krok 1. Powrót do Schematu blokowego 3 bez odnalezienia uprawnień. ROSSM nie jest właścicielem zbioru PRICES.
c. Schemat blokowy 3, krok 4.
   1) Schemat blokowy 5, kroki 1, 2 i 3. Uprawnienia publiczne nie są wystarczające.
d. Schemat blokowy 3, krok 5.
e. **Schemat blokowy 3, krok 6**. ROSSM nie ma uprawnień prywatnych do zbioru PRICES.
f. Schemat blokowy 3, kroki 7 i 8. Zbiór PRICES nie jest zabezpieczony listą autoryzacji. Powrót do Schematu blokowego 1 bez odnalezienia uprawnień.

3. Schemat blokowy 1, kroki 3 i 4. DPTSM jest profilem grupowym użytkownika ROSSM.
   a. Schemat blokowy 6, kroki 1, 2 i 3.
      1) Schemat blokowy 4, krok 1. DPTSM nie jest właścicielem zbioru PRICES.
   b. Schemat blokowy 6, krok 4. DPTSM nie jest grupą podstawową dla zbioru PRICES.
   c. **Schemat blokowy 6, krok 6**. Autoryzowanie. (DPTSM ma uprawnienia *CHANGE.)

Rezultat: Użytkownik ROSSM został autoryzowany, ponieważ profil grupowy DPTSM ma uprawnienia *CHANGE.

Analiza: Użycie uprawnień grupowych w tym przykładzie jest dobrym sposobem na zarządzanie uprawnieniami. Zmniejsza liczbę uprawnień prywatnych w systemie i jest łatwe do zrozumienia oraz kontrolowania. Użycie prywatnego uprawnienia grupowego najczęściej powoduje dwa wyszukiwania uprawnień prywatnych (dla użytkownika i grupy), gdy uprawnienia publiczne nie są wystarczające. Jednego wyszukiwania uprawnienia prywatnego można uniknąć, ustawiając DPTSM jako grupę podstawową dla zbioru PRICES.

Przypadek 2: Używanie uprawnień grupy podstawowej

Użytkownik ANDERSJ potrzebuje uprawnień *CHANGE do zbioru CREDIT. Użytkownik ANDERSJ jest członkiem grupy DPTAR. Ani użytkownik ANDERSJ, ani profil DPTAR nie mają uprawnień specjalnych *ALLOBJ. Rys. 23 pokazuje uprawnienia do zbioru CREDIT.

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   CREDIT          Właściciel . . . . . :   OWNAR
  Biblioteka . . . :   ACCTSRCV      Grupa podstawowa . . :   DPTAR
Typ obiektu  . . . :   *FILE         Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji . . . . . :   *NONE

                       Uprawnienia
Użytkownik  Grupa      do obiektu
OWNAR                  *ALL
DPTAR                  *CHANGE
*PUBLIC                *USE
```

Rysunek 23. Uprawnienia do zbioru CREDIT

Aby określić, czy użytkownik ANDERSJ może uzyskać dostęp do zbioru CREDIT z wykorzystaniem uprawnień *CHANGE, system wykonuje następujące kroku:

1. Schemat blokowy 1, krok 1.
   a. Schemat blokowy 2, krok 1. Uprawnienia profilu DPTAR są uprawnieniami grupy podstawowej, a nie uprawnieniami prywatnymi.
   b. Schemat blokowy 2, kroki 2, 3, 4, 5 i 6. Uprawnienia publiczne nie są wystarczające.
2. Schemat blokowy 1, krok 2.

a. Schemat blokowy 3, kroki 1 i 2. Obiekt do sprawdzenia = ACCTSRCV/CREDIT *FILE.
b. Schemat blokowy 3, krok 3.
   1) Schemat blokowy 4, krok 1. Użytkownik ANDERSJ nie jest właścicielem zbioru CREDIT. Powrót do Schematu blokowego 3 bez odnalezienia uprawnień.
c. Schemat blokowy 3, krok 4.
   1) Schemat blokowy 5, krok 1. Zbiór CREDIT nie ma uprawnień prywatnych.
   2) Schemat blokowy 5, krok 3. Uprawnienia publiczne nie są wystarczające. Powrót do Schematu blokowego 3 bez odnalezienia uprawnień.
d. Schemat blokowy 3, kroki 5, 7 i 8. Zbiór CREDIT nie jest chroniony przez listę autoryzacji. Powrót do Schematu blokowego 1 bez odnalezienia uprawnień.

3. Schemat blokowy 1, kroki 3 i 4. Użytkownik ANDERSJ jest członkiem profilu grupowego DPTAR.
   a. Schemat blokowy 6, kroki 1 i 2. Obiekt do sprawdzenia = ACCTSRCV/CREDIT *FILE.
   b. Schemat blokowy 6, krok 3.
      1) Schemat blokowy 4, krok 1. Profil DPTAR nie jest właścicielem zbioru CREDIT. Powrót do Schemat blokowy 6 bez odnalezienia uprawnień.
   c. Schemat blokowy 6, kroki 4 i 5. Autoryzowanie. Profil DPTAR jest grupą podstawową dla zbioru CREDIT i ma uprawnienia *CHANGE.

Rezultat: Użytkownik ANDERSJ został autoryzowany, ponieważ profil DPTAR jest grupą podstawową dla zbioru CREDIT i ma uprawnienia *CHANGE.

Analiza: Jeśli używane są uprawnienia grupy podstawowej, wydajność sprawdzania uprawnień jest lepsza, niż jeśli dla grupy podane zostaną uprawnienia prywatne. Ten przykład nie wymaga przeszukiwania uprawnień prywatnych.

Przypadek 3: Używanie uprawnień publicznych

Użytkownik JONESP chce uzyskać dostęp do zbioru CREDIT korzystając z programu CPPGM06. Program CPPGM06 wymaga uprawnień *USE do zbioru. Użytkownik JONESP jest członkiem profilu grupowego DPTSM i nie ma uprawnień specjalnych *ALLOBJ. W celu określenia, czy umożliwić użytkownikowi JONESP dostęp do zbioru CREDIT, system wykonuje następujące kroki:

1. Schemat blokowy 1, krok 1.
   a. Schemat blokowy 2, krok 1. Zbiór CREDIT nie ma uprawnień prywatnych. Uprawnienia profilu DPTAR są uprawnieniami grupy podstawowej, a nie uprawnieniami prywatnymi.
   b. Schemat blokowy 2, kroki 2 i 3. Uprawnienia właściciela (OWNAR) są wystarczające.
   c. Schemat blokowy 2, kroki 4 i 5. Uprawnienia grupy podstawowej (DPTAR) są wystarczające.
   d. Schemat blokowy 2, krok 6. Autoryzowanie. Uprawnienia publiczne są wystarczające.

Analiza: Ten przykład pokazuje korzyści związane z wydajnością, osiągane gdy unika się definiowania uprawnień prywatnych dla obiektu.

Przypadek 4: Używanie uprawnień publicznych bez przeszukiwania uprawnień prywatnych

Użytkownik JONESP chce uzyskać dostęp do zbioru PRICES korzystając z programu CPPGM06. Program CPPGM06 wymaga uprawnień *USE do zbioru. Użytkownik JONESP jest członkiem profilu grupowego DPTSM i nie ma uprawnień specjalnych *ALLOBJ. W celu określenia, czy umożliwić użytkownikowi JONESP dostęp do zbioru PRICES, system wykonuje następujące kroki:

1. Schemat blokowy 1, krok 1.
   a. Schemat blokowy 2, krok 1. Zbiór PRICES ma uprawnienia prywatne.
2. Schemat blokowy 1, krok 2.
   a. Schemat blokowy 3, kroki 1 i 2. Obiekt do sprawdzenia = CONTRACTS/PRICES *FILE.
   b. Schemat blokowy 3, krok 3.

1) Schemat blokowy 4, krok 1. JONESP nie jest właścicielem zbioru PRICES. Powrót do Schematu blokowego 3 bez odnalezienia uprawnień.

c. Schemat blokowy 3, krok 4.

1) Schemat blokowy 5, kroki 1, 2 i 3. Uprawnienia publiczne są wystarczające.

2) Schemat blokowy 5, krok 4. Uprawnienia właściciela są wystarczające. (OWNCP ma uprawnienia *ALL.)

3) Schemat blokowy 5, krok 5. Zbiór PRICES nie ma grupy podstawowej.

4) Schemat blokowy 5, krok 6. Autoryzowanie. (Zbiór PRICES nie jest zabezpieczony listą autoryzacji.)

Analiza: Ten przykład pokazuje korzyści związane z wydajnością, osiągane gdy unika się definiowania uprawnień prywatnych dla obiektu, które są mniejsze niż uprawnienia publiczne. Chociaż dla zbioru PRICES istnieją uprawnienia prywatne, uprawnienia publiczne są wystarczające dla tego żądania i mogą być użyte bez konieczności przeszukiwania uprawnień prywatnych.

Przypadek 5: Używanie uprawnień adoptowanych

Użytkownik SMITHG chce uzyskać dostęp do zbioru PRICES korzystając z programu CPPGM08. Użytkownik SMITHG nie jest członkiem grupy i nie ma uprawnień specjalnych *ALLOBJ. Program CPPGM08 wymaga uprawnień *CHANGE do zbioru. Program CPPGM08 jest w posiadaniu profilu OWNCP i adoptuje uprawnienia właściciela (parametr USRPRF ma wartość *OWNER).

1. Schemat blokowy 1, krok 1.
   a. Schemat blokowy 2, krok 1.
2. Schemat blokowy 1, krok 2.
   a. Schemat blokowy 3, kroki 1 i 2. Obiekt do sprawdzenia = CONTRACTS/PRICES *FILE.
   b. Schemat blokowy 3, krok 3.
      1) Schemat blokowy 4, krok 1. SMITHG nie jest właścicielem zbioru PRICES. Powrót do Schematu blokowego 3 bez odnalezienia uprawnień.
   c. Schemat blokowy 3, krok 4.
      1) Schemat blokowy 5, kroki 1, 2 i 3. Uprawnienia publiczne nie są wystarczające.
   d. Schemat blokowy 3, krok 5.
   e. **Schemat blokowy 3, krok 6**. Użytkownik SMITHG nie ma uprawnień prywatnych.
   f. Schemat blokowy 3, kroki 7 i 8. Zbiór PRICES nie jest zabezpieczony listą autoryzacji. Powrót do Schematu blokowego 1 bez odnalezienia uprawnień.
3. Schemat blokowy 1, krok 3. Użytkownik SMITHG nie ma grupy.
4. Schemat blokowy 1, krok 5.
   a. Schemat blokowy 7, krok 1. Uprawnienia publiczne nie mają wartości *AUTL.
   b. Schemat blokowy 7, krok 3. Obiekt do sprawdzenia = CONTRACTS/PRICES *FILE.
   c. Schemat blokowy 7, krok 4. Uprawnienia publiczne nie są wystarczające.
5. Schemat blokowy 1, krok 6.
   a. Schemat blokowy 8A, krok 1. Obiekt do sprawdzenia = CONTRACTS/PRICES *FILE.
   b. Schemat blokowy 8A, kroki 2 i 3. Użytkownik OWNCP nie ma uprawnień *ALLOBJ.
   c. Schemat blokowy 8A, krok 4.
      1) Schemat blokowy 4, kroki 1, 2 i 3. Autoryzowanie. Użytkownik OWNCP jest właścicielem zbioru PRICES i ma wystarczające uprawnienia.

Analiza: Ten przykład demonstruje korzyści związane z wydajnością podczas używania uprawnień adoptowanych, gdy właściciel programu jest również właścicielem obiektow aplikacji.

Liczba czynności wymaganych do przeprowadzania sprawdzania uprawnień nie ma prawie żadnego wpływu na wydajność, ponieważ większość czynności nie wymaga wczytywania nowych informacji. W tym przykładzie, chociaż wykonywanych jest wiele kroków, uprawnienia prywatne sprawdzane są tylko jeden raz (dla użytkownika SMITHG).

Można to porównać z Przypadkiem 1 ze strony "Przypadek 1: Używanie prywatnych uprawnień grupowych" na stronie 166.

- Jeśli Przypadek 1 zostanie zmieniony tak, że profil DPTSM będzie właścicielem zbioru PRICES i będzie miał do niego uprawnienia *ALL, parametry wydajności dla obu przykładów będą takie same. Jednak profil grupowy, który jest właścicielem obiektów aplikacji, powoduje ryzyko naruszenia ochrony. Członkowie grupy zawsze mają uprawnienia grupy (właściciela), chyba że wyraźnie otrzymają mniejsze uprawnienia. Gdy używane są uprawnienia adoptowane, można kontrolować sytuacje, w których używane są uprawnienia właściciela.
- Można także zmienić Przypadek 1 tak, aby profil DPTSM był podstawową grupą dla zbioru PRICES i miał uprawnienie *CHANGE. Jeśli profil DPTSM jest pierwszą grupą dla użytkownika SMITHG (podaną w parametrze GRPPRF jego profilu użytkownika), parametry wydajności będą takie same jak dla Przypadku 5.

Przypadek 6: Uprawnienia użytkownika i grupowe

Użytkownik WILSONJ chce uzyskać dostęp do zbioru PRICES korzystając z programu CPPGM01, który wymaga uprawnień *CHANGE. Użytkownik WILSONJ jest członkiem profilu grupowego DPTSM i nie ma uprawnień specjalnych *ALLOBJ. Program CPPGM01 nie używa uprawnień adoptowanych i ignoruje wszystkie poprzednie uprawnienia adoptowane (parametr USEADPAUT ma wartość *NO).

1. Schemat blokowy 1, krok 1.
   a. Schemat blokowy 2, krok 1. Zbiór PRICES ma uprawnienia prywatne.
2. Schemat blokowy 1, krok 2.
   a. Schemat blokowy 3, kroki 1 i 2. Obiekt do sprawdzenia = CONTRACTS/PRICES *FILE.
   b. Schemat blokowy 3, krok 3.
      1) Schemat blokowy 4, krok 1. WILSONJ nie jest właścicielem zbioru PRICES. Powrót do Schematu blokowego 3 bez odnalezienia uprawnień.
   c. Schemat blokowy 3, krok 4.
      1) Schemat blokowy 5, kroki 1, 2 i 3. Uprawnienia publiczne nie są wystarczające.
   d. Schemat blokowy 3, krok 5.
   e. **Schemat blokowy 3, krok 6**. Użytkownik WILSONJ ma uprawnienia *USE, które nie są wystarczające.
   f. Schemat blokowy 3, krok 8. Obiekt do przetestowania = CONTRACTS/PRICES *FILE. Powrót do Schematu blokowego 1 z niewystarczającymi uprawnieniami.
3. Schemat blokowy 1, krok 6.
   a. Schemat blokowy 8A, krok 1. Obiekt do sprawdzenia = CONTRACTS/PRICES *FILE.
   b. Schemat blokowy 8A, krok 2. Program CPPGM01 nie adoptuje uprawnień.
   c. Schemat blokowy 8A, krok 5. Parametr *USEADPAUT dla programu CPPGM01 ma wartość *NO.
   d. Schemat blokowy 8A, kroki 8 i 9.
      1) Schemat blokowy 8B, krok 1. Program CPPGM01 nie adoptuje uprawnień.
      2) Schemat blokowy 8B, krok 7. Parametr *USEADPAUT dla programu CPPGM01 ma wartość *NO. Dostęp jest odmawiany.

Analiza: Ten przykład demonstruje, że użytkownik może mieć odmówiony dostęp do obiektu, nawet jeśli uprawnienia jego grupy są wystarczające.

Nadanie użytkownikowi uprawnień takich samych, jak uprawnienia publiczne, ale mniejszych niż uprawnienia grupy tego użytkownika nie wpływa na wydajność procesu sprawdzania uprawnień dla innych użytkowników. Jednak jeśli użytkownik WILSONJ ma uprawnienia *EXCLUDE (mniejsze niż prywatne), utracone zostaną korzyści związane z wydajnością przedstawione w Przypadku 4.

Chociaż w tym przykładzie jest dużo kroków, uprawnienia prywatne przeszukiwane są tylko raz. Powinno to zapewnić zadowalającą wydajność.

Przypadek 7: Uprawnienia publiczne bez uprawnień prywatnych

Informacje o uprawnieniach dla zbioru ITEM wyglądają następująco:

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   ITEM           Właściciel . . . . . :   OWNIC
  Biblioteka . . . :   ITEMLIB      Grupa podstawowa . . :   *NONE
Typ obiektu  . . . :   *FILE        Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji . . . . . :   *NONE

                       Uprawnienia
Użytkownik  Grupa      do obiektu
OWNIC                  *ALL
*PUBLIC                *USE
```

Rysunek 24. Wyświetlenie uprawnień dla obiektu (Display Object Authority)

Użytkownik ROSSM potrzebuje uprawnień *USE do zbioru ITEM. Jest członkiem profilu grupowego DPTSM. Oto kroki procesu sprawdzania uprawnień:

1. Schemat blokowy 1, krok 1.
   a. Schemat blokowy 2, kroki 1, 2 i 3. Uprawnienia właściciela OWNIC są wystarczające.
   b. Schemat blokowy 2, krok 4. Zbiór ITEM nie ma grupy podstawowej.
   c. Schemat blokowy 2, krok 6. Autoryzowanie. Uprawnienia publiczne są wystarczające.

Analiza: Uprawnienia publiczne zapewniają najlepszą wydajność, gdy używane są bez uprawnień prywatnych. W tym przykładzie uprawnienia prywatne nigdy nie są przeszukiwane.

Przypadek 8: Uprawnienia adoptowane bez uprawnień prywatnych

W tym przykładzie wszystkie programy w aplikacji należą do profilu OWNIC. Każdy program aplikacji wymagający uprawnień większych niż *USE adoptuje uprawnienia właściciela. Oto kroki wykonane dla użytkownika WILSONJ, w celu uzyskania uprawnień *CHANGE do zbioru ITEM, z wykorzystaniem programu ICPGM10, który adoptuje uprawnienia:

1. Schemat blokowy 1, krok 1.
   a. Schemat blokowy 2, kroki 1, 2, 3, 4 i 6. Uprawnienia publiczne nie są wystarczające.
2. Schemat blokowy 1, krok 2.
   a. Schemat blokowy 3, kroki 1 i 2. Obiekt do sprawdzenia = ITEMLIB/ITEM *FILE.
   b. Schemat blokowy 3, krok 3.
      1) Schemat blokowy 4, krok 1. WILSONJ nie jest właścicielem zbioru ITEM. Powrót do Schematu blokowego 3 bez odnalezienia uprawnień.
   c. Schemat blokowy 3, krok 4.
      1) Schemat blokowy 5, kroki 1 i 3. Uprawnienia publiczne nie są wystarczające. Powrót do Schematu blokowego 3 bez odnalezienia uprawnień.
   d. Schemat blokowy 3, kroki 5, 7 i 8. Zbiór ITEM nie jest chroniony przez listę autoryzacji. Powrót do Schematu blokowego 1 bez odnalezienia uprawnień.
3. Schemat blokowy 1, kroki 3 i 5. (Użytkownik WILSONJ nie ma profilu grupowego.)
   a. Schemat blokowy 7, kroki 1, 3 i 4. Użytkownicy publiczni mają uprawnienia *USE, które nie są wystarczające.
4. Schemat blokowy 1, krok 6.
   a. Schemat blokowy 8A, krok 1. Obiekt do sprawdzenia = ITEMLIB/ITEM *FILE.
   b. Schemat blokowy 8A, kroki 2, 3 i 4. Profil OWNIC nie ma uprawnień *ALLOBJ.

1) Schemat blokowy 4, kroki 1, 2 i 3. Autoryzowanie. Profil OWNIC ma wystarczające uprawnienia do zbioru ITEM.

Analiza: Ten przykład opisuje korzyści z używania uprawnień adoptowanych bez uprawnień prywatnych, w szczególności jeśli właściciel programów posiada także obiekty aplikacji. Ten przykład nie wymaga przeszukiwania uprawnień prywatnych.

Przykład 9: Używanie listy autoryzacji

Zbiór ARWKR01 z biblioteki CUSTLIB jest chroniony przez listę autoryzacji ARLST1. Rys. 25 i Rys. 26 pokazują uprawnienia:

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   ARWRK01       Właściciel . . . . . :   OWNAR
  Biblioteka . . . . :   CUSTLIB       Grupa podstawowa . . :   *NONE
Typ obiektu  . . . . :   *FILE         Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji . . . . . :   ARLST1

                        Uprawnienia
Użytkownik  Grupa       do obiektu
OWNCP                   *ALL
*PUBLIC                 *USE
```

Rysunek 25. Uprawnienia do zbioru ARWRK01

```
            Wyświetlenie listy autoryzacji
             (Display Authorization List)
Obiekt . . . . . :   ARLST1      Właściciel . . . . . :   OWNAR
  Biblioteka . . . . :   QSYS        Grupa podstawowa . . :   *NONE

           Uprawnienia Zarząd.
Użytkownik  Grupa       Upraw. zarządz.
OWNCP                   *ALL
AMESJ                   *CHANGE
*PUBLIC                 *USE
```

Rysunek 26. Uprawnienia do listy autoryzacji ARLST1

Użytkownik AMESJ, który nie jest członkiem profilu grupowego, wymaga uprawnień *CHANGE do zbioru ARWRK01. Oto kroki procesu sprawdzania uprawnień:

1. Schemat blokowy 1, krok 1.
   a. Schemat blokowy 2, kroki 1 i 2. Zbiór ARWRK01 zabezpieczany jest przez listę autoryzacji.
2. Schemat blokowy 1, krok 2.
   a. Schemat blokowy 3, kroki 1 i 2. Obiekt do sprawdzenia = CUSTLIB/ARWRK01 *FILE.
   b. Schemat blokowy 3, krok 3.
      1) Schemat blokowy 4, krok 1. Użytkownik AMESJ nie jest właścicielem zbioru ARWRK01. Powrót do Schematu blokowego 2 bez odnalezienia uprawnień.
   c. Schemat blokowy 3, krok 4.
      1) Schemat blokowy 5, kroki 1 i 3. Uprawnienia publiczne nie są wystarczające. Powrót do Schematu blokowego 3 bez odnalezienia uprawnień.

d. Schemat blokowy 3, kroki 5, 7 i 9. Obiekt do sprawdzenia = ARLST1 *AUTL.
e. Schemat blokowy 3, krok 3.
   1) Schemat blokowy 4, krok 1. Użytkownik AMESJ nie jest właścicielem listy autoryzacji ARLST1. Powrót do Schematu blokowego 3 bez odnalezienia uprawnień.
f. Schemat blokowy 3, kroki 4 i 5.
g. **Schemat blokowy 3, krok 6**. Autoryzowanie. Użytkownik AMESJ ma uprawnienia *CHANGE do listy autoryzacji ARLST1.

Analiza: Ten przykład demonstruje, że listy autoryzacji mogą ułatwiać zarządzanie uprawnieniami i zapewniać dobrą wydajność. Jest tak zwłaszcza wtedy, gdy obiekty zabezpieczane przez listę autoryzacji nie mają uprawnień prywatnych.

Gdyby użytkownik AMESJ był członkiem profilu grupowego, spowodowałoby to dodanie do tego przykładu dodatkowych kroków, ale nie spowodowałoby dodatkowego przeszukiwania uprawnień prywatnych, ponieważ dla zbioru ARWRK01 nie są zdefiniowane żadne uprawnienia prywatne. Problemy z wydajnością mogą wystąpić, gdy używana jest kombinacja uprawnień prywatnych, list autoryzacji i profili grupowych, tak jak w “Przypadek 11: Łączenie metod autoryzowania” na stronie 174.

Przypadek 10: Używanie wielu grup

Użytkownik WOODBC potrzebuje uprawnień *CHANGE do zbioru CRLIM. Jest członkiem trzech grup: DPTAR, DPTSM i DPTMG. DPTAR jest jego podstawowym profilem grupowym (parametr GRPPRF). Grupy DPTSM i DPTMG są dodatkowymi profilami grupowymi (parametr SUPGRPPRF). Rys. 27 pokazuje uprawnienia do zbioru CRLIM:

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   CRLIM          Właściciel . . . . . :   OWNAR
  Biblioteka . . . :   CUSTLIB       Grupa podstawowa . . :   DPTAR
Typ obiektu  . . . :   *FILE          Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji . . . . . :   *NONE

                       Uprawnienia
Użytkownik  Grupa      do obiektu
OWNAR                  *ALL
DPTAR                  *CHANGE
DPTSM                  *USE
*PUBLIC                *EXCLUDE
```

Rysunek 27. Uprawnienia do zbioru CRLIM

Oto kroki procesu sprawdzania uprawnień:

1. Schemat blokowy 1, krok 1.
   a. Schemat blokowy 2, krok 1. Powrót do wywołującego schematu blokowego z niewystarczającymi uprawnieniami.
2. Schemat blokowy 1, krok 2.
   a. Schemat blokowy 3, kroki 1 i 2. Obiekt do sprawdzenia = CUSTLIB/CRLIM *FILE.
   b. Schemat blokowy 3, krok 3.
      1) Schemat blokowy 4, krok 1. WOODBC nie jest właścicielem zbioru CRLIM. Powrót do Schematu blokowego 3 bez odnalezienia uprawnień.
   c. Schemat blokowy 3, krok 4.
      1) Schemat blokowy 5, kroki 1, 2 i 3. Uprawnienia publiczne nie są wystarczające.

d. Schemat blokowy 3, krok 5.

e. **Schemat blokowy 3, krok 6**. Użytkownik WOODBC nie ma żadnych uprawnień do zbioru CRLIM.

f. Schemat blokowy 3, kroki 7 i 8. Zbiór CRLIM nie jest zabezpieczony listą autoryzacji. Powrót do Schematu blokowego 1 bez odnalezienia uprawnień.

3. Schemat blokowy 1, kroki 3 i 4. Pierwszą grupą użytkownika WOODBC jest profil DPTAR.

   a. Schemat blokowy 6, kroki 1 i 2. Obiekt do sprawdzenia = CUSTLIB/CRLIM *FILE.

   b. Schemat blokowy 6, krok 3.

      1) Schemat blokowy 4, krok 1. Profil DPTAR nie jest właścicielem zbioru CRLIM. Powrót do Schemat blokowy 6 bez odnalezienia uprawnień.

   c. Schemat blokowy 6, kroki 4 i 5. Autoryzowanie. Profil DPTAR jest grupą podstawową i ma wystarczające uprawnienia.

Przypadek 11: Łączenie metod autoryzowania

Użytkownik WAGNERB potrzebuje uprawnień *ALL do zbioru CRLIMWRK. Jest członkiem następujących grup: DPTSM, DPT702 i DPTAR. Jego pierwszą grupą (parametr GRPPRF) jest grupa DPTSM. Rys. 28 pokazuje uprawnienia do zbioru CRLIMWRK.

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   CRLIMWRK        Właściciel . . . . . :   OWNAR
  Biblioteka . . . :   CUSTLIB        Grupa podstawowa . . :   *NONE
Typ obiektu  . . . :   *FILE          Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji . . . . . :   CRLST1

                       Uprawnienia
Użytkownik  Grupa      do obiektu
OWNAR                  *ALL
DPTSM                  *USE
WILSONJ                *EXCLUDE
*PUBLIC                *USE
```

Rysunek 28. Uprawnienia do zbioru CRLIMWRK

Zbiór CRLIMWRK jest chroniony przez listę autoryzacji CRLST1. Rys. 29 pokazuje uprawnienia do listy autoryzacji CRLST1.

```
            Wyświetlenie listy autoryzacji
             (Display Authorization List)
Obiekt . . . . . :   CRLST1        Właściciel . . . . . :   OWNAR
  Biblioteka . . . :     QSYS        Grupa podstawowa . . :   DPTAR

           Uprawnienia Zarząd.
Użytkownik  Grupa      Upraw. zarządz.
OWNAR                  *ALL        X
DPTAR                  *ALL
*PUBLIC                *EXCLUDE
```

Rysunek 29. Uprawnienia do listy autoryzacji CRLST1

Ten przykład pokazuje wiele możliwości sprawdzania uprawnień. Demonstruje także, jak używanie zbyt wielu opcji uprawnień do obiektu może wpłynąć na złą wydajność.

Poniżej przedstawiono kroki wymagane do sprawdzenia uprawnień użytkownika WAGNERB do zbioru CRLIMWRK:

1. Schemat blokowy 1, krok 1.
   a. Schemat blokowy 2, krok 1.
2. Schemat blokowy 1, krok 2.
   a. Schemat blokowy 3, kroki 1 i 2. Obiekt do sprawdzenia = CUSTLIB/CRLIMWRK *FILE.
   b. Schemat blokowy 3, krok 3.
      1) Schemat blokowy 4, krok 1. WAGNERB nie jest właścicielem zbioru CRLIMWRK. Powrót do Schematu blokowego 3 bez odnalezienia uprawnień.
   c. Schemat blokowy 3, krok 4.
      1) Schemat blokowy 5, kroki 1 i 2. Użytkownik WILSONJ ma uprawnienia *EXCLUDE, które są mniejsze niż uprawnienia publiczne *USE.
   d. Schemat blokowy 3, kroki 5 i 6 (**pierwsze przeszukiwanie uprawnień prywatnych**). Użytkownik WAGNERB nie ma uprawnień prywatnych.
   e. Schemat blokowy 3, kroki 7 i 9. Obiekt do sprawdzenia = CRLST1 *AUTL.
   f. Schemat blokowy 3, krok 3.
      1) Schemat blokowy 4, krok 1. WILSONJ nie jest właścicielem listy CRLST1. Powrót do Schematu blokowego 3 bez odnalezienia uprawnień.
   g. Schemat blokowy 3, kroki 4 i 5.
   h. Schemat blokowy 3, krok 6 (**drugie przeszukiwanie uprawnień prywatnych**). Użytkownik WAGNERB nie ma uprawnień prywatnych do listy CRLST1.
   i. Schemat blokowy 3, kroki 7 i 8. Obiekt do sprawdzenia = CUSTLIB/CRLIMWRK *FILE.
3. Schemat blokowy 1, kroki 3 i 4. Pierwszym profilem grupowym użytkownika WAGNERB jest profil DPTSM.
   a. Schemat blokowy 6, kroki 1 i 2. Obiekt do sprawdzenia = CUSTLIB/CRLIMWRK *FILE.
   b. Schemat blokowy 6, krok 3.
      1) Schemat blokowy 4, krok 1. Profil DPTSM nie jest właścicielem zbioru CRLIMWRK. Powrót do Schemat blokowy 6 bez odnalezienia uprawnień.
   c. Schemat blokowy 6, krok 4. DPTSM nie jest grupą podstawową dla zbioru CRLIMWRK.
   d. Schemat blokowy 6, krok 6 (**trzecie przeszukiwanie uprawnień prywatnych**). Profil DPTSM ma uprawnienia *USE do zbioru CRLIMWRK, które nie są wystarczające.
   e. Schemat blokowy 6, kontynuowany jest krok 6. Do już odnalezionych uprawnień dla grup użytkownika WAGNERB dodawane są uprawnienia *USE (brak). Wystarczające uprawnienia nie zostały jeszcze odnalezione.
   f. Schemat blokowy 6, kroki 9 i 10. Następną grupą użytkownika WAGNERB jest profil DPT702.
   g. Schemat blokowy 6, kroki 1 i 2. Obiekt do sprawdzenia = CUSTLIB/CRLIMWRK *FILE.
   h. Schemat blokowy 6, krok 3.
      1) Schemat blokowy 4, krok 1. Profil DPT702 nie jest właścicielem zbioru CRLIMWRK. Powrót do Schemat blokowy 6 bez odnalezienia uprawnień.
   i. Schemat blokowy 6, krok 4. DPT702 nie jest grupą podstawową dla zbioru CRLIMWRK.
   j. Schemat blokowy 6, krok 6 (**czwarte przeszukiwanie uprawnień prywatnych**). Profil DPT702 nie ma uprawnień do zbioru CRLIMWRK.
   k. Schemat blokowy 6, kroki 7 i 8. Obiekt do sprawdzenia = CRLST1 *AUTL.
   l. Schemat blokowy 6, krok 3.
      1) Schemat blokowy 5, krok 1. Profil DPT702 nie jest właścicielem listy autoryzacji CRLST1. Powrót do Schematu blokowego 6 bez odnalezienia uprawnień.
   m. Schemat blokowy 6, kroki 4 i 6 (**piąte przeszukiwanie uprawnień prywatnych**). Profil DPT702 nie ma uprawnień do listy autoryzacji CRLST1.
   n. Schemat blokowy 6, kroki 7, 9 i 10. Profil DPTAR jest następnym profilem grupowym użytkownika WAGNERB.

o. Schemat blokowy 6, kroki 1 i 2. Obiekt do sprawdzenia = CUSTLIB/CRLIMWRK *FILE.
p. Schemat blokowy 6, krok 3.
   1) Schemat blokowy 4, krok 1. Profil DPTAR nie jest właścicielem zbioru CRLIMWRK. Powrót do Schemat blokowy 6 bez odnalezienia uprawnień.
q. Schemat blokowy 6, kroki 4 i 6 (**szóste przeszukiwanie uprawnień prywatnych**). Profil DPTAR nie ma uprawnień do zbioru CRLIMWRK.
r. Schemat blokowy 6, kroki 7 i 8. Obiekt do sprawdzenia = CRLST1 *AUTL.
s. Schemat blokowy 6, krok 3.
   1) Schemat blokowy 4, krok 1. Profil DPTAR nie jest właścicielem listy autoryzacji CRLST1. Powrót do Schematu blokowego 6 bez odnalezienia uprawnień.
t. Schemat blokowy 6, kroki 4 i 5. Autoryzowanie. Profil DPTAR jest grupą podstawową dla listy autoryzacji CRLST1 i ma uprawnienia *ALL.

Rezultat: Użytkownik WAGNERB ma uprawnienia do wykonania żądanej operacji za pomocą uprawnień grupy podstawowej DPTAR do listy autoryzacji CRLIST1.

Analiza: Ten przykład demonstruje projekt uprawnień niepoprawny zarówno z punktu widzenia zarządzania jak i wydajności. Użyto zbyt wielu opcji, co powoduje duże trudności w zrozumieniu, zmianach i kontrolowaniu. Uprawnienia prywatne przeszukiwane są 6 razy, co może powodować zauważalne problemy związane z wydajnością:

Profil	Obiekt	Typ	Wynik
WAGNERB	CRLIMWRK	*FILE	Nie odnaleziono uprawnień
WAGNERB	CRLST1	*AUTL	Nie odnaleziono uprawnień
DPTSM	CRLIMWRK	*FILE	Uprawnienia *USE (niewystarczające)
DPT702	CRLIMWRK	*FILE	Nie odnaleziono uprawnień
DPT702	CRLST1	*AUTL	Nie odnaleziono uprawnień
DPTAR	CRLIMWRK	*FILE	Nie odnaleziono uprawnień

Zmiana kolejności profili grupowych użytkownika WAGNERB mogłaby spowodować zmianę parametrów wydajności. Przyjmijmy, że profil DPTAR jest pierwszym profilem grupowym użytkownika WAGNERB (parametr GRPPRF). System przeszuka wtedy uprawnienia prywatne 3 razy, zanim znajdzie uprawnienia grupy podstawowej DPTAR do listy autoryzacji CRLST1.

- uprawnienia użytkownika WAGNERB do zbioru CRLIMWRK,
- uprawnienia użytkownika WAGNERB do listy autoryzacji CRLST1,
- uprawnienia profilu DPTAR do zbioru CRLIMWRK.

Dla dobrej wydajności systemu istotne jest ostrożne planowanie profili grupowych oraz list autoryzacji.

Pamięć podręczna uprawnień

W wersji 3, wydaniu 7, dla użytkownika uzyskującego dostęp do obiektu po raz pierwszy, system tworzy pamięć podręczną uprawnień. Za każdym razem, gdy uzyskiwany jest dostęp do obiektu, system sprawdza uprawnienia w pamięci podręcznej użytkownika, zanim sprawdzi jego profil. Wynikiem tego jest szybsze sprawdzenie uprawnień prywatnych.

Pamięć podręczna uprawnień zawiera do 32 uprawnień prywatnych do obiektów i do 32 uprawnień prywatnych do list autoryzacji. Pamięć ta jest aktualizowana, gdy użytkownik ma nadawane lub odbierane uprawnienia. Wszystkie pamięci podręczne użytkownika są czyszczone podczas przeprowadzania IPL.

Zalecane jest ograniczone użycie uprawnień prywatnych, natomiast pamięć podręczna oferuje elastyczność. Można na przykład wybrać dowolny sposób ochrony obiektów, ponieważ jego wpływ na wydajność będzie znikomy. Jest to szczególnie ważne, jeśli użytkownicy często odwołują się do tych samych obiektów.

Rozdział 6. Ochrona zarządzania pracą

Ten rozdział omawia zagadnienia związane z zarządzaniem pracą w systemie:

- Inicjalizacja zadania
- Stacje robocze
- Opisy podsystemów
- Opisy zadań
- Listy bibliotek
- Drukowanie
- Atrybuty sieciowe
- Strojenie wydajności

Pełne informacje dotyczące tematów związanych z zarządzaniem pracą zawiera książka *Zarządzanie pracą w systemie AS/400*.

Inicjalizacja zadania

Gdy w systemie uruchamiane jest zadanie, przypisywane są do niego obiekty, takie jak kolejka wyjściowa, opis zadania oraz biblioteki z listy bibliotek. Przed zezwoleniem na uruchomienie zadania, a także po jego uruchomieniu w przypadku innych obiektów, sprawdzane są uprawnienia do niektórych z wyżej wymienionych obiektów. Niewystarczające uprawnienia mogą powodować błędy lub zakończyć zadanie.

Obiekty, które są częścią struktury zadania, mogą być podane w opisie zadania, profilu użytkownika oraz komendzie Wprowadzenie zadania (Submit Job - SBMJOB) w przypadku zadania wsadowego.

Uruchamianie zadania interaktywnego

Poniżej przedstawiono opis działania ochrony podczas uruchamiania zadania interaktywnego. Jest to jedynie przykład, ponieważ podczas podawania obiektów dla zadania istnieje wiele możliwości.

Jeśli podczas procesu wpisywania się wystąpi błąd uprawnień, u dołu ekranu Wpisanie Się (Sign On) pojawia się komunikat opisujący błąd. Niektóre błędy uprawnień mogą powodować także powstanie zapisu w protokole zadania. Jeśli użytkownik nie może wpisać się z powodu błędu uprawnień, należy zmienić profil użytkownika w celu podania innego obiektu lub nadać użytkownikowi uprawnienia do obiektu.

Po podaniu przez użytkownika identyfikatora i hasła, przed uruchomieniem zadania w systemie wykonywane są poniższe czynności:

1. Sprawdzany jest profil użytkownika i jego hasło. Status profilu musi mieć wartość *ENABLED. Profil użytkownika podany na ekranie wpisania się musi mieć uprawnienia *OBJOPR i *CHANGE do samego siebie.
2. Sprawdzane są uprawnienia użytkownika do stacji roboczej. Więcej informacji na ten temat zawiera sekcja “Stacje robocze” na stronie 181.
3. System sprawdza uprawnienia dla wartości w profilu użytkownika oraz w opisie zadania użytkownika, które używane są do utworzenia struktury zadania, takiej jak:
   - Opis zadania
   - Kolejka wyjściowa
   - Biblioteka bieżąca
   - Biblioteki na liście bibliotek

   Jeśli któryś z tych obiektów nie istnieje lub użytkownik nie ma odpowiednich uprawnień, u dołu ekranu Wpisanie Się (Sign On) wyświetlany jest komunikat i użytkownik nie może się wpisać. Jeśli uprawnienia do tych obiektów zostaną zweryfikowane pomyślnie, zadanie jest uruchamiane.

Uwaga: Uprawnienia do drukarki i kolejki zadań nie są sprawdzane do momentu aż użytkownik spróbuje ich użyć.

Po uruchomieniu zadania, zanim użytkownik zobaczy pierwszy ekran lub menu, wykonywane są następujące czynności:

1. Jeśli pozycja routingu dla zadania określa program użytkownika, dla tego programu, jego biblioteki i wszystkich obiektów używanych przez ten program, przeprowadzane jest zwykłe sprawdzanie uprawnień. Jeśli uprawnienia nie są wystarczające, do użytkownika wysyłany jest komunikat, a zadanie zostaje zakończone.
2. Jeśli pozycja routingu określa procesor komend (QCMD):
   a. Sprawdzanie uprawnień przeprowadzane jest dla programu procesora QCMD, biblioteki programu oraz wszystkich używanych obiektów, tak jak opisano to w kroku 1.
   b. Sprawdzane są uprawnienia użytkownika do programu obsługi klawisza ATTN. Jeśli uprawnienia są niewystarczające, do użytkownika wysyłany jest komunikat oraz zapisywana jest pozycja w protokole zadania. Przetwarzanie jest kontynuowane.

      Jeśli uprawnienia są wystarczające, program obsługi klawisza ATTN jest aktywowany. Program jest uruchamiany dopiero wtedy, gdy użytkownik po raz pierwszy naciśnie klawisz ATTN. W tym momencie dla obiektów używanych przez program przeprowadzane jest zwykłe sprawdzanie uprawnień.
   c. Dla programu początkowego (i jego obiektów) podanego w profilu użytkownika przeprowadzane jest zwykłe sprawdzanie uprawnień. Jeśli uprawnienia są wystarczające, program jest uruchamiany. Jeśli uprawnienia są niewystarczające, do użytkownika wysyłany jest komunikat oraz zapisywana jest pozycja w protokole zadania. Zadanie zostaje zakończone.
   d. Dla menu początkowego (i jego obiektów) podanego w profilu użytkownika przeprowadzane jest zwykłe sprawdzanie uprawnień. Jeśli uprawnienia są wystarczające, menu jest wyświetlane. Jeśli uprawnienia są niewystarczające, do użytkownika wysyłany jest komunikat oraz zapisywana pozycja w protokole zadania. Zadanie zostaje zakończone.

Uruchamianie zadania wsadowego

Poniżej przedstawiono opis działania ochrony podczas uruchamiania zadania wsadowego. Ponieważ do wprowadzania zadań wsadowych oraz podawania obiektów używanych przez takie zadanie istnieje kilka metod, są to jedynie wskazówki. Ten przykład korzysta z wprowadzonego za pomocą komendy Wprowadzenie zadania (Submit job - SBMJOB) zadania z zadania interaktywnego.

Gdy użytkownik podaje komendę SBMJOB, przed dodaniem zadania do kolejki zadań wykonywane jest następujące sprawdzanie:

1. Jeśli w komendzie SBMJOB podano profil użytkownika, użytkownik musi mieć uprawnienia *USE do tego profilu.
2. Sprawdzane są uprawnienia dla obiektów podanych jako parametry komendy SBMJOB oraz w opisie zadania. Sprawdzane są uprawnienia dla profilu użytkownika, który uruchamia zadanie.
3. Jeśli określony jest poziom ochrony 40, a dla komendy SBMJOB podano parametr USER(*JOBD), użytkownik wprowadzający zadanie musi mieć uprawnienia *USE do profilu użytkownika z opisu zadania.
4. Jeśli obiekt nie istnieje lub uprawnienia nie są wystarczające, do użytkownika wysyłany jest komunikat, a zadanie nie jest wprowadzane.

Gdy system wybiera zadanie z kolejki zadań i próbuje je uruchomić, kolejność sprawdzania uprawnień jest podobna do kolejności dla uruchamiania zadania interaktywnego.

Uprawnienia adoptowane a zadania wsadowe

Gdy uruchamiane jest nowe zadanie, tworzony jest dla niego nowy stos programów. Uprawnienia adoptowane nie zadziałają, dopóki na stos nie zostanie dodany pierwszy program. Uprawnienia adoptowane nie mogą być użyte w celu uzyskania dostępu do dowolnych obiektów, takich jak kolejka wyjściowa lub opis zadania, które dodawane są do

struktury zadania przed jego routingiem. Dlatego, nawet jeśli podczas wprowadzania zadanie interaktywne działa pod kontrolą uprawnień adoptowanych, te uprawnienia nie są używane do sprawdzania uprawnień dla obiektów w żądaniu SBMJOB.

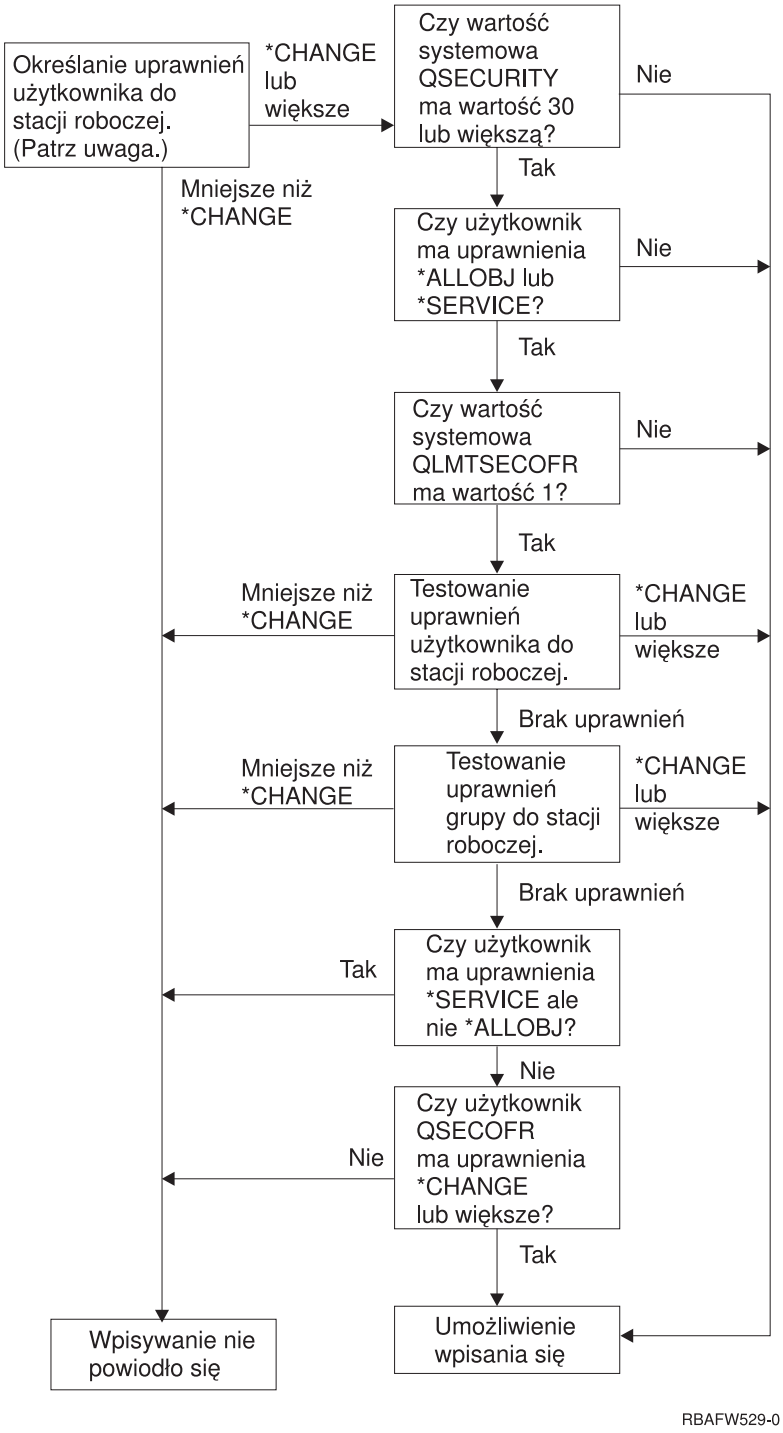
Za pomocą komendy Zmiana zadania (Change Job - CHGJOB) można zmienić parametry zadania wsadowego. Uprawnienia wymagane do zmiany parametrów zadania opisano w sekcji 366.

Stacje robocze

Opis urządzenia zawiera informacje dotyczące danego urządzenia lub jednostki logicznej, która jest podłączona do systemu. Gdy użytkownik wpisuje się do systemu, jego stacja podłączana jest do fizycznego lub wirtualnego opisu urządzenia. Aby wpisać się pomyślnie, użytkownik musi mieć uprawnienia *CHANGE do opisu urządzenia.

Wartość systemowa QLMTSECOFR (ograniczenie dostępu dla szefa ochrony) określa, czy użytkownicy z uprawnieniami specjalnymi *ALLOBJ lub *SERVICE muszą być autoryzowani do opisów urządzeń.

Rys. 30 na stronie 182 pokazuje logikę określania, czy użytkownik może wpisać się do urządzenia:



Rysunek 30. Sprawdzanie uprawnień do stacji roboczych

Uwaga: W celu określenia, czy użytkownik ma co najmniej uprawnienia *CHANGE do opisu urządzenia, przeprowadzane jest zwykłe sprawdzanie uprawnień. Uprawnienia *CHANGE mogą być odnalezione za pomocą:

- uprawnień specjalnych *ALLOBJ z profilu użytkownika, profilu grupowego lub dodatkowych profili grupowych,
- uprawnień prywatnych do opisu urządzenia w profilu użytkownika, profilu grupowym lub dodatkowych profilach grupowych,
- uprawnień do listy autoryzacji używanej do zabezpieczania opisu urządzenia,

- uprawnień do listy autoryzacji używanej do zabezpieczania uprawnień publicznych.

Sprawdzanie uprawnień do opisu urządzenia przeprowadzane jest przed umieszczeniem programów na stosie programów dla zadania i dlatego nie są używane uprawnienia adoptowane.

Opis sprawdzania uprawnień do stacji roboczych

System określa uprawnienia użytkownika do stacji roboczej. (Patrz uwaga 1) Jeśli uprawnienia są mniejsze niż *CHANGE, wpisywanie nie powiedzie się. Jeśli użytkownik ma uprawnienia *CHANGE lub większe, system sprawdza, czy poziom ochrony systemu jest na poziomie 30 lub wyższym. Jeśli nie jest, użytkownik może wpisać się.

Jeśli poziom ochrony ma wartość 30 lub wyższą, system sprawdza, czy użytkownik ma uprawnienia specjalne *ALLOBJ lub *SERVICE. Jeśli nie ma tych uprawnień, może się wpisać.

Jeśli użytkownik ma uprawnienia specjalne *ALLOBJ lub *SERVICE, system sprawdza, czy wartość systemowa QLMTSECOFR ustawiona jest na 1. Jeśli nie jest ustawiona, użytkownik może się wpisać.

Jeśli wartość systemowa QLMTSECOFR ustawiona jest na 1, system sprawdzi uprawnienia użytkownika do stacji roboczej. Jeśli użytkownik ma uprawnienia *CHANGE lub wyższe, może się wpisać. Jeśli uprawnienia użytkownika są niższe niż *CHANGE, wpisywanie się nie powiedzie. Jeśli użytkownik nie ma uprawnień do stacji roboczej, system sprawdza uprawnienia grupowe użytkownika do danej stacji roboczej.

Jeśli uprawnienia grupowe użytkownika to *CHANGE lub wyższe, może się wpisać. Jeśli uprawnienia grupowe użytkownika są niższe niż *CHANGE, wpisywanie się nie powiedzie. Jeśli użytkownik nie ma uprawnień do stacji roboczej, system sprawdza, czy użytkownik ma uprawnienie *SERVICE i nie ma uprawnienia specjalnego *ALLOBJ.

Jeśli użytkownik ma uprawnienia *SERVICE i nie ma uprawnień *ALLOBJ, wpisywanie się nie powiedzie. Jeśli użytkownik ma uprawnienia *SERVICE i nie ma uprawnień specjalnych *ALLOBJ, system sprawdza, czy użytkownik QSECOFR ma uprawnienia *CHANGE lub wyższe.

Jeśli użytkownik QSECOFR nie ma uprawnień *CHANGE lub wyższych, wtedy wpisywanie się nie powiedzie. Jeśli użytkownik QSECOFR ma uprawnienia *CHANGE lub wyższe, wtedy może się wpisać.

Profile użytkowników szefa ochrony (QSECOFR), serwisu (QSRV) i serwisu podstawowego (QSRVBAS) zawsze mają zezwolenie na wpisywanie się na konsoli. Wartość systemowa QCONSOLE (konsola) używana jest do określania, które urządzenie jest konsolą. Jeśli na konsoli próbuje się wpisać użytkownik o profilu QSRV lub QSRVBAS, który nie ma uprawnień *CHANGE, system nadaje mu uprawnienia *CHANGE i zezwala na wpisanie się.

Prawo własności do opisów urządzeń

Domyślne uprawnienia publiczne do komend CRTDEVxxx to uprawnienia *LIBCRTAUT. Urządzenia tworzone są w bibliotece QSYS, dla której wartość domyślna parametru CRTAUT jest równa *SYSVAL. Wartością domyślną wartości systemowej QCRTAUT jest *CHANGE.

Aby ograniczyć użytkowników, którzy mogą wpisywać się do stacji roboczej, należy ustawić uprawnienia publiczne do takiej stacji na *EXCLUDE, a określonym użytkownikom lub grupom nadać uprawnienia *CHANGE.

Szef ochrony (QSECOFR) nie ma nadanych uprawnień do urządzeń. Jeśli wartość systemowa QLMTSECOFR ustawiona jest na 1 (tak), szefowi ochrony należy nadawać uprawnienia *CHANGE do urządzeń. Uprawnienia *CHANGE może nadać dowolny użytkownik z uprawnieniami *OBJMGT i *CHANGE do urządzenia.

Jeśli opis urządzenia tworzony jest przez szefa ochrony, to jest on właścicielem urządzenia i ma do niego uprawnienia *ALL. Gdy urządzenia konfigurowane są automatycznie przez system, większość urządzeń należy do profilu QPGMR. Urządzenia tworzone przez program QLUS (urządzenia typu *APPC) należą do profilu QSYS.

Jeśli do ograniczanie wpisywania się szefa ochrony planuje się użyć wartość systemową QLMTSECOFR, tworzone urządzenia powinny być w posiadaniu profilu innego niż QSECOFR.

Aby zmienić prawo własności opisu urządzenia graficznego, urządzenie musi być włączone i udostępnione. Należy się wpisać do takiego urządzenia i za pomocą komendy CHGOBJOWN zmienić prawo własności. Jeśli użytkownik nie jest wpisany do urządzenia, przed zmianą prawa własności, za pomocą komendy Przydzielenie obiektu (Allocate Object - ALCOBJ) należy przydzielić to urządzenie. Urządzenie można przydzielić, jeśli nikt go nie używa. Po zmianie prawa własności należy zwolnić urządzenie, korzystając z komendy Zwolnienie obiektu (Deallocate Object - DLCOBJ).

Zbiór ekranowy ekranu wpisania się

Administrator systemu może zmienić systemowy ekran wpisywania się, dodając do niego tekst lub logo przedsiębiorstwa. Podczas dodawania tekstu do zbioru ekranowego należy uważać, aby nie zmienić nazw pól lub długości buforów tego zbioru. Zmiana nazw pól lub długości buforów może spowodować niepowodzenie podczas wpisywania się.

Zmienianie ekranu wpisania się

Z systemem operacyjnym dostarczany jest kod źródłowy dla zbioru ekranowego ekranu wpisywania się. Kod źródłowy znajduje się z zbiorze QSYS/QAWTSSRC. Kod można zmienić w celu dodania tekstu do ekranu wpisywania się. Nie należy zmieniać nazw pól oraz długości buforów.

Wyświetlanie kodu źródłowego zbioru dla ekranu wpisania się

Kod źródłowy dla zbioru ekranu wpisywania się dostarczany jest jako podzbiór (QDSIGNON lub QDSIGNON2) zbioru fizycznego QSYS/QAWTSSRC. Podzbiór QDSIGNON zawiera kod źródłowy dla ekranu wpisywania się używanego, gdy wartość systemowa QPWDLVL ustawiona jest na 0 lub 1. Podzbiór QDSIGNON2 zawiera kod ekranu wpisywania się używanego, gdy wartość systemowa QPWDLVL ustawiona jest na 2 lub 3.

Zbiór QSYS/QAWTSSRC jest **usuwany i odtwarzany** za każdym razem, gdy instalowany jest system operacyjny OS/400. Jeśli planuje się utworzenie własnej wersji ekranu wpisywania się, najpierw do własnego zbioru z kodem należy skopiować odpowiedni podzbiór z kodem źródłowym, QDSIGNON lub QDSIGNON2, a następnie wprowadzić w nim zmiany.

Zmienianie zbioru ekranu wpisywania się

Aby zmienić format ekranu wpisywania się:

1. Utwórz zmieniony zbiór ekranu wpisywania się.

   Aby zarządzać mniejszymi polami, można zmienić w zbiorze ekranowym ukryte pole UBUFFER. Pole UBUFFER ma długość 128 bajtów i jest ostatnim polem zbioru ekranowego. Pole to można zmienić, aby funkcjonowało jako bufor wejściowy/wyjściowy, tak że dane podane w tym polu ekranu będą dostępne dla programów podczas uruchamiania zadania interaktywnego. Pole UBUFFER można zmienić, tak aby zawierało tyle potrzebnych mniejszych pól, ile wymaga użytkownik, jeśli spełnione zostaną następujące wymagania:

   - nowe pola muszą znajdować się za pozostałymi polami zbioru ekranowego; umiejscowienie pól na ekranie nie ma znaczenia dopóki porządek, w jakim są wstawiane w specyfikacji opisu danych (data description specifications - DDS) spełnia te wymagania,
   - długość nie może przekraczać 128 bajtów; jeśli długość pól jest większa niż 128, niektóre dane nie zostaną przekazane,
   - wszystkie pola muszą być polami typu wejście/wyjście (typ B w kodzie DDS) lub polami ukrytymi (typ H w kodzie DDS).

2. Porządek deklarowania pól w zbiorze ekranowym nie może być zmieniony. Miejsce ich pojawiania się na ekranie może zostać zmienione. Nie należy zmieniać w kodzie źródłowym istniejących nazw pól dla zbioru ekranowego ekranu wpisywania się.
3. Nie należy zmieniać całkowitej wielkości buforów wyjściowych. Jeśli zostanie zmieniony porządek lub wielkość tych buforów, mogą powstać poważne problemy.
4. W zbiorze ekranu wpisywania się nie należy używać funkcji pomocy specyfikacji opisu danych.

5. Należy zmienić opis podsystemu, tak aby używał zmienionego zbioru ekranowego zamiast domyślnego zbioru QSYS/QDSIGNON. Opisy podsystemów można zmienić dla tych podsystemów, dla których ma być używany nowy ekran. Aby zmienić opis podsystemu:
   a. Użyj komendy Zmiana opisu podsystemu (Change Subsystem Description - CHGSBSD).
   b. W parametrze SGNDSPF podaj nowy zbiór ekranowy.
   c. Przed przystąpieniem do zmiany podsystemu sterującego użyj testowej wersji podsystemu, aby sprawdzić, czy ekran jest poprawny.
6. Przetestuj zmianę.
7. Zmień inne opisy podsystemów.

Uwagi:

1. Długość bufora dla zbioru ekranowego musi mieć 318 bajtów. Jeśli jest mniejsza niż 318, podsystem użyje domyślnego ekranu wpisywania się (podzbiór QDSIGNON z biblioteki QSYS, gdy wartość systemowa QPWDLVL ustawiona jest na 0 lub 1 i podzbiór QDSIGNON2 z biblioteki QSYS gdy wartość QPWDLVL ustawiona jest na 2 lub 3).
2. Linia praw autorskich nie może być usunięta.

Opisy podsystemów

Opisy podsystemów kontrolują:

W jaki sposób do systemu wprowadzane są zadania

Jak zadania są uruchamiane

Parametry wydajności zadań

Do zmiany opisów podsystemów powinni być uprawnieni tylko niektórzy użytkownicy, a zmiany powinny być uważnie monitorowane.

Kontrolowanie, w jaki sposób do systemu wprowadzane są zadania

Z systemem dostarczanych jest kilka opisów podsystemów. Po zmianie poziomu ochrony (wartość systemowa QSECURITY) na poziom 20 lub wyższy, wpisywanie się do podsystemów dostarczanych przez IBM, bez podania identyfikatora użytkownika i hasła nie jest możliwe.

Jest możliwe zdefiniowanie opisu podsystemu oraz opisu zadania tak, aby umożliwić domyślne wpisywanie się (bez identyfikatora użytkownika i hasła), jednak powoduje to ryzyko naruszenia ochrony. Gdy system przekierowuje zadanie interaktywne, sprawdza w opisie podsystemu pozycję stacji roboczej dla opisu zadania. Jeśli w opisie zadania jest wartość USER(*RQD), użytkownik musi podać na ekranie Wpisanie się (Sign On) poprawny identyfikator użytkownika (i hasło). Jeśli w opisie zadania, w polu *Użytkownik* podany jest profil użytkownika, każdy może wpisać się jako ten użytkownik, naciskając klawisz Enter.

Na poziomie ochrony 30 i wyższym, jeśli następuje próba domyślnego wpisania się, system protokołuje w kronice kontroli pozycję (typ AF, podtyp S) (gdy aktywna jest funkcja kontroli). Na poziomie ochrony 40 i wyższym, system nie zezwala na domyślne wpisywanie się, nawet jeśli pozycja stacji roboczej i opisu zadania umożliwia to. Więcej informacji na ten temat zawiera sekcja “Wpisywanie się bez identyfikatora użytkownika i hasła” na stronie 14.

Należy się upewnić, że wszystkie pozycje stacji roboczych dla podsystemów interaktywnych odnoszą się do opisów zadań z parametrem USER(*RQD). Należy także kontrolować uprawnienia do zmiany opisów zadań oraz monitorować wszystkie zmiany dokonywane w tych opisach. Jeśli funkcja kontroli jest aktywna, system zapisuje w kronice kontroli pozycję JD za każdym razem, gdy w opisie zadania zmieniany jest parametr USER.

Pozycje komunikacji w opisie podsystemu kontrolują, w jaki sposób zadania komunikacji wprowadzane są do systemu. Pozycja komunikacji wskazuje na domyślny profil użytkownika, który umożliwia uruchomienie zadania bez identyfikatora użytkownika i hasła. Powoduje to powstanie potencjalnego ryzyka naruszenia ochrony. Należy

przeanalizować pozycje komunikacji w danym systemie i użyć atrybutów sieciowych w celu kontrolowania sposobu wprowadzania zadań komunikacyjnych do systemu. Sekcja “Atrybuty sieciowe” na stronie 193 omawia atrybuty sieciowe, które są ważne dla ochrony.

Opisy zadań

Opis zadania to wartościowe narzędzie ochrony oraz zarządzania pracą. Opis zadania można skonfigurować dla grupy użytkowników, która potrzebuje takiej samej początkowej listy bibliotek, kolejki wyjściowej i kolejki zadań. Opis zadania można skonfigurować także dla grupy zadań wsadowych, które mają podobne wymagania.

Opis zadania stanowi także potencjalne ryzyko naruszenia ochrony. W niektórych przypadkach opis zadania, w którym dla parametru USER podano profil użytkownika, umożliwia wprowadzanie zadań do systemu bez odpowiedniego sprawdzania ochrony. W sekcji “Kontrolowanie, w jaki sposób do systemu wprowadzane są zadania” na stronie 185 znajduje się omówienie sposobów zapobiegania temu dla zadań interaktywnych i komunikacyjnych.

Gdy wprowadzane jest zadanie wsadowe, zadanie może działać pod kontrolą profilu innego niż użytkownika, który je wprowadził. Profil można podać w komendzie SBMJOB lub parametrze USER opisu zadania. Jeśli system jest na poziomie ochrony (wartość systemowa QSECURITY) 30 lub niższym, użytkownik wprowadzający zadanie musi mieć uprawnienia do opisu zadania, ale nie potrzebuje uprawnień do profilu użytkownika podanego w opisie. Stanowi to ryzyko naruszenia ochrony. Na poziomie ochrony 40 i wyższym, użytkownik wprowadzający musi mieć uprawnienia zarówno do opisu zadania, jak i do profilu użytkownika.

Na przykład:

- UŻYTKOWNIK_A nie jest autoryzowany do zbioru PAYROLL,
- UŻYTKOWNIK_B ma uprawnienia *USE do zbioru PAYROLL i do programu PRLIST, który wyświetla zbiór PAYROLL,
- opis zadania PRJOBD ma parametr USER(UŻYTKOWNIK_B); uprawnienia publiczne do opisu PRJOBD to *USE.

Na poziomie ochrony 30 lub niższym UŻYTKOWNIK_A może wyświetlić zbiór payroll wprowadzając zadanie wsadowe:

```
SBMJOB RQSDTA("Call PRLIST") JOBD(PRJOBD) +
                       USER(*JOBD)
```

Można temu zapobiec korzystając z poziomu ochrony 40 lub wyższego lub przez kontrolowanie uprawnień do opisów zadań, które mają podany profil użytkownika.

Czasami, dla poprawnego funkcjonowania niektórych rodzajów zadań wsadowych, wymagane jest podanie w opisie zadania określonej nazwy profilu użytkownika. Na przykład opis zadania QBATCH domyślnie ma ustawiony parametr USER(QPGMR). Ten opis zadania ma uprawnienia publiczne *EXCLUDE.

Jeśli poziom ochrony systemu ma wartość 30 lub mniejszą, dowolny użytkownik systemu z uprawnieniem do komendy Wprowadzenie zadania (Submit Job - SBMJOB) lub komend uruchamiania programu czytającego, i z uprawnieniem *USE do opisu zadania QBATCH, może wprowadzać zadania, korzystając z profilu programisty (QPGMR), jeśli ma do niego uprawnienia. Na poziomie ochrony 40 i wyższym, wymagane są uprawnienia *USE do profilu QPGMR.

Kolejka komunikatów operatora systemu

Menu Asysta Operacyjna (ASSIST) systemu iSeries udostępnia opcje do zarządzania systemem, użytkownikami oraz urządzeniami. Menu Zarządzanie systemem, użytkownikami i urządzeniami (Manage Your System, Users, and Devices) udostępnia opcję do pracy z komunikatami operatora systemu. Użytkownik może chcieć zapobiec odpowiadaniu na komunikaty z kolejki komunikatów QSYSOPR (operator systemu) przez użytkowników. Nieprawidłowe odpowiedzi na komunikaty operatora systemu mogą powodować problemy.

Odpowiadanie na komunikaty wymaga uprawnień *USE i *ADD do kolejki komunikatów. Usuwanie komunikatów wymaga uprawnień *USE i *DLT. (Patrz sekcja 391.) Uprawnienia do odpowiadania i usuwania komunikatów w

kolejce QSYSOPR należy nadać tylko użytkownikom z odpowiedzialnością operatora systemu. Uprawnieniami publicznymi do tej kolejki powinny być uprawnienia *OBJOPR i *ADD, co umożliwia dodawanie nowych komunikatów do kolejki QSYSOPR.

Uwaga: Wszystkie zadania muszą mieć możliwość dodawania nowych komunikatów do kolejki komunikatów QSYSOPR. Nie należy ustawiać uprawnień publicznych do kolejki QSYSOPR na uprawnienia *EXCLUDE.

Listy bibliotek

Lista bibliotek dla zadania wskazuje, które biblioteki mają być przeszukiwane, oraz kolejność, w jakiej mają być przeszukiwane. Gdy program określa obiekt, można podać jego nazwę kwalifikowaną, która obejmuje zarówno nazwę obiektu, jak i nazwę biblioteki. Biblioteka dla obiektu może być podana jako parametr *LIBL (lista bibliotek). Do odszukania obiektu wykorzystywane są biblioteki podane na liście bibliotek (w zadanej kolejności).

Tabela 117 podsumowuje części listy bibliotek oraz ich budowanie podczas zadania. Przedstawione poniżej sekcje omawiają ryzyko oraz sposoby zabezpieczania list bibliotek.

Tabela 117. Części listy bibliotek. Lista bibliotek przeszukiwana jest w następującej kolejności:

Część	Jak jest budowana
Część systemowa, 15 pozycji	Początkowo budowana za pomocą wartości systemowej QSYSLIBL. Może być zmieniona podczas zadania za pomocą komendy CHGSYSLIBL.
Część biblioteki produktu, 2 pozycje	Początkowo puste. Biblioteka dodawana jest do tej części, gdy jest uruchamiana komenda lub menu, dla którego podczas tworzenia podano tę bibliotekę w parametrze PRDLIB. Biblioteka pozostaje w części biblioteki produktu listy bibliotek do czasu zakończenia działania komendy lub menu.
Biblioteka bieżąca, 1 pozycja	Podawana w profilu użytkownika lub na ekranie Wpisanie się. Może być zmieniona, gdy komenda lub menu uruchamia bibliotekę podaną w parametrze CURLIB. Może być zmieniona podczas zadania za pomocą komendy CHGCURLIB.
Część użytkownika, 250 pozycji	Początkowo budowana za pomocą początkowej listy bibliotek z opisu zadania użytkownika. Jeśli opis zadania ma wartość *SYSVAL, używana jest wartość systemowa QUSRLIBL. Podczas zadania część użytkownika listy bibliotek może być zmieniona za pomocą komend ADDLIBLE, RMVLIBLE, CHGLIBL i EDTLIBL.

Ryzyko związane z ochroną w przypadku list bibliotek

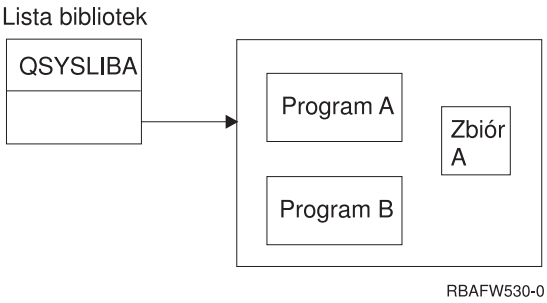
Listy bibliotek stanowią potencjalne ryzyko naruszenia ochrony. Jeśli użytkownik ma możliwość zmiany kolejności bibliotek na liście bibliotek lub możliwość dodania dodatkowych bibliotek do tej listy, to ma możliwość wykonywania funkcji, które naruszają wymagania ochrony.

Sekcja “Ochrona biblioteki i listy bibliotek” na stronie 117 udostępnia niektóre ogólne informacje dotyczące zagadnień związanych z listami bibliotek. Ten temat zawiera więcej przykładów możliwych naruszeń oraz sposoby ich uniknięcia.

Poniżej przedstawiono dwa przykłady pokazujące, jak zmiany na liście bibliotek mogą naruszyć wymagania ochrony:

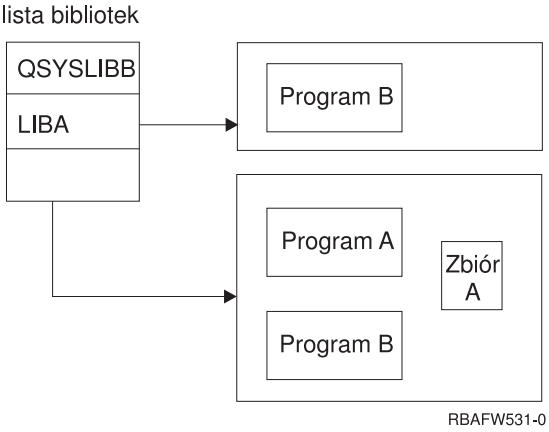
Zmiana w funkcji

Rys. 31 na stronie 188 pokazuje bibliotekę aplikacji. Program A wywołuje Program B, który znajduje się w bibliotece LIBA. Program B wykonuje aktualizację Zbioru A. Program B wywoływany jest bez nazwy kwalifikowanej, tak więc w celu jego odnalezienia przeszukiwana jest lista bibliotek.



Rysunek 31. Lista bibliotek – oczekiwane środowisko

Programista lub inny doświadczony użytkownik może umieścić inny Program B w bibliotece LIBB. Podstawiony program może wykonywać inne funkcje, takie jak kopiowanie poufnych danych lub nieprawidłowe aktualizowanie zbiorów. Jeśli biblioteka LIBB zostanie umieszczona na liście bibliotek przed biblioteką LIBA, zamiast oryginalnego Programu B uruchamiany jest podstawiony Program B, ponieważ program wywoływany jest bez nazwy kwalifikowanej:



Rysunek 32. Lista bibliotek – aktualne środowisko

Dostęp bez uprawnień do informacji

Przyjmijmy, że Program A z Rys. 31 adoptuje uprawnienia UŻYTKOWNIKA_1, który ma uprawnienia *ALL do Zbioru A. Program B jest wywoływany przez Program A (stosowane są uprawnienia adoptowane). Użytkownik, który ma odpowiednią wiedzę, może utworzyć podstawiony Program B, który po prostu wywołuje procesor komend. Użytkownik mógłby w ten sposób uzyskać dostęp do wiersza komend oraz do Zbioru A.

Zalecenia dotyczące części systemowej listy bibliotek

Część systemowa listy bibliotek przeznaczona jest dla bibliotek IBM. W tej części mogą być umieszczone biblioteki aplikacji, które są uważnie kontrolowane. Część systemowa listy bibliotek stanowi największe ryzyko naruszenia ochrony, ponieważ biblioteki znajdujące się w tej części przeszukiwane są w pierwszej kolejności.

Tylko użytkownik z uprawnieniami specjalnymi *ALLOBJ i *SECADM może zmieniać wartość systemową QSYSLIBL. Należy kontrolować i monitorować wszystkie zmiany dokonywane w części systemowej listy bibliotek. Podczas dodawania bibliotek należy skorzystać z następujących wskazówek:

- na tej liście powinny być umieszczane tylko te biblioteki, które są kontrolowane,
- użytkownicy publiczni nie powinni mieć do tych bibliotek uprawnień *ADD,
- kilka bibliotek IBM, takie jak QGPL ma domyślne uprawnienia publiczne *ADD z powodów produkcyjnych; należy regularnie monitorować jakie obiekty (szczególnie programy, zbiory źródłowe i komendy) dodawane są do tych bibliotek.

Komenda CHGSYSLIBL domyślne uprawnienia publiczne ma ustawione na *EXCLUDE. Tylko użytkownicy z uprawnieniami *ALLOBJ mogą korzystać z tej komendy, chyba że odpowiednie uprawnienie zostanie nadane innym użytkownikom. Jeśli systemowa lista bibliotek musi być tymczasowo zmieniona podczas zadania, można użyć techniki opisanej w temacie “Zmienianie systemowej listy bibliotek” na stronie 206.

Zalecenia dla bibliotek produktów

Część biblioteki produktu listy bibliotek przeszukiwana jest przed częścią użytkownika. Użytkownik, który ma wystarczającą wiedzę, może utworzyć komendę lub menu, które wstawia bibliotekę produktu do listy bibliotek. Na przykład poniższa instrukcja tworzy program CMDX, który uruchamia program PGMA:

```
CRTCMD CMDX PGM(PGMA) PRDLIB(LIBB)
```

Tak długo, jak działa program CMDX, biblioteka LIBB znajduje się w części produktu listy bibliotek.

Do zabezpieczenia części produktu listy bibliotek należy zastosować następujące środki:

- Należy kontrolować uprawnienia do komend Tworzenie komendy (Create Command - CRTCMD), Zmiana komendy (Change Command - CHGCMD), Tworzenie menu (Create Menu - CRTMNU) i Zmiana menu (Change Menu - CHGMNU).
- Podczas tworzenia komend i menu należy podać parametr PRDLIB(*NONE), który usuwa pozycje znajdujące się aktualnie w części produktu listy bibliotek. Zabezpiecza to przed przeszukiwaniem nieznanych bibliotek, zanim przeszukana zostanie biblioteka przeznaczona dla komendy lub menu.

  Uwaga: Wartością domyślną podczas tworzenia komendy lub menu jest PRDLIB(*NOCHG). Wartość *NOCHG oznacza, że gdy komenda lub menu jest uruchamiane, część biblioteki produktu listy bibliotek nie jest zmieniana.

Zalecenia dla biblioteki bieżącej

Biblioteka bieżąca może być użyta przez narzędzia do wspomagania podejmowania decyzji, takie jak Query/400. Wszystkie programy zapytania tworzone przez użytkownika domyślnie umieszczane są w bibliotece bieżącej użytkownika. Podczas tworzenia menu lub komendy można podać bibliotekę bieżącą, która ma być użyta podczas aktywowania menu.

Biblioteka bieżąca udostępnia użytkownikowi i programiście łatwy sposób tworzenia nowych obiektów, takich jak programy zapytania, bez konieczności martwienia się, gdzie powinny one być umieszczone. Jednak biblioteka bieżąca stanowi ryzyko ochrony, ponieważ jest ona przeszukiwana przed częścią użytkownika listy bibliotek. W celu zabezpieczenia ochrony systemu użytkownik może podjąć kilka środków ostrożności, pozostawiając możliwość używania biblioteki bieżącej:

- Dla pola *Ograniczenie możliwości* w profilu użytkownika należy podać wartość *YES. Zapobiega to zmianie biblioteki bieżącej na ekranie Wpisanie się (Sing On) lub używaniu komendy CHGPRF.
- Należy ograniczyć uprawnienia do komend Zmiana bieżącej biblioteki (Change Current Library - CHGCURLIB), Tworzenie menu (Create Menu - CRTMNU), Zmiana menu (Change Menu - CHGMNU), Tworzenie komendy (Create Command - CRTCMD) i Zmiana komendy (Change Command - CHGCMD).
- W celu ustawienia biblioteki bieżącej podczas przetwarzania aplikacji należy użyć techniki opisanej w sekcji “Kontrolowanie listy bibliotek użytkownika” na stronie 205.

Zalecenia dla części użytkownika listy bibliotek

Fragment listy bibliotek zawierający nazwy użytkowników często zmienia więcej niż inne fragmenty i jest trudniejszy do kontrolowania. Listę bibliotek zmienia wiele aplikacji. Mają na nią wpływ także opisy zadań.

Poniżej przedstawiono kilka sugerowanych alternatyw dotyczących kontrolowania części użytkownika listy bibliotek, które uniemożliwiają użycie nieuprawnionych bibliotek z podstawionymi programami i zbiorami podczas przetwarzania:

- Należy ograniczyć użytkowników aplikacji produkcyjnych do środowiska menu. Pole *Ograniczenie możliwości* w profilu użytkownika należy ustawić na *YES, w celu ograniczenia możliwości wprowadzania komend. Sekcja “Planowanie menu” na stronie 207 udostępnia przykład takiego środowiska.
- W aplikacjach należy używać nazw kwalifikowanych (dla obiektów i bibliotek). Zapobiega to przeszukiwaniu przez system listy bibliotek.
- Należy kontrolować możliwość zmiany opisów zadań, ponieważ opis zadania ustawia początkową listę bibliotek dla zadania.
- Na początku programu należy użyć komendy Dodanie pozycji listy bibliotek (Add Library List Entry - ADDLIBLE), aby upewnić się, że żądane obiekty znajdują się na początku części użytkownika listy bibliotek. Na końcu programu biblioteka może być usunięta.

  Jeśli biblioteka już znajduje się na liście, ale użytkownik nie jest pewien, czy znajduje się ona na początku listy, należy ją usunąć i dodać ponownie. Jeśli kolejność listy bibliotek jest ważna dla innych aplikacji w systemie, należy użyć następnej metody.
- Należy użyć programu, który odtwarza i składuje listę bibliotek dla zadania. Listę bibliotek należy zastąpić listą wymaganą dla aplikacji. Gdy aplikacja zakończy swoje działanie, należy przywrócić ustawienie początkowe listy bibliotek. Przykład użycia tej techniki zawiera sekcja “Kontrolowanie listy bibliotek użytkownika” na stronie 205.

Drukowanie

Większość informacji drukowanych w systemie przechowywana jest jako zbiory buforowe w kolejce wyjściowej, które oczekują na wydrukowanie. Gdy ochrona kolejek wyjściowych w systemie nie jest kontrolowana, nieuprawnieni użytkownicy mogą wyświetlać, drukować, a nawet kopiować poufne informacje oczekujące na drukowanie.

Jedną z metod zabezpieczania poufnych wydruków jest utworzenie specjalnej kolejki wyjściowej. Poufne wydruki należy wysyłać do takiej kolejki wyjściowej i kontrolować, kto może przeglądać i zmieniać zbiory buforowe w tej kolejce.

Aby określić, gdzie wydruki są kierowane, system sprawdza kolejno zbiór drukarkowy, atrybuty zadania, profil użytkownika, opis stacji roboczej oraz wartość systemową drukarki (QPRTDEV). Jeśli używane są wartości domyślne, używana jest kolejka wyjściowa związana z drukarką QPRTDEV. Przykłady kierowania wydruków do określonej kolejki wyjściowej zawiera podręcznik *Printer Device Programming*.

Ochrona zbiorów buforowych

Zbiór buforowy to specjalny typ obiektu. Nie można bezpośrednio nadać lub odwołać uprawnień do przeglądania i zmieniania zbioru buforowego. Uprawnienia do takiego zbioru kontrolowane są przez kilka parametrów kolejki wyjściowej, w której się znajduje.

Użytkownik tworzący zbiór buforowy jest jego właścicielem. Zawsze może on przeglądać i zmieniać dowolne, własne zbiory buforowe, bez względu na to, jak zdefiniowane są uprawnienia do kolejki wyjściowej. W celu dodawania nowych pozycji do kolejki wyjściowej użytkownik musi mieć uprawnienia *READ. Jeśli uprawnienia do kolejki wyjściowej zostaną usunięte, użytkownik nadal ma dostęp do własnych pozycji znajdujących się w takiej kolejce, za pomocą komendy Praca ze zbiorami buforowymi (Work with Spooled Files - WRKSPLF).

Parametry ochrony dla kolejki wyjściowej określane są za pomocą komendy Tworzenie kolejki wyjściowej (Create Output Queue - CRTOUTQ) lub Zmiana kolejki wyjściowej (Change Output Queue - CHGOUTQ). Parametry ochrony dla kolejki wyjściowej można wyświetlić za pomocą komendy Praca z opisem kolejki wyjściowej (Work with Output Queue Description - WRKOUTQD).

Uwaga: Użytkownik z uprawnieniami specjalnymi *SPLCTL może wykonywać dowolne funkcje na wszystkich pozycjach, bez względu na to, jak jest zdefiniowana kolejka wyjściowa. Niektóre parametry kolejki wyjściowej umożliwiają użytkownikowi z uprawnieniami specjalnymi *JOBCTL przeglądanie zawartości pozycji takiej kolejki.

Parametr kolejki wyjściowej - wyświetlanie danych (DSPDTA)

Parametr DSPDTA przeznaczony jest do zabezpieczenia zawartości zbioru buforowego. Określa, jakie uprawnienia potrzebne są do wykonania następujących funkcji na zbiorach buforowych, których właścicielami są inni użytkownicy:

- przeglądanie zawartości zbioru buforowego (komenda DSPSPLF),
- kopiowanie zbioru buforowego (komenda CPYSPLF)
- wysyłanie zbioru buforowego (komenda SNDNETSPLF)
- przenoszenie zbioru buforowego do innej kolejki wyjściowej (komenda CHGSPLFA).

Możliwe wartości parametru DSPDTA

***NO**	Użytkownik nie może wyświetlać, wysyłać lub kopiować zbiorów buforowych, którychwłaścicielami są inni użytkownicy, chyba że ma następujące uprawnienia: • uprawnienia specjalne *JOBCTL, jeśli parametr OPRCTL ma wartość *YES, • uprawnienia *READ, *ADD i *DLT do kolejki wyjściowej, jeśli parametr *AUTCHK ma wartość *DTAAUT, • prawo własności do kolejki wyjściowej, jeśli parametr *AUTCHK ma wartość *OWNER.
***YES**	Każdy użytkownik z uprawnieniami *READ do kolejki wyjściowej może wyświetlać, kopiować lub wysyłać dane zbiorów buforowych należących do innych użytkowników.
***OWNER**	Tylko właściciel zbioru buforowego lub użytkownik z uprawnieniami *SPLCTL (kontrola buforu) może wyświetlać, kopiować, wysyłać lub przenosić zbiór. Jeśli wartość parametru OPRCTL jest równa *YES, użytkownicy z uprawnieniami specjalnymi *JOBCTL mogą wstrzymywać, zmieniać, usuwać i zwalniać zbiory buforowe z kolejki wyjściowej, ale nie mogą ich wyświetlać, kopiować, wysyłać lub przenosić. Ta opcja przeznaczona jest dla operatorów w celu zarządzania pozycjami w kolejce wyjściowej, bez możliwości przeglądania ich zawartości.

Parametr kolejki wyjściowej - Uprawnienia do sprawdzania (AUTCHK)

Parametr AUTCHK określa, czy uprawnienia *READ, *ADD i *DLT do kolejki wyjściowej umożliwiają użytkownikowi zmianę i usuwanie zbiorów buforowych należących do innych użytkowników.

Możliwe wartości parametru AUTCHK

***OWNER**	Tylko użytkownik, który jest właścicielem kolejki wyjściowej, może zmieniać lub usuwać zbiory buforowe należące do innych użytkowników.
***DTAAUT**	Określa, że każdy użytkownik z uprawnieniami *READ, *ADD i *DLT do kolejki wyjściowej może zmienić lub usunąć zbiory buforowe należące do innych użytkowników.

Parametr kolejki wyjściowej: Sterowane przez operatora (OPRCTL)

Parametr OPRCTL określa, czy użytkownik z uprawnieniami specjalnymi *JOBCTL może sterować kolejką wyjściową.

Możliwe wartości parametru OPRCTL

***YES**	Użytkownik z uprawnieniami specjalnymi *JOBCTL może wykonywać wszystkie funkcje na zbiorach buforowych, chyba że parametr DSPDTA ma wartość *OWNER. Jeśli parametr DSPDTA ma wartość *OWNER, uprawnienia specjalne *JOBCTL nie zezwalają użytkownikowi na wyświetlanie, kopiowanie, wysyłanie lub przenoszenie zbiorów buforowych.
***NO**	Uprawnienia specjalne *JOBCTL nie dają użytkownikowi uprawnień do wykonywania operacji na kolejce wyjściowej. Zastosowanie mają zwykłe reguły uprawnień.

Uprawnienia do kolejki wyjściowej i parametry wymagane do drukowania

Tabela 118 pokazuje, jaka kombinacja parametrów kolejki wyjściowej oraz uprawnień do takiej kolejki jest wymagana do wykonywania w systemie funkcji zarządzania drukowaniem. Dla niektórych funkcji przedstawiona jest więcej niż jedna kombinacja. Właściciel zbioru buforowego zawsze może wykonywać wszystkie funkcje na tym zbiorze. Więcej informacji na ten temat zawiera sekcja “Komendy programu piszącego” na stronie 443.

Uprawnienia oraz parametry kolejki wyjściowej dla wszystkich komend związanych ze zbiorami buforowymi zostały opisane w sekcji “Komendy zbioru buforowego” na stronie 428. Komendy kolejki wyjściowej zostały opisane w sekcji “Komendy kolejki wyjściowej” na stronie 404.

Uwaga: Użytkownik z uprawnieniami specjalnymi *SPLCTL (kontrola buforu) nie jest obiektem żadnych ograniczeń uprawnień związanych z kolejkami wyjściowymi. Uprawnienia specjalne *SPLCTL umożliwiają użytkownikowi wykonywanie wszystkich operacji na wszystkich kolejkach wyjściowych. Dlatego należy rozważnie nadawać uprawnienia specjalne *SPLCTL.

Tabela 118. Uprawnienia wymagane do wykonywania funkcji drukowania

	Parametry kolejki wyjściowej			Uprawnienia do kolejki wyjściowej	Uprawnienie specjalne
Funkcja drukowania	**DSPDTA**	**AUTCHK**	**OPRCTL**		
Dodawanie zbiorów buforowych do kolejki[1]				*READ	Brak
			*YES		*JOBCTL
Przeglądanie listy zbiorów buforowych (komenda WRKOUTQ[2])				*READ	Brak
			*YES		*JOBCTL
Wyświetlanie, kopiowanie lub wysyłanie zbiorów buforowych	*YES			*READ	Brak
	*NO	*DTAAUT		*READ, *ADD, *DLT	Brak
(DSPSPLF, CPYSPLF, SNDNETSPLF, SNDTCPSP[2])					
	*NO	*OWNER		Właściciel [3]	Brak
	*YES		*YES		*JOBCTL
	*NO *OWNER		*YES		*JOBCTL
Zmiana, usunięcie, wstrzymanie i zwolnienie zbioru buforowego (CHGSPLFA, DLTSPLF, HLDSPLF, RLSSPLF [2])		*DTAAUT		*READ, *ADD, *DLT	Brak
		*OWNER		Właściciel [3]	Brak
			*YES		*JOBCTL
Zmiana, usunięcie zawartości, wstrzymanie i zwolnienie kolejki wyjściowej (CHGOUTQ, CLROUTQ, HLDOUTQ, RLSOUTQ [2])		*DTAAUT		*READ, *ADD, *DLT	Brak
		*OWNER		Właściciel [3]	Brak
			*YES		*JOBCTL
Uruchomienie programu piszącego dla kolejki (STRPRTWTR, STRRMTWTR [2])		*DTAAUT		*CHANGE	Brak
			*YES		*JOBCTL

[1] Jest to uprawnienie wymagane do kierowania wydruków do kolejki wyjściowej.

[2] Na ekranie należy używać tych komend lub odpowiadających im opcji.

[3] Użytkownik musi być właścicielem kolejki wyjściowej.

[4] Wymaga także uprawnień *USE do opisu drukarki.

[5] Parametr *CHGOUTQ oprócz uprawnień *READ, *ADD i *DLT wymaga uprawnienia *OBJMGT do kolejki wyjściowej.

Przykłady: kolejka wyjściowa

Poniżej przedstawiono kilka przykładów ustawiania parametrów dla kolejek wyjściowych, tak aby spełniały różne wymagania:

- Tworzenie kolejki wyjściowej ogólnego przeznaczenia. Wszyscy użytkownicy mają uprawnienia do wyświetlania wszystkich zbiorów buforowych. Operatorzy systemu mogą zarządzać kolejką i zmieniać zbiory buforowe:

  ```
  CRTOUTQ OUTQ(QGPL/GPOUTQ) DSPDTA(*YES) +
          OPRCTL(*YES) AUTCHK(*OWNER) AUT(*USE)
  ```

- Tworzenie kolejki wyjściowej dla aplikacji. Taką kolejkę wyjściową mogą wykorzystywać jedynie członkowie profilu grupowego GRPA. Wszyscy uprawnieni użytkownicy kolejki wyjściowej mogą wyświetlać wszystkie zbiory buforowe. Operatorzy systemu nie mogą pracować z kolejką wyjściową:

  ```
  CRTOUTQ OUTQ(ARLIB/AROUTQ) DSPDTA(*YES) +
          OPRCTL(*NO) AUTCHK(*OWNER) AUT(*EXCLUDE)
  GRTOBJAUT OBJ(ARLIB/AROUTQ) OBJTYP(*OUTQ) +
          USER(GRPA)  AUT(*CHANGE)
  ```

- Tworzenie poufnej kolejki wyjściowej dla szefów ochrony, do drukowania informacji dotyczących profili użytkowników i uprawnień. Kolejka wyjściowa jest tworzona i należy do profil QSECOFR.

  ```
  CRTOUTQ OUTQ(QGPL/SECOUTQ) DSPDTA(*OWNER) +
          AUTCHK(*DTAAUT) OPRCTL(*NO) +
           AUT(*EXCLUDE)
  ```

  Nawet jeśli szefowie ochrony w systemie mają uprawnienia *ALLOBJ, nie mają możliwości dostępu do zbiorów buforowych w kolejce wyjściowej SECOUTQ należących do innych użytkowników.

- Tworzenie kolejki wyjściowej, która jest współużytkowana przez użytkowników drukujących poufne zbiory i dokumenty. Użytkownicy mogą pracować tylko z własnymi zbiorami buforowymi. Operatorzy systemu mogą pracować ze zbiorami buforowymi, ale nie mogą wyświetlać ich zawartości.

  ```
  CRTOUTQ OUTQ(QGPL/CFOUTQ) DSPDTA(*OWNER) +
          AUTCHK(*OWNER) OPRCTL(*YES) AUT(*USE)
  ```

Atrybuty sieciowe

Atrybuty sieciowe kontrolują sposób komunikowania się systemu z innymi systemami. Niektóre atrybuty sieciowe kontrolują sposób przetwarzania zadań oraz obsługę dostępu do informacji przez zdalne żądania. Niżej wymienione atrybuty sieciowe mają bezpośredni wpływ na ochronę systemu i zostały omówione w przedstawionych poniżej tematach:

działanie zadania (JOBACN),

dostęp Żądanie klienta (PCSACC),

dostęp żądanie DDM (DDMACC).

Możliwe wartości każdego atrybutu sieciowego. Wartość domyślna została podkreślona. Aby ustawić wartość atrybutu sieciowego, należy użyć komendy Zmiana atrybutów sieciowych (Change Network Attribute - CHGNETA).

Atrybut sieciowy: działanie zadania (JOBACN)

Atrybut sieciowy JOBACN, określa w jaki sposób system przetwarza nadchodzące żądania uruchomienia zadań.

Możliwe wartości parametru JOBACN:

***REJECT**	Strumień wejściowy jest odrzucany. Do wysyłającego oraz do przewidywanego odbiorcy wysyłany jest komunikat informujący, że strumień wejściowy został odrzucony.
***FILE**	Strumień wejściowy wprowadzany jest do kolejki zbiorów sieciowych dla użytkownika odbierającego. Taki użytkownik może wyświetlić, anulować lub odebrać strumień wejściowy do zbioru bazy danych lub wprowadzić go do kolejki zadań. Do wysyłającego oraz do odbiorcy wysyłany jest komunikat informujący, że strumień wejściowy został wprowadzony.
***SEARCH**	Tabela zadań sieciowych kontroluje działania za pomocą wartości w tabeli.

Zalecenia

Jeśli użytkownik nie oczekuje na zdalne żądania zadań, atrybut JOBACN należy ustawić na *REJECT.

Więcej informacji na temat atrybutu JOBACN zawiera podręcznik *SNA Distribution Services*.

Atrybut sieciowy: dostęp Żądanie klienta (PCSACC)

Atrybut sieciowy PCSACC określa sposób przetwarzania przez program licencjonowany iSeries Access for Windows żądań dostępu do obiektów pochodzących z przyłączonych komputerów osobistych. Atrybut sieciowy PCSACC kontroluje, czy zadania komputera osobistego mogą uzyskać dostęp do obiektów systemu iSeries, a nie czy komputer osobisty może korzystać z funkcji emulowania stacji roboczej.

Uwaga: Atrybut sieciowy PCSACC kontroluje jedynie klientów DOS i OS/2. Ten atrybut nie wpływa na pozostałych klientów iSeries Access.

Możliwe wartości parametru PCSACC:

***REJECT**	Program iSeries Access odrzuca każde żądanie z komputera osobistego dotyczące dostępu do obiektów w systemie iSeries. Do aplikacji PC wysyłany jest komunikat o błędzie.
***OBJAUT**	Programy iSeries Access w systemie sprawdzają zwykłe uprawnienia do obiektu dla każdego żądania obiektu przez programu PC. Na przykład jeśli żądane jest przesłanie zbioru, sprawdzane są uprawnienia do kopiowania danych ze zbioru bazy danych.
***REGFAC**	System korzysta z systemowego narzędzia do rejestracji w celu określenia, który program obsługi wyjścia (jeśli istnieje) ma być uruchomiony. Jeśli dla punktu wyjścia nie zdefiniowano żadnego programu obsługi wyjścia, a podano powyższą wartość, użyta zostanie wartość *OBJAUT.
kwalifikowana_nazwa_programu	Program iSeries Access wywołuje ten program obsługi wyjścia napisany przez użytkownika w celu określenia, czy żądanie komputera PC powinno zostać odrzucone. Program obsługi wyjścia wywoływany jest tylko wtedy, gdy zwykłe sprawdzanie uprawnień zakończy się pomyślnie. Program iSeries Access przekazuje do programu obsługi wyjścia informacje o użytkowniku oraz żądanej funkcji. Program zwraca kod wskazujący, czy żądanie powinno być przyjęte, czy odrzucone. Jeśli kod powrotu wskazuje, że żądanie powinno zostać odrzucone lub wystąpi błąd, do komputera osobistego wysyłany jest komunikat o błędzie.

Niebezpieczeństwa i zalecenia

Jeśli w systemie zainstalowany jest program iSeries Access, zwykłe środki ochrony mogą być niewystarczające. Na przykład jeśli użytkownik ma uprawnienia *USE do zbioru, a atrybut sieciowy PCSACC ma wartość *OBJAUT, użytkownik może użyć programu iSeries Access oraz programu na komputerze osobistym, w celu przesłania całego zbioru do komputera osobistego. Następnie może skopiować dane na dyskietkę lub taśmę i usunąć je lokalnie.

Jest kolka metod zabezpieczania się przed kopiowaniem zbioru przez użytkownika stacji roboczej systemu iSeries z uprawnieniami *USE:

- ustawienie parametru LMTCPB(*YES) w profilu użytkownika,
- ograniczanie uprawnień do komend, które kopiują zbiory,
- ograniczanie uprawnień do komend używanych przez program iSeries Access,
- nie nadawanie użytkownikowi uprawnień *ADD do biblioteki; uprawnienia *ADD wymagane są do utworzenia nowego zbioru w bibliotece,
- nie nadawanie użytkownikowi dostępu do urządzeń *SAVRST.

Żadna z tych metod nie nie dotyczy użytkownika PC programu licencjonowanego iSeries. Jedynym odpowiednim środkiem ochrony jest używanie programu obsługi wyjścia sprawdzającego wszystkie żądania.

Program iSeries Access przekazuje informacje do programu obsługi wyjścia użytkownika wywoływanego przez atrybut sieciowy PCSACC, dla następujących typów dostępu:

przesyłanie zbioru,
drukowanie wirtualne,
komunikat,
folder współużytkowany.

Dodatkowe informacje dotyczące produktu iSeries Access znajdują się w Centrum informacyjnym (patrz “Informacje wstępne i pokrewne” na stronie xvi, aby uzyskać szczegółowe informacje).

Atrybut sieciowy: żądanie dostępu DDM (DDMACC)

Atrybut sieciowy DDMACC określa, w jaki sposób system przetwarza żądania z innych systemów dotyczące dostępu do danych za pomocą funkcji zarządzania danymi rozproszonymi (DDM) lub rozproszonej relacyjnej bazy danych.

Możliwe wartości parametru DDMACC:

***REJECT**	System nie zezwala na żądania DDM lub DRDA ze zdalnych systemów. Wartość *REJECT nie zabezpiecza takiego systemu przed działaniem jako systemu requestera oraz wysyłaniem żądań do innych serwerów.
***OBJAUT**	Zdalne żądania kontrolowane są przez uprawnienia do obiektu.
kwalifikowana_nazwa_programu	Ten program obsługi wyjścia napisany przez użytkownika wywoływany jest po sprawdzeniu zwykłych uprawnień do obiektu. Program obsługi wyjścia wywoływany jest tylko dla zbiorów DDM, a nie dla funkcji rozproszonej relacyjnej bazy danych. Program obsługi wyjścia otrzymuje listę parametrów, utworzoną przez system zdalny, która identyfikuje użytkownika systemu lokalnego oraz żądanie. Program analizuje żądanie i wysyła kod powrotu, nadający lub odmawiający żądanego dostępu.

Więcej informacji dotyczących atrybutu sieciowego DDMACC oraz zagadnień dotyczących ochrony związanej z DDM zawiera Centrum informacyjne (patrz sekcja “Informacje wstępne i pokrewne” na stronie xvi).

Operacje składowania i odtwarzania

Możliwość składowania obiektów z danego systemu lub odtwarzania ich w systemie stanowi ryzyko naruszenia ochrony.

Na przykład programiści często mają uprawnienia *OBJEXIST do programów, ponieważ są one wymagane do ponownego kompilowania programu (i usuwania starej kopii). Uprawnienia *OBJEXIST wymagane są także do składowania obiektu. Dlatego typowy programista może wykonać kopię programów, które mają sporą wartość finansową.

Użytkownik z uprawnieniami *OBJEXIST do obiektu może także odtworzyć nową kopię obiektu na istniejącym obiekcie. W przypadku programu, odtwarzany program mógł być tworzony w innym systemie. Może wykonywać inne funkcje. Na przykład gdy oryginalny program pracował z poufnymi danymi. Nowa wersja może wykonywać te same funkcje, ale może także zapisywać kopię poufnych informacji w tajnym zbiorze w bibliotece programisty. Programista nie potrzebuje uprawnień do poufnych danych, ponieważ to zwykli użytkownicy będą uzyskiwali dostęp do danych.

Ograniczanie operacji składowania i odtwarzania

Użytkownik może kontrolować możliwość składowania i odtwarzania obiektów na kilka sposobów:

- przez ograniczenie dostępu do urządzeń składowania i odtwarzania, takich jak jednostki taśm, jednostki optyczne i jednostki dyskietek,
- przez ograniczenie uprawnień do obiektów opisów urządzeń dla urządzeń składowania i odtwarzania; aby zeskładować obiekt na jednostce taśm, użytkownik musi mieć uprawnienia *USE do opisu urządzenia dla jednostki taśm,
- przez ograniczenie komend składowania i odtwarzania; umożliwia to kontrolowanie, jakie dane składowane z systemu oraz odtwarzane we wszystkich interfejsach - łącznie ze zbiorami składowania; przykład sposobu działania

tej metody zawiera sekcja “Przykład: ograniczanie komend składowania i odtwarzania”; podczas instalowania systemu uprawnienia publiczne do komend odtwarzania ustawiane są na PUBLIC(*EXCLUDE),

- przez nadawanie uprawnień specjalnych *SAVSYS tylko zaufanym użytkownikom.

Przykład: ograniczanie komend składowania i odtwarzania

Poniżej przedstawiono przykład czynności, które można wykonać w celu ograniczenia komend składowania i odtwarzania:

1. Aby utworzyć listę autoryzacji, którą można wykorzystać do nadania uprawnień do komend dla operatorów systemu, należy wpisać następującą komendę:

   ```
   CRTAUTL AUTL(SRLIST) TEXT('Lista składowania i odtwarzania')
            AUT(*EXCLUDE)
   ```

2. Aby użyć tej listy do zabezpieczenia komend składowania, należy wpisać:

   ```
   GRTOBJAUT OBJ(SAV*) OBJTYPE(*CMD) AUTL(SRLIST)
   ```

3. Aby upewnić się, że uprawnienia *PUBLIC pochodzą z listy autoryzacji, należy wpisać komendę:

   ```
   GRTOBJAUT OBJ(SAV*) OBJTYPE(*CMD) USER(*PUBLIC)
      AUT(*AUTL)
   ```

4. Aby użyć tej listy do zabezpieczenia komend odtwarzania, należy wpisać:

   ```
   GRTOBJAUT OBJ(RST*) OBJTYPE(*CMD) AUTL(SRLIST)
   ```

5. Aby upewnić się, że uprawnienia *PUBLIC pochodzą z listy autoryzacji, należy wpisać komendę:

   ```
   GRTOBJAUT OBJ(RST*) OBJTYPE(*CMD) USER(*PUBLIC)
      AUT(*AUTL)
   ```

6. Chociaż operatorzy systemu odpowiedzialni za składowanie systemu mają uprawnienia specjalne *SAVSYS, muszą mieć nadane jawne uprawnienia do komend SAVxxx. Można to zrobić dodając operatorów systemu do listy autoryzacji:

   ```
   ADDAUTLE AUTL(SRLIST) USER(USERA USERB) AUT(*USE)
   ```

   Uwaga: Operatorzy systemu mogą mieć uprawnienia tylko do komend składowania. W takim przypadku należy zabezpieczyć komendy składowania i odtwarzania za pomocą oddzielnych list autoryzacji.

7. Aby ograniczyć funkcje API do składowania i odtwarzania oraz zabezpieczyć je za pomocą listy autoryzacji, należy wpisać następujące komendy:

   ```
   GRTOBJAUT OBJ(QSRSAVO) OBJTYPE(*PGM) AUTL(SRLIST)
   GRTOBJAUT OBJ(QSRSAVO) OBJTYPE(*PGM) USER(*PUBLIC)
      AUT(*AUTL)
   GRTOBJAUT OBJ(QSRLIB01) OBJTYPE(*SRVPGM) AUTL(SRLIST)
   GRTOBJAUT OBJ(QSRLIB01) OBJTYPE(*SRVPGM) USER(*PUBLIC)
      AUT(*AUTL)
   ```

Strojenie wydajności

Monitorowanie oraz strojenie wydajności nie należy do obowiązków szefa ochrony. Jednak szef ochrony powinien upewnić się, że użytkownicy nie zmieniają parametrów wydajności systemu, aby przyspieszać własne zadania kosztem innych.

Na wydajność zadań w systemie ma wpływ kilka obiektów zarządzania pracą:

- Klasa ustawia priorytet uruchomienia oraz przedział czasu dla zadania.
- Pozycja routingu w opisie podsystemu określa klasę oraz pulę pamięci używane przez zadanie.
- Opis zadania może określać kolejkę wyjściową, priorytet wyjścia, kolejkę zadań oraz priorytet zadania.

Użytkownicy z odpowiednimi uprawnieniami, którzy mają wystarczającą wiedzę, mogą utworzyć w systemie własne środowisko i zyskać dla siebie lepszą wydajność niż inni użytkownicy. Należy to kontrolować ograniczając uprawnienia do tworzenia i zmiany obiektów zarządzania pracą. Uprawnienia publiczne dla komend zarządzania pracą należy ustawić na *EXCLUDE i nadać uprawnienia do nich tylko kilku zaufanym użytkownikom.

Parametry wydajności mogą być zmienione także interaktywnie. Na przykład na ekranie Praca ze statusem systemu (Work with System Status - WRKSYSSTS) można zmienić wielkości pul pamięci oraz poziomów aktywności. Użytkownik z uprawnieniami specjalnymi *JOBCTL (sterowanie zadaniem) może także zmienić priorytet harmonogramu dowolnego zadania w systemie, w zależności od limitu priorytetu (PTYLMT) w profilu użytkownika. Uprawnienia specjalne *JOBCTL oraz parametr PTYLMT w profilach użytkowników należy ustawiać ostrożnie.

Aby umożliwić użytkownikom przeglądanie za pomocą komendy WRKSYSSTS informacji o wydajności, ale nie ich zmianę, należy wykonać następujące komendy:

```
GRTOBJAUT OBJ(CHGSHRPOOL) OBJTYPE(*CMD) +
          USER(*PUBLIC)   AUT(*EXCLUDE)
```

Użytkownikom odpowiedzialnym za strojenie systemu należy nadać uprawnienia do zmiany parametrów wydajności:

```
GRTOBJAUT OBJ(CHGSHRPOOL) OBJTYPE(*CMD) +
          USER(USRTUNE)   AUT(*USE)
```

Ograniczanie zadań do wsadowych

Istnieje możliwość utworzenia lub zmiany komend w celu ograniczenia pewnych zadań, aby były uruchamiane tylko w środowisku wsadowym. Na przykład niektóre raporty lub programy mają być uruchamiane tylko w środowisku wsadowym. Zadanie uruchomione w trybie wsadowym często wpływa na wydajność systemu mniej niż takie samo zadanie uruchomione interaktywnie.

Na przykład, aby ograniczyć komendę, która uruchamia program RPTA, aby uruchamiała go tylko jako zadanie wsadowe, należy wykonać następujące czynności:

- Utwórz komendę do uruchamiania programu RPTA i określ, że ta komenda może być uruchamiana jedynie w środowisku wsadowym:

  ```
  CRTCMD CMD(RPTA) PGM(RPTA) ALLOW(*BATCH *BPGM)
  ```

Aby ograniczyć kompilowanie tylko do zadań wsadowych, dla komendy tworzenia dla każdego typu programu należy wykonać następujące polecenie:

```
CHGCMD CMD(CRTxxxPGM) ALLOW(*BATCH *BPGM),
```

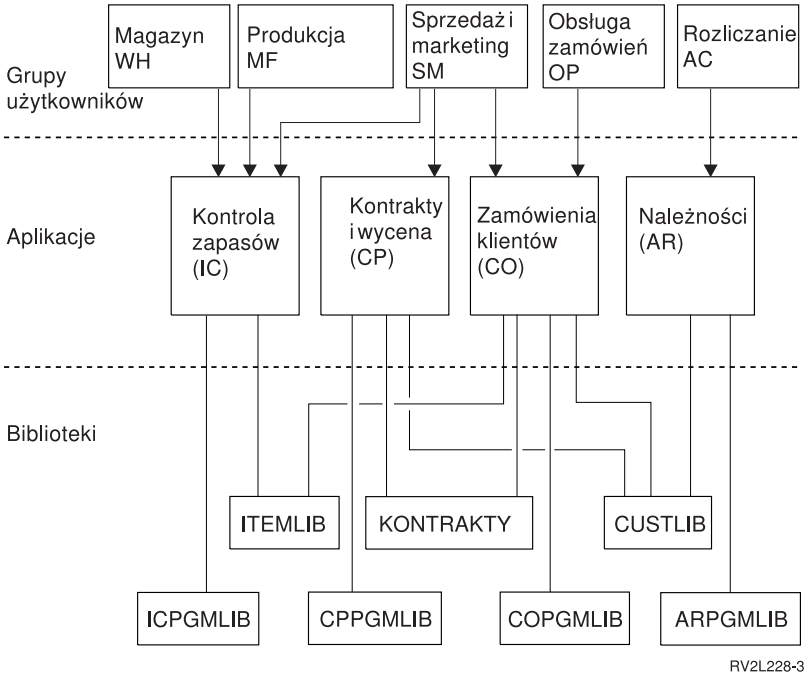
Rozdział 7. Projektowanie ochrony

Ochrona informacji jest ważną częścią większości aplikacji. Dlatego już podczas projektowania aplikacji należy, razem z innymi wymaganiami, rozważyć także zagadnienia dotyczące ochrony. Na przykład podczas decydowania o sposobie zorganizowania informacji aplikacji w biblioteki, należy spróbować zrównoważyć wymagania ochrony z innymi zagadnieniami, takimi jak wydajność aplikacji oraz składowanie i odtwarzanie.

Ten rozdział zawiera wskazówki pomagające programistom aplikacji oraz menedżerom systemów włączyć ochronę jako część ogólnego projektu. Zawiera także przykłady technik, których można użyć do spełnienia wymagań dotyczących ochrony systemu. Niektóre przykłady w tym rozdziale zawierają przykładowe programy. Te programy zostały dołączone jedynie w celu ilustracji. Wiele z nich nie skompiluje się lub nie uruchomi się pomyślnie w podanej postaci, ani nie zawiera obsługi komunikatów oraz odzyskiwania po błędzie.

Temat Podstawowa ochrona systemu i jej planowanie znajdujący się w Centrum informacyjnym przeznaczony jest dla administratorów ochrony. Zawiera formularze, przykłady oraz wskazówki dotyczące planowania ochrony dla aplikacji, które już zostały napisane. Jeśli użytkownik jest odpowiedzialny za projektowanie aplikacji, przydatne może być zapoznanie się z formularzami oraz przykładami z Centrum informacyjnego (patrz sekcja “Informacje wstępne i pokrewne” na stronie xvi). Mogą one pomóc spojrzeć na aplikację z perspektywy administratora ochrony oraz zrozumieć, jakie informacje należy udostępnić.

Temat Podstawowa ochrona systemu i jej planowanie w Centrum informacyjnym korzysta także z zestawu przykładowych aplikacji dla fikcyjnego przedsiębiorstwa nazwanego JKL Toy Company. Ten rozdział omawia uwagi dotyczące projektowania dla tego samego zestawu przykładowych aplikacji. Rys. 33 pokazuje powiązania między grupami użytkowników, aplikacjami oraz bibliotekami dla przedsiębiorstwa JKL Toy Company:



Rysunek 33. Przykładowe aplikacje

Opis rysunku

Ten rysunek pokazuje, w jaki sposób pięć zestawów grup użytkowników korzysta z dostępu do aplikacji oraz bibliotek w systemie przedsiębiorstwa JKL Toy. Grupy użytkowników to: Magazyn, Produkcja, Sprzedaż i marketing, Obsługa

zamówień oraz Księgowość. Grupy użytkowników Magazynu, Produkcji oraz Sprzedaży i marketingu mają dostęp do aplikacji Kontrola zapasów. Grupa użytkowników Sprzedaży i marketingu ma także dostęp do aplikacji Kontrakty i wycena oraz Zamówienia klientów. Użytkownicy z grupy Obsługa zamówień mają dostęp do aplikacji Zamówienia klientów. Księgowość korzysta z aplikacji Należności.

Zalecenia ogólne

Zalecenia przedstawione w tym rozdziale oraz w temacie Podstawowa ochrona systemu i jej planowanie w Centrum informacyjnym opierają się na jednej ważnej zasadzie: prostota. Utrzymywanie projektu ochrony tak prostego jak to tylko możliwe, ułatwia zarządzanie i kontrolę ochrony. Zwiększa także wydajność aplikacji oraz tworzenia kopii zapasowych.

Poniżej przedstawiono listę ogólnych zaleceń dotyczących projektu ochrony:

- Aby zabezpieczyć informacje, ochrony zasobów należy używać razem z innymi dostępnymi metodami, takimi jak ograniczanie możliwości w profilu użytkownika oraz ograniczanie użytkowników do zestawu menu.

  Uwaga: W przypadku użycia produktu iSeries Access lub bezpośredniego podłączenia linii komunikacyjnej do systemu ograniczenie możliwości profili i dostępu do menu nie jest wystarczające, aby zapewnić ochronę systemu. Należy użyć ochrony zasobów, aby zabezpieczyć te obiekty, do których dostęp za pośrednictwem tych interfejsów ma być niemożliwy.
- Należy zabezpieczać tylko te obiekty, które naprawdę wymagają ochrony. Należy przeanalizować bibliotekę, aby określić, które obiekty, takie jak zbiory danych, są poufne, i zabezpieczyć te obiekty. Dla pozostałych obiektów, takich jak obszary danych i kolejki komunikatów, należy wykorzystać uprawnienia publiczne.
- Od ogółu do szczegółu:
  - należy planować ochronę bibliotek i katalogów; pojedynczymi obiektami należy zająć się tylko w razie konieczności,
  - najpierw należy planować uprawnienia publiczne, po nich uprawnienia grupowe, a następnie pojedynczych użytkowników.
- Uprawnienia publiczne dla nowych obiektów w bibliotece (parametr CRTAUT) powinny być takie same, jak uprawnienia dla większości obiektów istniejących w bibliotece.
- Aby ułatwić kontrolę oraz zwiększyć wydajność sprawdzania uprawnień, należy unikać definiowania uprawnień prywatnych, które są mniejsze niż uprawnienia publiczne do obiektu.
- Do grupowania obiektów z tymi samymi wymaganiami ochrony należy używać list autoryzacji. Listy autoryzacji są prostsze do zarządzania niż pojedyncze uprawnienia oraz pomagają podczas odtwarzania informacji o ochronie.

Planowanie zmian poziomu haseł

Zmiana poziomu haseł powinna być odpowiednio zaplanowana. Jeśli zmiany poziomu haseł nie zostaną odpowiednio zaplanowane, wymiana danych z innymi systemami może się nie powieść lub użytkownicy nie będą mogli wpisać się do systemu. Przed zmianą wartości systemowej QPWDLVL należy zeskładować dane ochrony, uruchamiając komendę SAVSECDTA lub SAVSYS. Jeśli dostępna jest aktualna kopia zapasowa, można zresetować hasła dla wszystkich profili użytkowników w sytuacji, gdy konieczny będzie powrót do niższego poziomu haseł.

Programy wykorzystywane w systemie i w klientach, z którymi system się komunikuje, mogą stwarzać problemy, gdy poziom haseł (wartość systemowa QPWDLVL) jest ustawiony na 2 lub 3. Należy zaktualizować produkty i klientów wysyłających do systemu hasła w postaci zaszyfrowanej (czyli inne niż te, w których użytkownik wpisuje hasło na ekranie wpisywania się), aby obsługiwały nowe reguły szyfrowania haseł dla poziomu QPWDLVL równego 2 lub 3. Wysyłanie zaszyfrowanego hasła nazywa się podstawieniem hasła. Podstawienie hasła zabezpiecza przed przechwyceniem hasła podczas przesyłania go przez sieć. Podstawienia haseł wygenerowane przez starszych klientów, którzy nie obsługują nowego algorytmu dla poziomu QPWDLVL 2 lub 3, nawet jeśli specyficzne znaki są poprawne, nie będą akceptowane. Dotyczy to także dostępu do serwera iSeries do równorzędnego serwera iSeries z użyciem szyfrowania w celu uwierzytelnienia systemów.

Problem jest spowodowany tym, że niektóre produkty (na przykład IBM Toolbox for Java) są dostarczane jako oprogramowanie pośrednie. Produkty firm innych niż IBM wykorzystujące wcześniejszą wersję jednego z tych produktów nie będą pracowały poprawnie, dopóki nie zostaną odbudowane za pomocą zaktualizowanej wersji oprogramowania pośredniego.

Dlatego właśnie przed zmianą wartości systemowej QPWDLVL konieczne jest ostrożne planowanie.

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 0 na 1

Poziom hasła 1 umożliwia systemowi, który nie musi komunikować się z produktem Windows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer), wyeliminowanie haseł produktu NetServer z systemu. Eliminacja zbędnych zaszyfrowanych haseł z systemu zwiększa ogólne bezpieczeństwo systemu.

Na poziomie QPWDLVL 1 wszystkie bieżące (sprzed wersji V5R1) podstawienia haseł i mechanizmy uwierzytelniania będą nadal działać. Istnieje bardzo niewielkie prawdopodobieństwo włamania, z wyjątkiem funkcji/usług wymagających hasła NetServer.

Funkcje/usługi wymagające hasła NetServer:

- iSeries Support for Windows Network Neighborhood, Windows 95/98/ME edition, (NetServer)

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 0 lub 1 na 2

Poziom haseł 2 oznacza użycie haseł z rozróżnianiem wielkości liter, o długości do 128 znaków (jedno lub kilka słów); powrót do poziomu QPWDLVL 0 lub 1 jest możliwy.

Niezależnie od poziomu haseł w systemie, hasła dla 2 i 3 poziomu są tworzone przy każdej zmianie hasła i za każdym razem, gdy użytkownik wpisuje się do systemu. Tworzenie haseł dla poziomów 2 i 3 w systemie, który jest na poziomie 0 lub 1, pomaga w przygotowaniu zmiany poziomu haseł na 2 lub 3.

Przed zmianą poziomu hasła na QPWDLVL 2 administrator systemu powinien użyć komendy PRTUSRPRF TYPE(*PWDLVL) w celu zlokalizowania wszystkich profili użytkowników, których hasła nie mogą być użyte na drugim poziomie haseł. W zależności od znalezionych profili, administrator może użyć jednego z następujących mechanizmów, aby hasło poziomu 2 i 3 zostało dodane do profili.

- Zmienić hasło profilu za pomocą komendy CHGUSRPRF lub CHGPWD, albo za pomocą funkcji API QSYCHGPW. Spowoduje to zmianę hasła użytecznego na poziomach 0 i 1. System utworzy także dwa odpowiednie hasła użyteczne na poziomach 2 i 3 (z rozróżnianiem wielkości liter). Zostaną także utworzone dwie wersje hasła do użycia na poziomach 2 i 3: w całości małymi i w całości wielkimi literami.

  Na przykład zmiana hasła na C4D2RB4Y spowoduje wygenerowanie haseł C4D2RB4Y i c4d2rb4y dla poziomu 2.
- Wpisać się do systemu metodą wyświetlającą hasła w postaci niezaszyfrowanej (bez podstawienia). Jeśli hasło jest poprawne, a profil użytkownika nie ma hasła użytecznego na poziomach 2 i 3, system utworzy dwa odpowiednie hasła użyteczne na poziomach 2 i 3 (z rozróżnianiem wielkości liter). Zostaną także utworzone dwie wersje hasła do użycia na poziomach 2 i 3: w całości małymi i w całości wielkimi literami.

Brak hasła użytecznego na poziomie 2 lub 3 może być problemem w sytuacji, gdy profil użytkownika nie ma hasła użytecznego na poziomach 0 i 1, albo też gdy próbuje wpisać się za pomocą produktu używającego podstawiania haseł. W takich sytuacjach, po zmianie poziomu haseł na 2 użytkownik nie będzie w stanie wpisać się do systemu.

Jeśli profil użytkownika nie ma hasła użytecznego na poziomach 2 i 3, ale ma hasło użyteczne na poziomach 0 i 1, to po wpisaniu się tego użytkownika za pomocą produktu wysyłającego hasła w postaci niezaszyfrowanej system uwierzytelnia użytkownika z użyciem hasła na poziomie 0 i tworzy dwa hasła dla poziomu 2 (w sposób opisany powyżej) dla tego profilu użytkownika. Następnie uwierzytelnianie będzie odbywało się z użyciem haseł dla poziomu 2.

Żaden klient ani usługa używająca podstawiania haseł nie będzie poprawnie działała na poziomie QPWDLVL 2, jeśli nie została zaktualizowana pod kątem użycia nowych reguł. Administrator powinien sprawdzić, czy wymagana jest aktualizacja klientów/usług.

Klienci/usługi używające podstawiania haseł to między innymi:

- TELNET
- iSeries Access
- iSeries Host Servers
- QFileSrv.400
- Obsługa drukowania iSeries NetServer
- DDM
- DRDA
- SNA LU6.2

Przed zmianą poziomu haseł na QPWDLVL 2 zaleca się zeskładowanie danych ochrony. Ułatwi to późniejsze przejście do poziomu QPWDLVL 0 lub 1, jeśli będzie to konieczne.

Zaleca się także, aby inne wartości systemowe dotyczące haseł, takie jak QPWDMINLEN i QPWDMAXLEN, nie były zmieniane, dopóki poziom QPWDLVL 2 nie zostanie przetestowany. W razie potrzeby ułatwi to powrót do poziomu QPWDLVL 1 lub 0. Jednakże, aby system zezwolił na zmianę poziomu QPWDLVL na 2, wartość systemowa QPWDVLDPGM musi być równa *REGFAC lub *NONE. Dlatego, jeśli korzysta się z programu sprawdzającego hasła, może zaistnieć potrzeba napisania nowego, który za pomocą komendy ADDEXITPGM zostanie zarejestrowany dla punktu wyjścia QIBM_QSY_VLD_PASSWRD.

Hasła NetServer są wciąż obsługiwane na poziomie QPWDLVL 2, więc dowolne funkcje/usługi wymagające hasła NetServer powinny wciąż poprawnie działać.

Gdy administrator jest zadowolony z działania systemu na poziomie QPWDLVL 2, może zacząć zmieniać odpowiednie wartości systemowe, aby wykorzystać możliwość tworzenia dłuższych haseł. Musi jednak wiedzieć, że ma to następujące konsekwencje:

- Jeśli podane zostanie hasło dłuższe niż 10 znaków, na poziomach 0 i 1 zostaną one usunięte. Dany profil użytkownika nie będzie mógł wpisać się do systemu, jeśli zostanie przywrócony poziom haseł 0 lub 1.
- Jeśli hasło zawiera znaki specjalne lub nie odpowiada regułom tworzenia prostych nazw obiektów (z wyjątkiem rozróżniania wielkości znaków), hasła dla poziomów 0 i 1 zostaną usunięte.
- Jeśli zostaną podane hasła dłuższe niż 14 znaków, hasło NetServer dla profilu użytkownika zostanie usunięte.
- Wartości systemowe hasła są stosowane tylko do wartości 2 poziomu nowego hasła i nie dotyczą generowanego przez system hasła poziomu 0 lub wartości haseł NetServer (jeśli są generowane).

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 2 na 3

Gdy system przez jakiś czas pracuje na poziomie haseł (QPWDLVL) równym 2, administrator może rozważyć zmianę poziomu QPWDLVL na 3 w celu dalszego zwiększenia bezpieczeństwa haseł.

Na poziomie QPWDLVL 3 wszystkie hasła NetServer są usuwane, więc system nie powinien być przenoszony na poziom QPWDLVL 3, dopóki nie ma potrzeby użycia haseł NetServer.

Na poziomie (QPWDLVL) równym 3 wszystkie hasła z poziomu 0 i 1 są usuwane. Administrator może użyć komend DSPAUTUSR lub PRTUSRPRF w celu znalezienia profili użytkowników, którzy nie mają haseł dla poziomu 2 lub 3.

Zmiana na niższy poziom haseł

Mimo iż powrót do niższej wartości QPWDLVL jest możliwy, z założenia jest on utrudniony. W zasadzie należy przyjąć, że zwiększenie wartości QPWDLVL jest nieodwracalne. Może jednak zaistnieć potrzeba przywrócenia poprzedniej wartości QPWDLVL.

Poniższe sekcje opisują czynności wymagane przy przejściu na niższy poziom haseł.

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 3 na 2

Zmiana ta jest względnie łatwa. Po ustawieniu poziomu QPWDLVL 2 administrator musi określić, czy jakikolwiek z profili użytkowników musi zawierać hasła NetServer lub hasła poziomu 0 lub 1, i jeśli tak, musi zmienić hasła profili użytkowników na dozwoloną wartość.

Ponadto może być konieczna zmiana wartości systemowej hasła na wartości zgodne z hasłami NetServer i hasłami poziomu 1 lub 2, jeśli te hasła są potrzebne.

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 3 na 1 lub 0

Ze względu na duże ryzyko wystąpienia problemów z systemem (na przykład brak możliwości wpisania się do systemu przez kogokolwiek z powodu usunięcia wszystkich haseł dla poziomu 0 i 1), zmiana ta nie jest możliwa w sposób bezpośredni. Aby zmienić poziom QPWDLVL 3 na 1 lub 0, należy najpierw zmienić poziom QPWDLVL na 2.

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 2 na 1

Przed zmianą poziomu QPWDLVL na wartość 1 administrator powinien użyć komendy DSPAUTUSR lub PRTUSRPRF TYPE(*PWDINFO) w celu zlokalizowania profili użytkowników, którzy nie mają haseł poziomu 0 lub 1. Jeśli profil użytkownika będzie wymagał hasła po zmianie poziomu QPWDLVL, administrator musi utworzyć dla tego profilu hasło dla poziomu 0 i 1 w jeden z poniższych sposobów:

- Zmienić hasło profilu za pomocą komendy CHGUSRPRF lub CHGPWD, albo za pomocą funkcji API QSYCHGPW. Spowoduje to zmianę hasła użytecznego na poziomach 2 i 3. System utworzy także odpowiednie hasło użyteczne na poziomach 0 i 1 (w całości wielkimi literami). System może utworzyć hasła dla poziomów 0 i 1 tylko wtedy, gdy:
  - długość hasła ma do 10 znaków;
  - hasło może zostać przekształcone do wielkich liter A-Z oraz znaków 0-9, @, #, $ i znaku podkreślenia w standardzie EBCDIC;
  - hasło nie zaczyna się od cyfry ani znaku podkreślenia.

  Na przykład zmiana hasła na RainyDay spowoduje wygenerowanie hasła RAINYDAY dla poziomów 0 i 1. Natomiast zmiana hasła na Rainy Days In April spowoduje usunięcie hasła dla poziomu 0 i 1, ponieważ podane hasło jest za długie i zawiera spacje.

  Jeśli nie można utworzyć hasła dla poziomu 0 i 1, nie zostanie wygenerowany żaden komunikat.
- Wpisać się do systemu metodą wyświetlającą hasła w postaci niezaszyfrowanej (bez podstawienia). Jeśli hasło jest poprawne, a profil użytkownika nie ma hasła użytecznego na poziomach 0 i 1, system utworzy odpowiednie hasło użyteczne na poziomach 0 i 1 (w całości wielkimi literami). Jest to możliwe tylko wtedy, gdy zostaną spełnione opisane wyżej warunki.

Administrator może następnie zmienić poziom QPWDLVL na 1. Wszystkie hasła NetServer zostaną usunięte, gdy zmiana na poziom QPWDLVL 1 zostanie wprowadzona (przy następnym IPL).

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 2 na 0

Uwagi są takie same, jak w przypadku zmiany wartości systemowej QPWDLVL z 2 na 1, z tym że mimo wprowadzenia zmian wszystkie hasła NetServer są zachowywane.

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 1 na 0

Po zmianie poziomu QPWDLVL na wartość 0 administrator powinien użyć komendy DSPAUTUSR lub PRTUSRPRF w celu zlokalizowania profili użytkowników, którzy nie mają hasła NetServer. Jeśli profil użytkownika wymaga hasła NetServer, może ono zostać utworzone przez zmianę hasła użytkownika lub wpisanie się przy użyciu mechanizmu wyświetlającego hasło w postaci jawnego tekstu.

Następnie administrator może zmienić poziom QPWDLVL na 0.

Planowanie bibliotek

Na sposób grupowania informacji aplikacji w biblioteki oraz na zarządzanie bibliotekami wpływ ma wiele czynników. Ten temat zwraca uwagę na niektóre zagadnienia związane z ochroną, a powiązane z projektowaniem bibliotek.

Aby uzyskać dostęp do obiektu, użytkownik potrzebuje uprawnień do samego obiektu oraz do biblioteki zawierającej dany obiekt. Dostęp do obiektu można ograniczyć przez ograniczenie dostępu do samego obiektu, biblioteki zawierającej obiekt lub obu równocześnie.

Biblioteka jest podobna do katalogu, w którym można przechowywać obiekty. Uprawnienia *USE do biblioteki umożliwiają użytkownikowi korzystanie z katalogu, w celu odnalezienia obiektów w bibliotece. Uprawnienia do samego obiektu określają, *w jaki sposób* użytkownik może korzystać z obiektu. Uprawnienia *USE do biblioteki są wystarczające do wykonywania większości operacji na obiektach znajdujących się w bibliotece. Więcej informacji dotyczących powiązań między uprawnieniami do biblioteki i do obiektu zawiera sekcja “Ochrona biblioteki” na stronie 116.

Używanie uprawnień publicznych do obiektów oraz ograniczanie dostępu do bibliotek może być prostą i efektywną techniką ochrony. Umieszczenie programów i obiektów aplikacji w różnych bibliotekach także może uprościć planowanie ochrony. Jest to istotne zwłaszcza wtedy, gdy zbiory są współużytkowane są przez więcej niż jedną aplikację. Aby kontrolować, kto może wykonywać funkcje aplikacji, można użyć uprawnień do bibliotek zawierających programy.

Poniżej przedstawiono dwa przykłady korzystania z ochrony biblioteki dla aplikacji przedsiębiorstwa JKL Toy Company. (Rys. 33 na stronie 199 przedstawia diagram aplikacji.)

- Informacje w bibliotece KONTRAKTY uważane są za poufne. Uprawnienie publiczne dla wszystkich obiektów w bibliotece jest wystarczające do użycia funkcji aplikacji Pricing and Contracts (*CHANGE). Uprawnienia publiczne do samej biblioteki CONTRACTS mają wartość *EXCLUDE. Tylko użytkownicy lub grupy uprawnieni do korzystania z aplikacji Kontrakty i wycena mają nadawane uprawnienia *USE do biblioteki.
- JKL Toy Company jest małym przedsiębiorstwem o nierestrykcyjnym podejściu do ochrony, z wyjątkiem informacji o kontraktach i cenach. Wszyscy użytkownicy systemu mogą przeglądać informacje o klientach oraz zapasach, chociaż zmieniać je mogą jedynie autoryzowani użytkownicy. Biblioteki CUSTLIB i ITEMLIB, oraz obiekty w tych bibliotekach, mają uprawnienia publiczne *USE. Użytkownicy mogą przeglądać informacje zawarte w tych bibliotekach za pomocą swoich podstawowych aplikacji lub za pomocą programu Query. Biblioteki zawierajace programy mają uprawnienia publiczne *EXCLUDE. Dostęp do programu ICPGMLIB mają jedynie użytkownicy, którzy mogą zmieniać informacje o zapasach. Programy, które zmieniają informacje o zapasach, adoptują uprawnienia właściciela aplikacji (OWNIC), a zatem mają uprawnienia *ALL do zbiorów w bibliotece ITEMLIB.

Ochrona biblioteki jest efektywna, jedynie jeśli zastosowane zostaną następujące reguły:

- biblioteka zawiera obiekty o podobnych wymaganiach ochrony,
- użytkownicy nie mają możliwości dodawania nowych obiektów do zastrzeżonych bibliotek; zmiany w programach w bibliotekach są kontrolowane; to znaczy, że biblioteki aplikacji powinny mieć uprawnienia publiczne *USE lub *EXCLUDE, chyba że użytkownicy muszą tworzyć obiekty bezpośrednio w bibliotece,
- listy bibliotek są kontrolowane.

Planowanie aplikacji pod kątem zapobiegania powstawaniu dużych profili

Z powodu potencjalnego wpływu na wydajność i ochronę, IBM **mocno zaleca** zastosowanie następujących uwag umożliwiających uniknięcie przepełnienia profili:

- Jeden profil nie powinien być właścicielem wszystkich obiektów w systemie.

  Należy utworzyć specjalne profile użytkowników, które będą właścicielami aplikacji. Profile właścicieli, które są przeznaczone dla danej aplikacji, ułatwiają odzyskiwanie aplikacji oraz przenoszenie ich między systemami. Umożliwiają także rozłożenie uprawnień prywatnych między kilka profili, co zwiększa wydajność. Korzystając z kilku profili właścicieli można zapobiec powstaniu zbyt dużych profili, będących właścicielami zbyt wielu obiektów. Profile właścicieli umożliwiają także adoptowanie uprawnień właściciela, zamiast zbyt mocnego profilu, który udostępnia niepotrzebne uprawnienia.
- Unikanie nadawania praw własności profilom dostarczanym przez firmę IBM, takim jak QSECOFR lub QPGMR.

  Te profile są właścicielami dużej liczby obiektów IBM i stają się trudne do zarządzania. Nadawanie praw własności profilom użytkowników IBM powoduje także problemy związane z ochroną, dotyczące przenoszenia aplikacji z

jednego systemu do innego. Aplikacje, których właścicielami są profile użytkownika dostarczone przez firmę IBM, mogą także wpływać na wykonywanie komend, jak na przykład CHKOBJITG i WRKOBJOWN.

- Używanie list autoryzacji do zabezpieczania obiektów.

  Jeśli uprawnienia prywatne do wielu obiektów nadawane są kilku użytkownikom, do zabezpieczenia obiektów należy rozważyć korzystanie z list autoryzacji. Listy autoryzacji powodują powstanie jednej pozycji uprawnień prywatnych do listy autoryzacji w profilu użytkownika, zamiast jednej pozycji uprawnień prywatnych dla każdego obiektu. Dla profilu właściciela obiektu, listy autoryzacji powodują powstanie pozycji uprawnień do obiektu dla każdego użytkownika, któremu nadawane są uprawnienia do listy autoryzacji, a nie pozycji uprawnień do obiektu dla każdego obiektu pomnożonych przez liczbę użytkowników, którym nadawane są uprawnienia prywatne.

Listy bibliotek

Lista bibliotek dla zadania zapewnia elastyczność. Stanowi także ryzyko naruszenia ochrony. To ryzyko jest szczególnie ważne, jeśli używane są uprawnienia publiczne do obiektów, a ochrona biblioteki jest podstawą zabezpieczania informacji. W takim przypadku użytkownik uzyskujący dostęp do biblioteki ma niekontrolowany dostęp do informacji w niej zawartych. Temat “Listy bibliotek” na stronie 187 zawiera omówienie zagadnień dotyczących ochrony związanych z listami bibliotek.

Aby uniknąć ryzyka ochrony związanego z listami bibliotek, w aplikacjach można podać nazwy kwalifikowane. Gdy podana jest zarówno nazwa obiektu, jak i biblioteka, system nie przeszukuje listy bibliotek. Zapobiega to używaniu przez potencjalnego intruza listy bibliotek w celu obejścia ochrony.

Jednak inne wymagania projektów aplikacji mogą uniemożliwiać korzystanie z nazw kwalifikowanych. Jeśli aplikacja opiera się na listach bibliotek, ryzyko naruszenia ochrony może zmniejszyć technika opisana w następnej sekcji.

Kontrolowanie listy bibliotek użytkownika

Elementem strategii ochrony może być upewnienie się przed uruchomieniem zadania, że część użytkownika listy bibliotek ma poprawne pozycje podane w oczekiwanej kolejności. Jedną z metod jest użycie programu CL składującego listę bibliotek użytkownika, odtwarzanie wymaganej listy, a następnie odtwarzanie listy po zakończeniu działania aplikacji. Przedstawiony poniżej program przykładowy wykonuje taką funkcję:

```
          PGM
          DCL      &USRLIBL *CHAR LEN(2750)
          DCL      &CURLIB  *CHAR LEN(10)
          DCL      &ERROR *LGL
          DCL      &CMD *CHAR LEN(2800)
          MONMSG   MSGID(CPF0000)  +
                   EXEC(GOTO SETERROR)
          RTVJOBA  USRLIBL(&USRLIBL) +
                   CURLIB(&CURLIB)
          IF COND(&CURLIB=('*NONE')) +
             THEN(CHGVAR &CURLIB '*CRTDFT  ')
          CHGLIBL  LIBL(QGPL) CURLIB(*CRTDFT)
          /*********************************/
          /*                               */
          /*     Zwykłe przetwarzanie      */
          /*                               */
          /*********************************/
          GOTO     ENDPGM
SETERROR: CHGVAR   &ERROR '1'
ENDPGM:   CHGVAR   &CMD +
                         ('CHGLIBL LIBL+
                         (' *CAT &USRLIBL *CAT')  +
                         CURLIB(' *CAT &CURLIB *TCAT ' )')
                   CALL     QCMDEXC PARM(&CMD 2800)
                   IF       &ERROR SNDPGMMSG MSGID(CPF9898) +
                            MSGF(QCPFMSG) MSGTYPE(*ESCAPE) +
                            MSGDTA('Wystąpił błąd xxxx')
                   ENDPGM
```

Rysunek 34. Program zastępujący i odtwarzający listę bibliotek

Uwagi:

1. Niezależnie od tego, jak program zakończy swoje działanie (normalnie lub niepoprawnie), lista bibliotek jestprzywracana do wersji sprzed wywołania programu, ponieważ obsługa błędu obejmuje odtwarzanie listy bibliotek.
2. Ponieważ komenda CHGLIBL wymaga listy nazw bibliotek, nie może być uruchomiona bezpośrednio. Dlatego komenda RTVJOBA odczytuje biblioteki używane do utworzenia komendy CHGLIBL jako zmienną. Zmienna przekazywana jest jako parametr do funkcji QCMDEXC.
3. Jeśli w trakcie działania programu nastąpi wyjście do niekontrolowanej funkcji (na przykład do programu użytkownika, menu umożliwiającego wprowadzanie komend lub ekranu Wprowadzanie komendy - Command Entry), program powinien zastąpić listę bibliotek na wyjściu, aby zapewnić odpowiednią kontrolę.

Zmienianie systemowej listy bibliotek

Jeśli aplikacja musi dodać pozycje do systemowej części listy bibliotek, można użyć programu CL podobnego do tego przedstawionego na Rys. 34, z następującymi zmianami:

- zamiast komendy RTVJOBA należy użyć komendy Odtworzenie wartości systemowej (Retrieve System Values - RTVSYSVAL), aby pobrać wartość systemową QSYSLIBL,
- do zmiany części systemowej listy bibliotek na wymaganą wartość należy użyć komendy Zmiana systemowej listy bibliotek (Change System Library List - CHGSYSLIBL),
- na końcu programu należy ponownie użyć komendy CHGSYSLIBL, aby odtworzyć systemową część listy bibliotek do jej początkowej wartości,
- Komenda CHGSYSLIBL domyślne uprawnienia publiczne ma ustawione na *EXCLUDE. aby użyć tej komendy w programie, należy wykonać następujące czynności:
  - właścicielowi programu należy nadać uprawnienia *USE do komendy CHGSYSLIBL i użyć uprawnień adoptowanych,
  - użytkownikom uruchamiającym program należy nadać uprawnienia *USE do komendy CHGSYSLIBL.

Opisywanie ochrony biblioteki

Jako projektant aplikacji, użytkownik musi udostępnić administratorowi ochrony informacje dotyczące biblioteki. Administrator ochrony używa tych informacji do zadecydowania, w jaki sposób zabezpieczyć bibliotekę i jej obiekty. Wymagane typowe informacje to:

- wszystkie funkcje aplikacji, które dodają obiekty biblioteki,
- czy podczas działania aplikacji z biblioteki usuwane są jakieś obiekty,
- jaki profil jest właścicielem biblioteki oraz znajdujących się w niej obiektów,
- czy biblioteka powinna być dołączona do list bibliotek.

Rys. 35 udostępnia przykładowy format tych informacji:

Nazwa biblioteki: ITEMLIB

Uprawnienia publiczne do biblioteki: *EXCLUDE

Uprawnienia publiczne do obiektów w bibliotece: *CHANGE

Uprawnienia publiczne do nowych obiektów (CRTAUT): *CHANGE

Właściciel biblioteki: OWNIC

Dołączyć do list bibliotek? Nie. Biblioteka dodawana jest do listy bibliotek przez program początkowy lub początkowy program zapytania.

Lista funkcji wymagających uprawnień *ADD do biblioteki:

Podczas zwykłego działania aplikacji do biblioteki nie są dodawane żadne obiekty. Lista obiektów wymagających uprawnień *OBJMGT lub *OBJEXIST oraz jakie funkcje wymagają tych uprawnień:

Na koniec miesiąca usuwana jest zawartość wszystkich zbiorów roboczych, których nazwy rozpoczynają się od znaków ICWRK. Wymaga to uprawnień *OBJMGT.

Rysunek 35. Format do opisywania ochrony biblioteki

Planowanie menu

Menu to dobra metoda zapewniania kontrolowanego dostępu do systemu. Menu można użyć do ograniczenia użytkowników do ściśle kontrolowanych funkcji, podając w ich profilach ograniczenie możliwości oraz menu początkowe.

Aby jako narzędzia kontroli dostępu użyć menu, podczas ich projektowania należy zastosować się do następujących wskazówek:

- wiersza komend lub menu nie należy udostępniać użytkownikom z ograniczonym dostępem,
- należy unikać funkcji o różnych wymaganiach ochrony w tym samym menu; na przykład jeśli niektórzy użytkownicy aplikacji mają możliwość jedynie przeglądania informacji, a nie ich zmieniania, należy udostępnić menu, które ma jedynie opcje wyświetlania i drukowania,
- należy upewnić się, że zestaw menu udostępnia wszystkie wymagane połączenia między menu, tak aby użytkownik nie potrzebował wiersza komend,
- należy zapewnić dostęp do kilku funkcji systemowych, takich jak przeglądanie zbiorów wydruku; menu systemowe ASSIST daje taką możliwość oraz może być zdefiniowane w profilu użytkownika jako program obsługi klawisza ATTN; jeśli profil użytkownika ma klasę *USER oraz ograniczone możliwości, nie może przeglądać wydruków lub zadań innych użytkowników,
- z poziomu menu należy zapewnić dostęp do narzędzi wspomagania podejmowania decyzji; przykład tego opisuje temat “Używanie uprawnień adoptowanych w projekcie menu” na stronie 208,
- należy rozważyć kontrolowanie dostępu do menu żądania systemowego (Request) lub niektórych opcji tego menu; więcej informacji na ten temat zawiera sekcja “Menu żądania systemowego (System Request)” na stronie 212,

- w przypadku użytkowników uprawnionych do uruchamiania tylko pojedynczej funkcji, należy całkowicie zabronić dostępu do menu, a w profilu użytkownika podać program początkowy; jako menu początkowe należy podać wartość *SIGNOFF.

W przedsiębiorstwie JKL Toy Company wszyscy użytkownicy widzą menu zapytań umożliwiające dostęp do większości zbiorów. W przypadku użytkowników, którzy nie mogą zmieniać informacji, jest to menu początkowe. Opcja wyjścia z menu wypisuje użytkownika. W przypadku pozostałych użytkowników, to menu wywoływane jest przez opcję zapytania z menu aplikacji. Naciskając klawisz F12 (Powrót), użytkownik wraca do wywołującego menu. Ponieważ dla bibliotek programu używana jest ochrona biblioteki, to menu oraz program je wywołujący przechowywane są w bibliotece QGPL:

```
 INQMENU       Menu zapytania

         1. Opisy elementów
         2. Bilansowanie elementów
         3. Informacje o klientach
         4. Zapytanie
         5. Biuro

Wpisz opcję ==>
F1=Pomoc  F12=Powrót
```

Rysunek 36. Przykładowe menu zapytania

Używanie uprawnień adoptowanych w projekcie menu

Dostępność narzędzia do wspomagania podejmowania decyzji, takiego jak Query/400, stanowi wyzwanie przy projektowaniu ochrony. Użytkownicy powinni mieć możliwość przeglądania informacji w zbiorach za pomocą narzędzia zapytań, ale prawdopodobnie te zbiory powinny być zmieniane jedynie przez przetestowane aplikacje.

W definicjach ochrony zasobów nie ma metody zapewniającej różne uprawnienia do zbioru dla użytkownika w różnych warunkach. Jednak użycie uprawnień adoptowanych umożliwia takie zdefiniowanie uprawnień, aby spełniały różne wymagania.

Uwaga: Sekcja “Obiekty, które adoptują uprawnienia właściciela” na stronie 128 opisuje sposób działania uprawnień adoptowanych. Natomiast sekcja “Schemat blokowy 8: Jak sprawdzane są uprawnienia adoptowane” na stronie 162 opisuje, w jaki sposób system sprawdza uprawnienia adoptowane.

Rys. 37 pokazuje przykładowe menu początkowe, które korzysta z uprawnień adoptowanych w celu zapewnienia kontrolowanego dostępu do zbiorów podczas korzystania z narzędzi zapytań:

```
MENU1         Menu początkowe

        1. Kontrola zapasów    (ICSTART)
        2. Zamówienia klientów (COSTART)
        3. Zapytania           (QRYSTART)
        4. Biuro               (OFCSTART)

(brak wiersza komend)
```

Rysunek 37. Przykładowe menu początkowe

Programy uruchamiające aplikacje (ICSTART i COSTART) adoptują uprawnienia profilu, który jest właścicielem obiektów aplikacji. Programy dodają do listy bibliotek biblioteki aplikacji oraz wyświetlają menu początkowe aplikacji. Poniżej przedstawiono przykład programu Kontroli zapasów (ICSTART).

```
PGM
ADDLIBLE ITEMLIB
ADDLIBLE ICPGMLIB
GO ICMENU
RMVLIBLE ITEMLIB
RMVLIBLE ICPGMLIB
ENDPGM
```

Rysunek 38. Przykład programu inicjującego aplikację

Program uruchamiający program Query (QRYSTART) adoptuje uprawnienia profilu (QRYUSR) udostępnianego w celu umożliwienia dostępu do zbiorów za pomocą zapytań. Rys. 39 pokazuje program QRYSTART:

```
PGM
ADDLIBLE ITEMLIB
ADDLIBLE CUSTLIB
STRQRYRMVLIBLE ITEMLIB
RMVLIBLE CUSTLIB
ENDPGM
```

Rysunek 39. Przykładowe zapytanie z uprawnieniami adoptowanymi

System menu korzysta z trzech typów profili użytkowników, które opisuje Tabela 119. Natomiast Tabela 120 opisuje obiekty używane przez system menu.

Tabela 119. Profile użytkowników dla systemu menu

Typ profilu	Opis	Hasło	Ograniczenie możliwości	Uprawnienia specjalne	Menu początkowe
Właściciel aplikacji	Jest właścicielem wszystkich obiektów aplikacji i ma uprawnienia *ALL. OWNIC jest właścicielem aplikacji Kontrola zapasów.	*NONE	Nie dotyczy	W miarę potrzeb aplikacji	Nie dotyczy
Użytkownik aplikacji [1]	Przykładowy profil dla każdego, kto korzysta z systemu menu	Tak	*YES	Brak	MENU1
Profil zapytania	Używany w celu zapewnienia dostępu do bibliotek dla zapytań	*NONE	Nie dotyczy	Brak	Nie dotyczy

[1] Biblioteka bieżąca podana w profilu użytkownika aplikacji używana jest do przechowywania utworzonych zapytań. Programem obsługi klawisza ATTN jest program *ASSIST, dający użytkownikowi dostęp do podstawowych funkcji systemowych.

Tabela 120. Obiekty używane przez system menu

Nazwa obiektu	Właściciel	Uprawnienia publiczne	Uprawnienia prywatne	Informacje dodatkowe
MENU1 w bibliotece QGPL	Patrz uwagi	*EXCLUDE	Uprawnienia *USE dla wszystkich użytkowników, którzy są uprawnieni do używania menu	W bibliotece QGPL, ponieważ użytkownicy nie mają uprawnień do bibliotek aplikacji
Program ICSTART w bibliotece QGPL	OWNIC	*EXCLUDE	Uprawnienia *USE dla użytkowników uprawnionych do aplikacji Kontrola zapasów	Utworzony z parametrem USRPRF(*OWNER), aby adoptować uprawnienia właściciela OWNIC
Program QRYSTART w bibliotece QGPL	QRYUSR	*EXCLUDE	Uprawnienia *USE dla użytkowników uprawnionych do tworzenia i uruchamiania zapytań	Utworzony z parametrem USRPRF(*OWNER), aby adoptować uprawnienia użytkownika QRYUSR
ITEMLIB	OWNIC	*EXCLUDE	Użytkownik QRYUSR ma uprawnienia *USE	
ICPGMLIB	OWNIC	*EXCLUDE		
Zbiory dostępne dla programu Query w bibliotece ITEMLIB	OWNIC	*USE		
Zbiory niedostępne dla programu Query w bibliotece ITEMLIB	OWNIC	*EXCLUDE		

Tabela 120. Obiekty używane przez system menu (kontynuacja)

Nazwa obiektu	Właściciel	Uprawnienia publiczne	Uprawnienia prywatne	Informacje dodatkowe
Programy w bibliotece ICPGMLIB	OWNIC	*USE		

Uwaga: Dla obiektów używanych przez wiele aplikacji można utworzyć specjalny profil właściciela.

Gdy UŻYTKOWNIK_A wybiera z MENU1 opcję 1 (Kontrola zapasów), uruchamiany jest program ICSTART. Program adoptuje uprawnienia właściciela OWNIC, nadające uprawnienia *ALL do obiektów aplikacji Kontroli zapasów w bibliotece ITEMLIB oraz programów w bibliotece ICPGMLIB. A zatem UŻYTKOWNIK_A, podczas korzystania z opcji z menu ICMENU, uprawniony jest do dokonywania zmian w zbiorach aplikacji Kontrola zapasów.

Gdy UŻYTKOWNIK_A wychodzi z menu ICMENU i powraca do MENU1, z jego listy bibliotek usuwane są biblioteki ITEMLIB i ICPGMLIB, a program ICSTART usuwany jest ze stosu programów. UŻYTKOWNIK_A nie działa już z uprawnieniami adoptowanymi.

Gdy UŻYTKOWNIK_A wybiera z MENU1 opcję 3 (Zapytanie), uruchamiany jest program QRYSTART. Program adoptuje uprawnienia użytkownika QRYUSR, nadające uprawnienia *USE do biblioteki ITEMLIB. Uprawnienia publiczne do zbiorów biblioteki ITEMLIB określają, do których zbiorów UŻYTKOWNIK_A może wysyłać zapytania.

Ta technika przynosi korzyści z minimalizowania liczby uprawnień prywatnych oraz zapewnia dobrą wydajność podczas sprawdzania uprawnień:

- obiekty w bibliotekach aplikacji nie mają uprawnień prywatnych; dla niektórych funkcji wystarczające są uprawnienia publiczne; jeśli uprawnienia publiczne nie są wystarczające, używane są uprawnienia właściciela; kroki sprawdzania uprawnień opisuje sekcja “Przypadek 8: Uprawnienia adoptowane bez uprawnień prywatnych” na stronie 171,
- dostęp do zbiorów dla zapytań zapewniają uprawnienia publiczne do tych zbiorów; profil QRYUSR jest wyraźnie autoryzowany jedynie do biblioteki ITEMLIB,
- domyślnie, wszystkie tworzone programy zapytań umieszczane są w bibliotece bieżącej użytkownika; biblioteka bieżąca powinna należeć do użytkownika, który powinien mieć do niej uprawnienia *ALL,
- pojedynczy użytkownicy muszą mieć uprawnienia tylko do opcji MENU1, ICSTART i QRYSTART.

Podczas korzystania z tej techniki należy rozważyć ryzyko oraz podjąć środki ostrożności:

- UŻYTKOWNIK_A, z poziomu menu ICMENU, ma uprawnienia *ALL do wszystkich obiektów aplikacji Kontrola zapasów. Należy uprawnić się, że menu nie umożliwia dostępu do wiersza komend lub niechcianych funkcji usuwania i aktualizowania.
- Wiele narzędzi wspomagania podejmowania decyzji umożliwia dostęp do wiersza komend. Aby zapobiec wykonywaniu nieautoryzowanych funkcji, profil QRYUSR powinien być użytkownikiem z ograniczonymi możliwościami bez uprawnień specjalnych.

Ignorowanie uprawnień adoptowanych

Sekcja Używanie uprawnień adoptowanych w projekcie menu opisuje technikę udostępniania możliwości tworzenia zapytań bez możliwości wprowadzania do zbiorów aplikacji niekontrolowanych zmian. Ta technika wymaga od użytkownika powrotu do menu początkowego, przed uruchomieniem zapytań. Jeśli ma być zapewniona wygoda uruchamiania zapytań z menu aplikacji, a także z menu początkowego, można tak ustawić program QRYSTART, aby ignorował uprawnienia adoptowane.

Uwaga: Sekcja “Programy, które ignorują uprawnienia adoptowane” na stronie 131 udostępnia więcej informacji dotyczących ignorowania uprawnień adoptowanych. “Schemat blokowy 8: Jak sprawdzane są uprawnienia adoptowane” na stronie 162 opisuje sposób sprawdzania przez system uprawnień adoptowanych.

Rys. 40 na stronie 211 opisuje menu aplikacji, które zawiera program QRYSTART:

```
ICMENU       Menu Kontroli zapasów

             1. Dochody (ICPGM1)
             2. Wpływy   (ICPGM2)
             3. Zakupy    (ICPGM3)
             4. Zapytanie  (QRYSTART)

(brak wiersza komend)
```

Rysunek 40. Przykładowe menu aplikacji z programem Query

Informacje o uprawnieniach dla programu QRYSTART są takie same, jak to pokazuje Tabela 120 na stronie 209. Program tworzony jest z parametrem użycia uprawnień adoptowanych (USEADPAUT) ustawionym na *NO, aby ignorować uprawnienia adoptowane poprzednich programów ze stosu.

Poniżej przedstawiono porównania stosów programów, gdy UŻYTKOWNIK_A wybiera zapytanie z MENU1 (patrz Rys. 37 na stronie 208) oraz z menu ICMENU:

Stos programów, gdy zapytanie wybierane jest z menu MENU1

MENU1 (brak uprawnień adoptowanych)

QRYSTART (uprawnienia adoptowane od QRYUSR)

Stos programów gdy zapytanie wybierane jest z menu ICMENU

MENU1 (brak uprawnień adoptowanych)

ICMENU (uprawnienia adoptowane od OWNIC)

QRYSTART (uprawnienia adoptowane od QRYUSR)

Podanie dla programu QRYSTART parametru USEADPAUT(*NO) powoduje, że uprawnienia poprzednich programów ze stosu nie są używane. Umożliwia to UŻYTKOWNIKOWI_A uruchamianie zapytania z menu ICMENU bez możliwości zmiany lub usuwania zbiorów, ponieważ uprawnienia właściciela OWNIC nie są używane przez program QRYSTART.

Gdy UŻYTKOWNIK_A kończy działanie zapytania i powraca do menu ICMENU, uprawnienia adoptowane ponownie stają się aktywne. Uprawnienia adoptowane ignorowane są tak długo, jak długo aktywny jest program QRYSTART.

Jeśli uprawnienia publiczne do programu QRYSTART mają wartość *USE, parametr USEADPAUT(*NO) można podać jako środek ostrożności. Zapobiega to niepożądanym działaniom użytkowników z uprawnieniami adoptowanymi podczas wywoływania programu QRYSTART i wykonywaniu nieautoryzowanych funkcji.

Menu zapytania (Rys. 36 na stronie 208) w przedsiębiorstwie JKL Toy Company także korzysta z tej techniki, ponieważ może być wywoływane z menu w różnych bibliotekach aplikacji. Adoptuje uprawnienia użytkownika QRYUSR i ignoruje inne uprawnienia ze stosu programów.

Opisywanie ochrony menu

Jako projektant aplikacji, użytkownik musi udostępnić administratorowi ochrony informacje dotyczące menu. Administrator ochrony używa tych informacji do zadecydowania, kto powinien mieć dostęp od menu oraz jakie uprawnienia są wymagane. Wymagane typowe informacje to:

- czy jakieś opcje menu wymagają uprawnień specjalnych, takich jak *SAVSYS lub *JOBCTL,
- czy opcje menu wywołują programy, które adoptują uprawnienia,
- jakie uprawnienia do obiektów wymagane są dla każdej opcji menu; użytkownik powinien przedstawić tylko te uprawnienia, które są wyższe niż zwykłe uprawnienia publiczne.

Rys. 41 przedstawia przykładowy format tych informacji.

Nazwa menu: MENU1 Biblioteka: QGPLNumer opcji: 3 Opis: Zapytanie

Wywoływany program: QRYSTART Biblioteka: QGPL

Adoptowane uprawnienia: QRYUSR

Wymagane uprawnienia specjalne: Brak

Wymagane uprawnienia do obiektu: Użytkownicy muszą mieć uprawnienia *USE do programu QRYSTART. Użytkownik QRYUSR musi mieć uprawnienia *USE do bibliotek zawierających zbiory, do których odnoszą się zapytania. Użytkownik QRYUSR lub użytkownik publiczny musi mieć uprawnienia *USE do zbiorów, do których odnoszą się uprawnienia.

Rysunek 41. Format dla wymagań ochrony menu

Menu żądania systemowego (System Request)

Użytkownik może używać funkcji żądania systemowego w celu zawieszenia bieżącego zadania i wyświetlenia menu żądania systemowego (System Request Menu). Menu żądania systemowego umożliwia użytkownikowi wysyłanie i wyświetlanie komunikatów, przejście do drugiego zadania lub zakończenie bieżącego zadania.

Gdy system jest dostarczany, uprawnienia publiczne do menu żądania systemowego ustawione są na *USE. Najprostszym sposobem zabezpieczenia przed dostępem do tego menu jest ograniczenie uprawnień do panelu grupowego QGMNSYSR:

- Aby niektórzy użytkownicy nie mogli widzieć menu żądania systemowego, należy dla nich podać uprawnienia *EXCLUDE:

```
GRTOBJAUT OBJ(QSYS/QGMNSYSR) +
          OBJTYPE(*PNLGRP)   +
          USER(USERA) AUT(*EXCLUDE)
```

- Aby większość użytkowników nie mogła widzieć menu żądania systemowego, należy odwołać uprawnienia publiczne i nadać uprawnienia *USE niektórym użytkownikom:

```
RVKOBJAUT OBJ(QSYS/QGMNSYSR) +
          OBJTYPE(*PNLGRP) +
          USER(*PUBLIC) AUT(*ALL)
GRTOBJAUT OBJ(QSYS/QGMNSYSR) +
          OBJTYPE(*PNLGRP)   +
          USER(USERA) AUT(*USE)
```

| Niektóre bieżące komendy używane dla menu żądania systemowego pochodzą z komunikatu CPX2313 ze zbioru
| komunikatów QCPFMSG. Począwszy od wersji V5R3, te komendy kwalifikowane są bibliotekami z wartościami
| *NLVLIBL i *SYSTEM z komunikatu CPX2373. Ktoś mógłby użyć komendy Przesłonięcie zbioru komunikatów
| (Override Message File - OVRMSGF) w celu zmiany komend, które używają opcji menu żądania systemowego. Aby
| zapobiec przesłanianiu komend używanych przez opcje menu żądania systemowego, do komendy OVRMSGF należy
| nadać uprawnienia *EXCLUDE:

```
| GRTOBJAUT OBJ(QSYS/OVRMSGF) OBJTYPE(*CMD) USER(*PUBLIC) AUT(*EXCLUDE)
```

Ograniczając uprawnienia do pewnych komend można zapobiec wybieraniu przez użytkowników niekrórych opcji z menu żądania systemowego. Tabela 121 pokazuje komendy związane z opcjami menu:

Tabela 121. Opcje i komendy dla menu żądania systemowego

Opcja	Komenda
1	Transfer zadania alternatywnego (Transfer Secondary Job - TFRSECJOB)
2	Zakończenie żądania (End Request - ENDRQS)
3	Wyświetlenie zadania (Display Job - DSPJOB)
4	Wyświetlenie komunikatów (Display Message - DSPMSG)

Tabela 121. Opcje i komendy dla menu żądania systemowego (kontynuacja)

Opcja	Komenda
5	Wysłanie komunikatu (Send Message - SNDMSG)
6	Wyświetlenie komunikatów (Display Message - DSPMSG)
7	Wyświetlenie użytkownika stacji roboczej (Display Workstation User - DSPWSUSR)
10	Uruchomienie żądania systemowego na poprzednim systemie (Start System Request at Previous System - TFRPASTHR). (Patrz uwaga poniżej.)
11	Transfer do poprzedniego systemu (Transfer to previous system - TFRPASTHR). (Patrz uwaga poniżej.)
12	Wyświetlenie opcji emulacji 3270 (patrz uwaga poniżej.)
13	Uruchomienie żądania systemowego na systemie początkowym (Start System Request at Home System - TFRPASTHR). (Patrz uwaga poniżej.)
14	Transfer do systemu początkowego (Transfer to Home System - TFRPASTHR). (Patrz uwaga poniżej.)
15	Transfer do systemu końcowego (Transfer to End System - TFRPASTHR). (Patrz uwaga poniżej.)
50	Zakończenie żądania w systemie zdalnym (End Request on Remote System - ENDRDBRQS). (Patrz uwaga poniżej.)
80	Odłączenie zadania (Disconnect Job - DSCJOB)
90	Wypisanie się (Sign-Off - SIGNOFF)

Uwagi:

1. Opcje 10, 11, 13, 14 i 15 wyświetlane są jedynie wtedy, gdy stacja graficzna tranzytu została uruchomiona za pomocą komendy Uruchomienie tranzytu (Start Pass-Through - STRPASTHR). Opcje 10, 13 i 14 wyświetlane są tylko w systemie docelowym.
2. Opcja 12 wyświetlana jest jedynie wtedy, gdy aktywna jest emulacja 3270.
3. Opcja 50 wyświetlana jest tylko wtedy, gdy aktywne są zadania zdalne.
4. Niektóre opcje mają ograniczenia dla środowiska System/36.

Na przykład, aby zabezpieczyć system przed przesyłaniem do alternatywnego zadania interaktywnego, należy odwołać uprawnienia publiczne do komendy Transfer do zadania alterantywnengo (Transfer to Secondary Job - TFRSECJOB) i nadać uprawnienia określonym użytkownikom:

```
RVKOBJAUT OBJ(TFRSECJOB) OBJTYPE(*CMD)
          USER(*PUBLIC) AUT(*ALL)
GRTOBJAUT OBJ(TFRSECJOB) OBJTYPE(*CMD)
          USER(USERA) AUT(*USE)
```

Jeśli użytkownik wybiera opcję, do której nie ma uprawnień, wyświetlany jest komunikat.

Aby zapobiec używaniu przez użytkowników komend z poziomu menu żądania systemowego, ale umożliwić im uruchamianie komend w określonym czasie (na przykład podczas wypisywania się), można utworzyć program CL adoptujący uprawnienia autoryzowanego użytkownika i uruchomić komendę.

Planowanie ochrony komend

Ochrona menu jest dobrą techniką dla użytkowników wymagających aplikacji oraz ograniczonych funkcji systemowych. Niektórzy użytkownicy wymagają bardziej elastycznego środowiska oraz możliwości uruchamiania komend. Gdy system jest dostarczany, możliwość używania komend jest tak skonfigurowana, aby spełniać wymagania ochrony dla większości instalacji. Niektóre komendy mogą być uruchamiane tylko przez szefa ochrony. Inne wymagają uprawnień specjalnych, takich jak *SAVSYS. Większość komend może być używana przez wszystkich użytkowników systemu.

Uprawnienia do komend można tak zmienić, aby spełniały wymagania ochrony. Na przykład można umożliwić pracę z komunikacją większości użytkowników w systemie. Do wszystkich komend pracujących z obiektami komunikacji, takich jak CHGCTLxxx, CHGLINxxx i CHGDEVxxx, uprawnienia publiczne można ustawić na *EXCLUDE.

Jeśli wymagana jest kontrola komend, które mogą być uruchamiane przez użytkowników, można użyć uprawnień do obiektu dla samych komend. Każda komenda w systemie jest obiektem typu *CMD i może być autoryzowana do użytku publicznego lub tylko dla konkretnych użytkowników. Aby uruchomić komendę, użytkownik musi mieć do niej uprawnienia *USE. Dodatek C opisuje wszystkie komendy, do których uprawnienia publiczne mają wartość domyślną równą *EXCLUDE.

Jeśli używana jest biblioteka System/38, komendy dotyczące ochrony należy także ograniczyć dla tej biblioteki. Można także ograniczyć dostęp do całej biblioteki. Jeśli w systemie używana jest jedna lub więcej wersji programu licencjonowanego OS/400 w języku narodowym, należy także ograniczyć komendy w dodatkowych bibliotekach QSYSxxx.

Dodatkowym środkiem ochrony jest zmiana wartości domyślnych niektórych dla komend. Wykonanie tego umożliwia komenda Zmiana wartości domyślnych komendy (Change Command Default - CHGCMDDFT).

Planowanie ochrony zbiorów

Informacje zawarte w zbiorach bazy danych są najczęściej najważniejszymi zasobami systemu. Ochrona zasobów umożliwia kontrolowanie, kto może przeglądać, zmieniać i usuwać informacje ze zbiorów. Jeśli użytkownicy wymagają różnych uprawnień do zbiorów, w zależności od sytuacji, należy używać uprawnień adoptowanych. Sekcja “Używanie uprawnień adoptowanych w projekcie menu” na stronie 208 zawiera przykład użycia tej metody.

W przypadku krytycznych zbiorów w systemie należy zapisać, którzy użytkownicy mają uprawnienia do zbioru. Jeśli używane są uprawnienia grupowe lub listy autoryzacji, należy śledzić użytkowników, którzy otrzymują uprawnienia za pomocą tych metod, a także użytkowników, którzy są bezpośrednio uprawnieni. Jeśli używane są uprawnienia adoptowane, za pomocą komendy Wyświetlenie adopcji programu (Display Program Adopt - DSPPGMADP) można wyświetlić listę programów, które adoptują uprawnienia danego użytkownika.

Do monitorowania aktywności krytycznych zbiorów można użyć także funkcji kronikowania. Chodziaż podstawowym przeznaczeniem kroniki jest odzyskiwanie informacji, może być ona wykorzystywana jako narzędzie ochrony. Kronika zawiera rekord dotyczący użytkownika uzyskującego dostęp do zbioru oraz sposobu, w jaki dostęp został uzyskany. Aby okresowo przeglądać pozycje kroniki, można użyć komendy Wyświetlenie kroniki (Display Journal - DSPJRN).

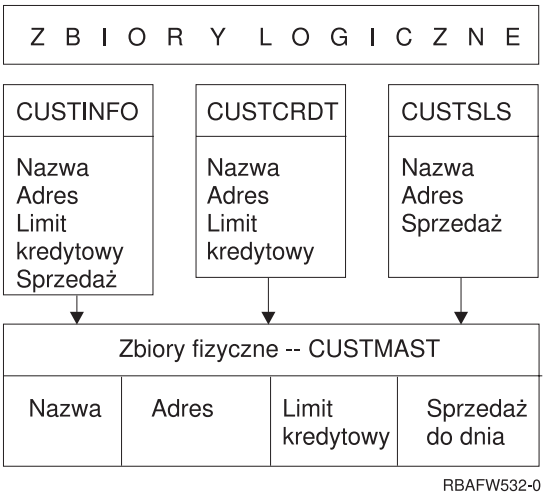
Ochrona zbiorów logicznych

Ochrona zasobów w systemie wspiera opcję zabezpieczania zbioru na poziomie pól. Do zabezpieczania pól lub rekordów w zbiorze można także użyć zbiorów logicznych. Więcej informacji na ten temat zawiera sekcja DB2 Universal Database dla iSeries w Centrum informacyjnym. Więcej informacji na ten temat zawiera sekcja “Informacje wstępne i pokrewne” na stronie xvi.

Zbiór logiczny może być użyty do podania podzbioru *rekordów*, do których użytkownik ma dostęp (za pomocą zbiorów logicznych wybierz/pomiń). Dlatego można zapobiec dostępowi niektórych użytkowników do pewnych typów rekordów. Zbiór logiczny może być użyty do podania podzbioru *pól* w rekordzie, do którego użytkownik może mieć dostęp. Dlatego można zapobiec dostepowi niektórych użytkowników do pewnych pól w rekordach.

Zbiór logiczny nie zawiera żadnych danych. Jest to szczególny rodzaj widoku jednego lub więcej zbiorów fizycznych, które zawierają dane. Zapewnienie dostępu do informacji zdefiniowanych przez zbiór logiczny wymaga uprawnień do zbioru logicznego oraz do związanych z nim zbiorów fizycznych.

Rys. 42 na stronie 215 przedstawia przykład zbioru fizycznego oraz trzech różnych związanych z nim zbiorów logicznych.



Rysunek 42. Korzystanie ze zbiorów logicznych do ochrony

Członkowie działu sprzedaży (profil grupowy DPTSM) uprawnieni są do przeglądania wszystkich pól, ale nie mogą zmieniać limitu kredytowego. Członkowie działu należności (profil grupowy DPTAR) uprawnieni są do przeglądania wszystkich pól, ale nie mogą zmieniać pól sprzedaży. Uprawnienia do zbioru fizycznego wyglądają następująco:

Tabela 122. Przykład zbioru fizycznego: zbiór CUSTMAST

Uprawnienie	**Użytkownicy: *PUBLIC**
Uprawnienia do obiektu	
*OBJOPR	
*OBJMGT	
*OBJEXIST	
*OBJALTER	
*OBJREF	
Uprawnienia do danych	
*READ	X
*ADD	X
*UPD	X
*DLT	X
*EXECUTE	X
*EXCLUDE	

Użytkownicy publiczni powinni mieć uprawnienia do danych; nie powinni jednak mieć uprawnień do działań na obiektach do zbioru fizycznego CUSTMAST. Użytkownicy publiczni nie mogą mieć bezpośredniego dostępu do zbioru CUSTMAST, ponieważ do otwarcia zbioru wymagane są uprawnienia *OBJOPR. Uprawnienia użytkowników publicznych powodują, że uprawnienia do danych są potencjalnie dostępne dla wszystkich użytkowników zbioru logicznego.

Uprawnienia do zbiorów logicznych wyglądają następująco:

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   CUSTINFO      Właściciel . . . . . :   OWNAR
  Biblioteka . . . :   CUSTLIB      Grupa podstawowa . . :   *NONE
Typ obiektu  . . . :   *FILE        Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji . . . . . :   *NONE

                       Uprawnienia
Użytkownik  Grupa      do obiektu
*PUBLIC                *USE
```

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   CUSTCRDT      Właściciel . . . . . :   OWNAR
  Biblioteka . . . :   CUSTLIB      Grupa podstawowa . . :   DPTAR
Typ obiektu  . . . :   *FILE        Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji . . . . . :   *NONE

                       Uprawnienia
Użytkownik  Grupa      do obiektu
DPTAR                  *CHANGE
*PUBLIC                *USE
```

```
                  Wyświetlenie uprawnień dla obiektu
                     (Display Object Authority)
Obiekt . . . . . :   CUSTSLS       Właściciel . . . . . :   OWNSM
  Biblioteka . . . :   CUSTLIB      Grupa podstawowa . . :   DPTSM
Typ obiektu  . . . :   *FILE        Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji . . . . . :   *NONE

                       Uprawnienia
Użytkownik  Grupa      do obiektu
DPTSM                  *CHANGE
*PUBLIC                *USE
```

Aby ten schemat uprawnień mógł działać, ustawienie profilu grupowego, takiego jak DPTSM, jako grupy podstawowej dla zbioru logicznego nie jest konieczne. Jednak użycie uprawnień grupy podstawowej eliminuje wyszukiwanie uprawnień prywatnych dla użytkownika próbującego uzyskać dostęp do zbioru oraz dla grupy użytkownika. Wpływ uprawnień grupy podstawowej na proces sprawdzania uprawnień opisuje sekcja “Przypadek 2: Używanie uprawnień grupy podstawowej” na stronie 167.

Począwszy od wersji V3R1 programu licencjonowanego OS/400 można podawać uprawnienia do danych dla zbiorów logicznych. Podczas instalowania systemu w ramach aktualizacji do wersji V3R1 z wcześniejszych wersji, zbiory logiczne są konwertowane. Podczas pierwszej próby dostępu do zbioru logicznego system nadaje mu wszystkie uprawnienia do danych.

Aby używać zbiorów logicznych narzędzi ochrony, należy wykonać następujące czynności:

- używanym zbiorom fizycznym należy nadać wszystkie uprawnienia do danych,

- należy odwołać uprawnienia *OBJOPR do zbiorów fizycznych; zapobiega to bezpośredniemu dostępowi do zbiorów fizycznych,
- zbiorom logicznych należy nadać odpowiednie uprawnienia do danych; należy odwołać wszystkie uprawnienia, których użytkownik nie potrzebuje,
- do zbiorów logicznych należy nadać uprawnienia *OBJOPR.

Przesłanianie zbiorów

Komendy przesłaniania mogą być używane podczas wykorzystywania przez program innego zbioru o tym samym formacie. Na przykład przyjmijmy, że program w aplikacji Kontrakty i wycena w przedsiębiorstwie JKL Toy Company przed zmianą cen zapisuje informacje o cenach w zbiorze roboczym. Użytkownik mający dostęp do wiersza komend, który chce przejąć poufne informacje, może użyć komendy przesłaniania, aby program zapisywał dane do innego zbioru znajdującego się w bibliotece kontrolowanej przez użytkownika. Używając komend przesłaniania z parametrem SECURE(*YES) przed uruchomieniem programu, można zapewnić, aby program przetwarzał poprawne zbiory.

Ochrona zbiorów a język SQL

Język Structured Query Language (SQL), w celu śledzenia zbiorów bazy danych oraz ich powiązań korzysta ze zbiorów odniesienia. Te zbiory razem są traktowane jako katalog SQL. Uprawnienia publiczne do katalogu SQL to uprawnienia *READ. Oznacza to, że każdy użytkownik mający dostęp do interfejsu SQL może wyświetlić nazwy oraz tekst opisu dla wszystkich zbiorów w systemie. Katalog SQL nie wpływa na zwykłe uprawnienia wymagane przy dostępie do zawartości zbiorów bazy danych.

Podczas używania programu CL adoptującego uprawnienia przy uruchamianiu programu SQL lub Query Manager należy postepować ostrożnie. Oba te programy umożliwiają użytkownikom podanie nazwy zbioru. W ten sposób użytkownik może uzyskać dostęp do dowolnego zbioru, do którego adoptowany profil ma uprawnienia.

Planowanie list autoryzacji

Lista autoryzacji daje następujące korzyści:

- Listy autoryzacji ułatwiają zarządzanie uprawnieniami. Definuje się uprawnienia użytkownika do listy autoryzacji, a nie do pojedynczych obiektów z listy. Jeśli lista autoryzacji zabezpiecza nowy obiekt, użytkownik zyskuje uprawnienia do tego obiektu.
- Do nadania użytkownikowi uprawnień do wszystkich obiektów na liście potrzebna jest jedna operacja.
- Listy autoryzacji zmniejszają liczbę uprawnień prywatnych w systemie. Każdy użytkownik ma uprawnienia prywatne do jednego obiektu - listy autoryzacji. Powoduje to nadanie użytkownikowi uprawnień do wszystkich obiektów z listy. Zmniejszenie liczby uprawnień prywatnych daje następujące korzyści:
  - zmniejsza wielkość profili użytkowników,
  - zwiększa wydajność podczas składowania systemu (SAVSYS) lub składowania danych ochrony (SAVSECDTA).
- Listy autoryzacji udostępniają dobry sposób zabezpieczania zbiorów. Jeśli używane są uprawnienia prywatne, każdy użytkownik będzie miał uprawnienia prywatne do każdego podzbioru. Jeśli używana jest lista autoryzacji, każdy użytkownik będzie miał tylko jedno uprawnienie. Otwartym zbiorom nie można nadawać ani odwoływać uprawnień do zbioru. Jeśli zbiór zabezpieczany jest listą autoryzacji, można zmienić uprawnienia, nawet jeśli zbiór jest otwarty.
- Listy autoryzacji udostępniają sposób na zapamiętywanie uprawnień, gdy obiekt jest składowany. Gdy składowany jest obiekt chroniony przez listę autoryzacji, nazwa listy składowana jest razem z obiektem. Jeśli obiekt zostanie usunięty i odtworzony w **tym samym** systemie, automatycznie jest powiązywany z listą autoryzacji. Jeśli obiekt jest odtwarzany w innym systemie, lista autoryzacji nie jest dowiązywana, chyba że w komendzie odtwarzania podano parametr ALWOBJDIF(*ALL).

Korzyści z używania listy autoryzacji

Z punktu widzenia zarządzania ochroną, listy autoryzacji są preferowaną metodą zarządzania obiektami mającymi takie same wymagania ochrony. Nawet jeśli jest tylko kilka obiektów, które mają być zabezpieczane przez listę, nadal będą korzyści z używania listy autoryzacji zamiast używania uprawnień prywatnych do obiektu. Ponieważ uprawnienia

znajdują się w jednym miejscu (na liście autoryzacji), łatwiej jest zmienić użytkowników uprawnionych do obiektu. Łatwiej także zabezpieczać nowe obiekty za pomocą takich samych uprawnień, jak istniejące obiekty.

Jeśli używane są listy autoryzacji, nie powinny istnieć uprawnienia prywatne do obiektu. Podczas sprawdzania uprawnień, jeśli obiekt ma uprawnienia prywatne oraz jest chroniony przez listę autoryzacji, wymagane są dwa przeszukiwania uprawnień prywatnych użytkownika. Pierwsze przeszukiwanie następuje dla uprawnień prywatnych do obiektu, drugie dla uprawnień prywatnych do listy autoryzacji. Dwa przeszukiwania wymagają użycia zasobów systemu, dlatego może to mieć wpływ na wydajność. Jeśli używana jest tylko lista autoryzacji, wykonywane jest tylko jedno przeszukiwanie. Dzięki buforowaniu uprawnień za pomocą listy autoryzacji, wydajność sprawdzania uprawnień będzie taka sama, jak podczas sprawdzania tylko uprawnień prywatnych do obiektu.

W przedsiębiorstwie JKL Toy Company lista autoryzacji wykorzystywana jest do zabezpieczania wszystkich zbiorów roboczych, które używane są podczas przetwarzania zapasów na koniec miesiąca. Ze zbiorów roboczych jest usuwana zawartość, co wymaga uprawnień *OBJMGT. W momencie zmiany wymagań aplikacji, można dodać więcej zbiorów roboczych. Podobnie jest, gdy zmienia się osoba odpowiedzialna za wykonanie zadania; różni użytkownicy mogą uruchamiać przetwarzanie na koniec miesiąca. Lista autoryzacji ułatwia zarządzanie tymi zmianami.

Poniżej opisano czynności wymagane do skonfigurowania listy autoryzacji:

1. Utwórz listę autoryzacji:
   ```
   CRTAUTL ICLIST1
   ```
2. Zabezpiecz wszystkie zbiory robocze za pomocą listy autoryzacji:
   ```
   GRTOBJAUT OBJ(ITEMLIB/ICWRK*) +
             OBJTYP(*FILE) AUTL(ICLIST1)
   ```
3. Do listy dodaj użytkowników, którzy wykonują przetwarzanie na koniec miesiąca:
   ```
   ADDAUTLE AUTL(ICLIST1) USER(USERA) AUT(*ALL)
   ```

Planowanie profili grupowych

Profil grupowy jest przydatnym narzędziem, gdy kilku użytkowników ma podobne wymagania ochrony. Przydatny jest szczególnie wtedy, gdy zmieniają się wymagania zadania oraz członkostwo w grupie. Na przykład jeśli członkowie działu są odpowiedzialni za aplikację, profil grupowy może być skonfigurowany dla działu. Gdy użytkownicy przychodzą lub opuszczają dział, pole profilu grupowego w ich profilach użytkownika może zostać zmienione. Jest to łatwiejszy sposób zarządzania niż usuwanie pojedynczych uprawnień z profilu użytkownika.

Profile można tworzyć od razu jako profile grupowe; można również zmienić na profil grupowy już istniejący profil. Profil grupowy jest po prostu specjalnym rodzajem profilu użytkownika. Staje się profilem grupowym, gdy wystąpi jeden z poniższych warunków:

- inny profil wyznaczy go jako profil grupowy,
- przypisany zostanie numer identyfikacyjny grupy (gid).

Na przykład:

1. Utwórz profil o nazwie GRPIC:
   ```
   CRTUSRPRF GRPIC
   ```
2. Gdy profil jest tworzony, jest zwykłym profilem, a nie profilem grupowym.
3. Wyznacz profil GRPIC jako profil grupowy dla innego profilu grupowego:
   ```
   CHGUSRPRF USERA GRPPRF(GRPIC)
   ```
4. System traktuje teraz profil GRPIC jako profil grupowy i nadaje mu identyfikator gid.

Planowanie grup podstawowych dla obiektów

Każdy obiekt w systemie może mieć grupę podstawową. Uprawnienia grupy podstawowej mogą przynieść korzyści związane z wydajnością, jeśli grupa podstawowa jest pierwszą grupą dla większości użytkowników obiektu.

Często jedna grupa użytkowników jest odpowiedzialna za niektóre informacje dotyczące systemu, jak na przykład informacje o klientach. Ta grupa wymaga więcej uprawnień do informacji niż inni użytkownicy systemu. Używając uprawnienia grupy podstawowej można skonfigurować tego rodzaju schemat uprawnień bez wpływu na wydajność sprawdzania uprawnień. Przykład opisuje sekcja “Przypadek 2: Używanie uprawnień grupy podstawowej” na stronie 167.

Planowanie wielu profili grupowych

Użytkownik może być członkiem do 16 grup: pierwszej grupy (parametr GRPPRF w profilu użytkownika) i 15 grup dodatkowych (parametr SUPGRPPRF). Używając profili grupowych można wydajniej zarządzać uprawnieniami oraz zmniejszyć liczbę pojedynczych uprawnień prywatnych dla obiektów. Niepoprawne użycie profili grupowych może negatywnie wpłynąć na wydajność sprawdzania uprawnień.

Poniżej przedstawiono sugestie, do których należy się stosować podczas używania wielu profili grupowych:

- Wielu grup należy używać w połączeniu z uprawnieniami grupy podstawowej i eliminować uprawnienia prywatne do obiektów.
- Kolejność przypisywania użytkownikom profili grupowych należy planować rozważnie. Pierwsza grupa użytkownika powinna być związana z podstawowym przydziałem użytkownika oraz najczęściej używanymi obiektami. Na przykład użytkownik WAGNERB regularnie przeprowadza inwentaryzację oraz czasami składa zamówienia. Pierwszą grupą użytkownika WAGNERB powinien być profil wymagany dla uprawnień do zapasów (DPTIC). Profil wymagany dla pracy z pozycjami zamówień (DPTOE) powinien być pierwszą grupą dodatkową użytkownika WAGNERB.

  Uwaga: Kolejność podania uprawnień prywatnych do obiektu nie ma wpływu na wydajność sprawdzania uprawnień.
- Jeśli planowane jest użycie wielu grup, należy przestudiować proces sprawdzania uprawnień opisany w sekcji “Sposób sprawdzania uprawnień” na stronie 149. Należy upewnić się, że zrozumiano wpływ używania wielu grup w połączeniu z innymi technikami uprawnień, takimi jak listy autoryzacji, na wydajność systemu.

Łączenie uprawnień specjalnych członków profilu grupowego

Uprawnienia specjalne profili grupowych dostępne są dla członków danej grupy. Profile użytkowników, które są członkami jednej lub więcej grup, mają własne uprawnienia specjalne, plus uprawnienia specjalne wszystkich profili grupowych, których użytkownik jest członkiem. Uprawnienia specjalne dla członków wielu grup są łączone. Na przykład profil GRUPA1 ma uprawnienia *JOBCTL, profil GRUPA3 ma uprawnienia *AUDIT, a profil GRUPA16 uprawnienia specjalne *IOSYSCFG. Profil użytkownika, który jako profile grupowe ma te trzy profile, ma uprawnienia specjalne *JOBCTL, *AUDIT i *IOSYSCFG.

Uwaga: UWAGA

Jeśli członek grupy jest właścicielem programu, program adoptuje tylko uprawnienia właściciela. Uprawnienia grupowe **nie** są adoptowane.

Używanie pojedynczego profilu jako profilu grupowego

Przekształcanie istniejących profili w profile grupowe nie jest dobrym rozwiązaniem, preferowane jest tworzenie od razu profili grupowych. Administrator może stwierdzić, że jeden z użytkowników ma wszystkie uprawnienia wymagane przez grupę użytkowników i przekształcić go w profil grupowy. Jednak używanie pojedynczych profili jako profili grupowych może w przyszłości powodować problemy:

- Jeśli użytkownik, którego profil został użyty jako profil grupowy, zmieni swoje obowiązki, jako profil grupowy trzeba będzie wyznaczyć nowy profil, zmienić uprawnienia oraz przenieść prawa własności do obiektów.
- Wszyscy członkowie grupy automatycznie otrzymują uprawnienia do obiektów tworzonych przez profil grupowy. Użytkownik, którego profil jest profilem grupowym, traci możliwość posiadania prywatnych obiektów, chyba że inni użytkownicy zostaną wykluczeni.

Profile grupowe należy planować z góry. Należy je tworzyć z hasłem *NONE. Jeśli po uruchomieniu aplikacji okaże się, że użytkownik ma uprawnienia, które powinny należeć do grupy użytkowników, należy wykonać następujące czynności:

1. Utwórz profil grupowy.
2. Za pomocą komendy GRTUSRAUT nadaj profilowi grupowemu potrzebne uprawnienia użytkownika.
3. Usuń uprawnienia prywatne użytkownika, ponieważ nie są już potrzebne. Użyj do tego komendy RVKOBJAUT lub EDTOBJAUT.

Porównanie profili grupowych i list autoryzacji

Profile grupowe są używane do uproszczenia zarządzania profilami użytkowników, które mają podobne wymagania ochrony. Listy autoryzacji używane są do zabezpieczania obiektów o podobnych wymaganiach ochrony. Tabela 123 opisuje charakterystyki obu metod:

Tabela 123. Porównanie listy autoryzacji i profilu grupowego

Porównywany element	Lista autoryzacji	Profil grupowy
Używane do zabezpieczania wielu obiektów	Tak	Tak
Użytkownik może należeć do więcej niż jednej	Tak	Tak
Uprawnienia prywatne przesłaniają pozostałe uprawnienia	Tak	Tak
Użytkownicy muszą mieć niezależnie przypisane uprawnienia	Tak	Nie
Podane uprawnienia są takie same dla wszystkich obiektów	Tak	Nie
Obiekt może być chroniony przez więcej niż jedno	Nie	Tak
Uprawnienia mogą być określane w momencie tworzenia obiektu	Tak	Tak[1]
Może zabezpieczać obiekty wszystkich typów	Nie	Tak
Powiązania z obiektem są usuwane podczas usuwania obiektu	Tak	Tak
Powiązania z obiektem są składowane podczas składowania obiektu	Tak	Nie[2]

[1] Profil grupowy może mieć nadawane uprawnienia gdy obiekt jest tworzony, przez użycie parametru GRPAUT w profilu użytkownika tworzącego obiekt.

[2] Uprawnienia grupy podstawowej są składowane razem z obiektem.

Planowanie ochrony dla programistów

Programiści stanowią problem dla szefa ochrony. Ich wiedza umożliwia im obejście procedur ochrony, które nie zostały uważnie zaprojektowane. Mogą oni obejść ochronę w celu dostępu do danych wymaganych do testowania. Mogą także obejść zwykłe procedury, które przydzielają zasoby systemu, aby uzyskać lepszą wydajność dla własnych zadań. Ochrona widziana jest przez nich często jako przeszkoda podczas wykonywania zadań wymaganych dla ich zadań, takich jak testowanie aplikacji. Jednak nadawanie programistom zbyt wielu uprawnień w systemie narusza podstawową zasadę ochrony, jaką jest oddzielanie obowiązków. Umożliwia także instalowanie nieautoryzowanych programów.

Podczas konfigurowania środowiska dla programistów aplikacji należy stosować się do następujących wskazówek:

- programistom nie należy nadawać **wszystkich** uprawnień specjalnych; jednak jeśli muszą mieć uprawnienia specjalne, należy nadawać im **tylko** te, które są wymagane do wykonywania zadań lub zajęć przypisanych programistom,
- jako profilu grupowego dla programistów nie należy używać profilu użytkownika QPGMR,
- należy używać bibliotek testowych oraz zapobiegać ich dostępowi do bibliotek produkcyjnych,
- należy tworzyć biblioteki programistów, a do kopiowania danych produkcyjnych do testowania używać programów, które adoptują uprawnienia,
- jeśli kwestią sporną jest wydajność interaktywna, należy rozważyć zamianę komend do tworzenia programów w celu uruchamiania wsadowego:

  ```
  CHGCMD CMD(CRTxxxPGM) ALLOW(*BATCH *BPGM),
  ```

- przed przeniesieniem aplikacji lub zmian w programach z bibliotek testowych do produkcyjnych należy wywołać funkcję kontroli ochrony,
- gdy aplikacja jest rozwijana, należy używać techniki profilu grupowego; wszystkie aplikacje powinny należeć do profilu grupowego; programistów pracujących nad aplikacją należy przydzielić do profilu grupowego i zdefiniować w ich profilach, że nowo tworzone obiekty należą do grupy (OWNER(*GRPPRF)); gdy programista przechodzi z jednego projektu do innego, w jego profilu można zmienić informacje o grupie; więcej informacji na ten temat zawiera sekcja “Grupowe prawo własności do obiektów” na stronie 123,
- należy opracować plan przypisywania prawa własności do aplikacji podczas ich przenoszenia do środowiska produkcyjnego; aby kontrolować zmiany w aplikacji produkcyjnej, wszystkie obiekty aplikacji, także programy, powinny należeć do profilu użytkownika przeznaczonego dla aplikacji,

  obiekty aplikacji nie powinny należeć do programisty, ponieważ programista miałby niekontrolowany dostęp do nich w środowisku produkcyjnym; profil, który jest właścicielem aplikacji, może być profilem pojedynczego użytkownikaodpowiedzialnego za aplikację lub profilem specjalnie utworzonym jako właściciel aplikacji.

Zarządzanie zbiorami źródłowymi

Zbiory źródłowe są bardzo ważne dla integralności systemu. Mogą być także wartościowymi aktywami przedsiębiorstwa, jeśli w przedsiębiorstwie są używane własne lub zakupione aplikacje. Zbiory źródłowe powinny być chronione, tak jak inne ważne zbiory w systemie. Należy rozważyć umieszczenie zbiorów źródłowych w oddzielnej bibliotece i kontrolowanie ich aktualizacji oraz przenoszenia do środowiska produkcyjnego.

Gdy w systemie tworzony jest zbiór źródłowy, domyślne uprawnienia publiczne mają wartość *CHANGE, co umożliwia użytkownikom aktualizowanie dowolnego podzbioru źródłowego. Domyślnie tylko właściciel zbioru źródłowego lub użytkownik z uprawnieniami *ALLOBJ może dodawać lub usuwać podzbiory. W większości przypadków te uprawnienia domyślne powinny być zmienione. Programiści pracujący z aplikacją wymagają uprawnień *OBJMGT do zbiorów źródłowych, w celu dodawania nowych podzbiorów. Uprawnienia publiczne powinny być zredukowane do *USE lub *EXCLUDE, chyba że zbiory źródłowe znajdują się w chronionej bibliotece.

Planowanie ochrony dla programistów systemowych lub menedżerów

Większość systemów ma osobę odpowiedzialną za funkcje zarządzające. Ta osoba monitoruje użycie zasobów systemowych, w szczególności pamięć dyskową, aby upewnić się, że użytkownicy regularnie usuwają nieużywane obiekty. Programiści systemowi potrzebują szerokich uprawnień do obserwowania wszystkich obiektów w systemie. Jednak nie muszą oni przeglądać zawartości tych obiektów.

W celu udostępnienia programistom systemowym zestawu komend wyświetlających, zamiast nadawania uprawnień specjalnych ich profilom użytkowników, można użyć uprawnień adoptowanych.

Planowanie użycia obiektów listy sprawdzania

Obiekty listy sprawdzania są nowym typem obiektów w wydaniu 1 wersji 4 i udostępniają aplikacji metodę bezpiecznego przechowywania informacji uwierzytelniających użytkowników.

Na przykład Internet Connection Server (ICS) korzysta z list sprawdzania do implementowania pojęcia **użytkownika Internetu**. W wersji 4, wydaniu 1, przed udostępnieniem strony WWW ICS może wykonać **podstawowe uwierzytelnianie**. Podstawowe uwierzytelnianie wymaga od użytkowników podania pewnego rodzaju informacji uwierzytelniających, takich jak hasło, numer PIN lub numer rachunku. Nazwa użytkownika oraz informacje uwierzytelniające mogą być bezpiecznie przechowywane w listach sprawdzania. ICS może użyć informacji z listy sprawdzania, zamiast wymagać od każdego użytkownika ICS podawania identyfikatora użytkownika systemu iSeries oraz hasła.

Użytkownik Internetu może mieć umożliwiony lub zabroniony dostęp do systemu iSeries z serwera WWW. Jednak nie ma on żadnych uprawnień do zasobów systemu iSeries lub uprawnień do wpisywania się i uruchamiania zadań. Dla użytkowników sieci Internet nigdy nie są tworzone profile użytkowników systemu iSeries.

Aby utworzyć lub usunąć listy sprawdzania, można użyć komendy CL Tworzenie listy sprawdzania (Create Validation List - CRTVLDL) i Usunięcie listy sprawdzania (Delete Validation List - DLTVLDL). Aplikacyjne interfejsy programistyczne (API) także udostępniają możliwość dodawania, zmiany, usuwania, sprawdzania (uwierzytelniania) oraz odnajdywania przez aplikację pozycji na liście sprawdzania. Więcej informacji oraz przykładów, zawiera temat Funkcje API w Centrum informacyjnym (patrz sekcja “Informacje wstępne i pokrewne” na stronie xvi).

Obiekty listy sprawdzania dostępne są dla każdej aplikacji. Na przykład jeśli aplikacja wymaga hasła, hasła aplikacji mogą być przechowywane na liście sprawdzania, a nie w zbiorze bazy danych. Aplikacja może używać funkcji API listy sprawdzania w celu sprawdzenia hasła użytkownika, które jest zaszyfrowane, zamiast wykonywania sprawdzania.

W wersji 4, wydaniu 1 informacje uwierzytelniania (hasło, PIN, numer rachunku), które związane są z listą sprawdzania, zawsze przechowywane są w postaci niemożliwej do odszyfrowania, która nie może być zwrócona użytkownikowi.

W wersji 4, wydaniu 2 można wybrać, czy informacje uwierzytelniania mają być przechowywane w postaci możliwej do odszyfrowania. Jeśli użytkownik ma odpowiednią ochronę, informacje te mogą zostać odszyfrowane i zwrócone do użytkownika. Informacje dotyczące kontrolowania przechowywania możliwych do odszyfrowania danych na listach sprawdzania, zawiera sekcja “Zachowanie ochrony serwera (QRETSVRSEC)” na stronie 27.

Ograniczanie dostępu do funkcji programu

Ograniczenie dostępu do funkcji programu umożliwia zdefiniowanie użytkowników mogących korzystać z aplikacji, części aplikacji lub funkcji programu. Ta obsługa **nie** zastępuje ochrony zasobów. Ograniczanie dostępu do funkcji programu nie zabezpiecza przed dostępem do zasobów (takich jak zbiór lub program) z innego interfejsu.

Obsługa ograniczania dostępu do funkcji programu udostępnia funkcje API do:

- rejestrowania funkcji,
- pobierania informacji o funkcji,
- definiowania, kto może, a kto nie może korzystać z funkcji,
- sprawdzania, czy użytkownik ma uprawnienia do korzystania z funkcji.

Aby wykorzystać tę obsługę w ramach aplikacji, dostawca aplikacji musi zarejestrować funkcje podczas instalowania aplikacji. Zarejestrowana funkcja odpowiada blokowi kodu realizującemu określone funkcje w aplikacji. Gdy użytkownik uruchamia aplikację, wywoływana jest funkcja API sprawdzania użycia, aby sprawdzić, czy użytkownik ma uprawnienia do korzystania z funkcji, która jest związana z blokiem kodu, zanim ten blok zostanie wywołany. Jeśli tak, uruchamiany jest blok kodu. Jeśli nie, użytkownik nie ma możliwości uruchomienia bloku kodu.

Administrator systemu określa, kto ma lub nie ma dostępu do funkcji. Do zarządzania dostępem do funkcji programu, administrator może użyć komendy Praca z informacjami o użyciu funkcji (Work with Function Usage Information - WRKFCNUSG) lub programu iSeries Navigator.

Rozdział 8. Składowanie i odtwarzanie informacji o ochronie

Ten rozdział opisuje, w jaki sposób ochrona związana jest z operacjami składowania i odtwarzania w systemie:

- W jaki sposób są składowane i odtwarzane informacje o ochronie.
- W jaki sposób ochrona wpływa na składowanie i odtwarzanie obiektów.
- Zagadnienia dotyczące ochrony, które związane są z uprawnieniami specjalnymi *SAVSYS.

Więcej informacji na temat składowania i odtwarzania udostępnia książka *Składowanie i odtwarzanie*. Można także zapoznać się z tematami Składowanie i odtwarzanie, które znajdują się w Centrum informacyjnym (patrz sekcja “Informacje wstępne i pokrewne” na stronie xvi).

Składowanie informacji o ochronie jest tak samo ważne, jak składowanie danych. W niektórych sytuacjach konieczne może być odtworzenie profili użytkowników, uprawnień do obiektu oraz danych. Jeśli będzie brakowało zeskładowanych informacji o ochronie, użytkownik będzie musiał ręcznie odbudowywać profile użytkowników oraz uprawnienia do obiektów. Taka operacja może być czasochłonna oraz prowadzić do błędów i ryzyka naruszenia ochrony.

Planowanie odpowiednich procedur składowania i odtwarzania informacji o ochronie wymaga zrozumienia, jak te informacje są przechowywane, składowanie oraz odtwarzane.

Tabela 124 opisuje komendy, które są używane do składowania i odtwarzania informacji o ochronie. Przedstawione poniżej sekcje prezentują szczegółowe omówienie składowania i odtwarzania informacji o ochronie.

Tabela 124. W jaki sposób są składowane i odtwarzane informacje o ochronie

	Użyte komendy do składowania i odtwarzania				
Składowane lub odtwarzane informacje o ochronie	**SAVSECDTA SAVSYS**	**SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG**	**RSTUSRPRF**	**RSTOBJ RSTLIB RSTDLO RSTCFG**	**RSTAUT**
Profile użytkowników	X		X		
Prawo własności[1]		X		X	
Grupa podstawowa[1]		X		X	
Uprawnienia publiczne[1]		X		X	
Uprawnienia prywatne	X				X
Listy autoryzacji	X		X		
Magazyny uprawnień	X		X		
Powiązania z listą autoryzacji i magazynami uprawnień		X		X	
Wartość kontroli obiektu		X		X	
Informacje rejestrowania funkcji[2]		X		X	
Informacje o używaniu funkcji	X		X		X

[1] Komendy SAVSECDTA, SAVSYS i RSTUSRPRF składują i odtwarzają prawa własności, grupę podstawową, uprawnienia grupy podstawowej oraz uprawnienia publiczne następujących typów obiektów: profilu użytkownika (*USRPRF), listy autoryzacji (*AUTL) i magazynu uprawnień (*AUTHLR).

[2] Obiektem do składowania/odtworzenia jest obiekt QUSEXRGOBJ, w bibliotece QUSRSYS; należy wpisać *EXITRG.

Jak przechowywane są informacje o ochronie

Informacje o ochronie przechowywane są z obiektami, profilami użytkowników i listami autoryzacji:

Informacje o uprawnieniach przechowywane z obiektem:

Uprawnienia publiczne

Nazwa właściciela

Uprawnienia właściciela do obiektu

Nazwa grupy podstawowej

Uprawnienia grupy podstawowej do obiektu

Nazwa listy autoryzacji

Wartość kontroli obiektu

Czy istnieją jakieś uprawnienia prywatne

Czy uprawnienia prywatne są mniejsze niż publiczne

Informacje o uprawnieniach przechowywane z profilem użytkownika:

Główne informacje:

Atrybuty profilu użytkownika wyświetlane na ekranie Tworzenie profilu użytkownika (Create User Profile).

Identyfikatory uid i gid.

Informacje o uprawnieniach prywatnych:

Uprawnienia prywatne do obiektów. Obejmuje to także uprawnienia prywatne do list autoryzacji.

Informacje o prawie własności:

Lista posiadanych obiektów.

Dla każdego posiadanego obiektu lista użytkowników z uprawnieniami prywatnymi do danego obiektu.

Informacje o grupie podstawowej:

Lista obiektów, dla których profil jest grupą podstawową.

Informacje o kontroli:

Wartość kontroli działania.

Wartość kontroli obiektu

Informacje o używaniu funkcji:

Ustawienia używania dla zarejestrowanych funkcji.

Informacje o uprawnieniach przechowywane z listami autoryzacji:

Zwykłe informacje o uprawnieniach przechowywane z dowolnym obiektem, takie jak uprawnienia publiczne i prawo własności.

Lista wszystkich obiektów zabezpieczanych przez listę autoryzacji.

Składowanie informacji o ochronie

Informacje o ochronie składowane są na nośnikach składowania inaczej niż w systemie. Gdy składowane są profile użytkowników, informacje o uprawnieniach prywatnych, przechowywanych razem z profilem, formatowane są w postaci tabeli uprawnień. Tabela uprawnień jest budowana i składowana dla każdego profilu użytkownika, który ma uprawnienia publiczne. W przypadku gdy użytkownik ma dużo uprawnień prywatnych, reformatowanie i składowanie może trwać długo.

Informacje o ochronie składowane są na nośnikach składowania w następujący sposób:

Informacje o uprawnieniach składowane z obiektem:

Uprawnienia publiczne

Nazwa właściciela

Uprawnienia właściciela do obiektu

Nazwa grupy podstawowej

Uprawnienia grupy podstawowej do obiektu

Nazwa listy autoryzacji

Uprawnienia na poziomie pola

Wartość kontroli obiektu

Czy istnieją jakieś uprawnienia prywatne

Czy uprawnienia prywatne są mniejsze niż publiczne

Informacje o uprawnieniach składowane z listą autoryzacji:

Zwykłe informacje o uprawnieniach przechowywane z dowolnym obiektem, takie jak uprawnienia publiczne, właściciel i grupa podstawowa.

Informacje o uprawnieniach składowane z profilem użytkownika:

Atrybuty profilu użytkownika wyświetlane na ekranie Tworzenie profilu użytkownika (Create User Profile).

Składowana tabela uprawnień powiązana z profilem użytkownika:

Jeden rekord na każde uprawnienie prywatne profilu użytkownika, w tym na ustawienia użycia zarejestrowanych funkcji.

Informacje o zarejestrowaniu funkcji składowane z obiektem QUSEXRGOBJ:

Informacje o zarejestrowaniu funkcji mogą być zeskładowane podczas składowania obiektu QUSEXRGOBJ *EXITRG w bibliotece QUSRSYS.

Odzyskiwanie informacji o ochronie

Odzyskiwanie systemu często wymaga odtworzenia danych i związanych z nimi informacji o ochronie. Zwykła sekwencja odzyskiwania wymaga:

1. Odtworzenia profili użytkowników i list autoryzacji (RSTUSRPRF USRPRF(*ALL)).
2. Odtworzenia obiektów (RSTLIB, RSTOBJ lub RSTCFG).
3. Odtworzenia uprawnień prywatnych do obiektów (RSTAUT).

Więcej informacji dotyczących planowania odtwarzania zawiera książka *Składowanie i odtwarzanie*.

Odtwarzanie profili użytkowników

Podczas odtwarzania profilu użytkownika można wprowadzić do niego kilka zmian. Są to między innymi:

- Jeśli profile odtwarzane są pojedynczo (nie podano parametru RSTUSRPRF USRPRF(*ALL)), parametr SECDTA(*PWDGRP) nie jest wymagany, a odtwarzany profil nie istnieje w systemie, na wartość *NONE zmieniane są następujące pola:
  - nazwa profilu grupowego (GRPPRF),
  - Hasło (PASSWORD)
  - Hasło do dokumentu (DOCPWD)
  - dodatkowe profile grupowe (SUPGRPPRF).

  Hasła do produktu zmieniane są na wartość *NONE, dlatego po odtworzeniu pojedynczego profilu użytkownika, który nie istniał w systemie, będą niepoprawne.
- Jeśli profile odtwarzane są pojedynczo (nie podano parametru RSTUSRPRF USRPRF(*ALL)), parametr SECDTA(*PWDGRP) nie jest wymagany, a profil istnieje w systemie, hasło, hasło do dokumentu oraz profil grupowy nie są zmieniane.

Za pomocą parametru SECDTA(*PWDGRP) komendy RSTUSRPRF profile użytkowników mogą być odtwarzane pojedynczo z nośnika składowania, z odtworzeniem hasła i informacji o grupie. Aby odtworzyć hasło oraz informacje o grupie, podczas odtwarzania pojedynczych profili, wymagane są uprawnienia specjalne *ALLOBJ i *SECADM. Po odtworzeniu pojedynczego profilu użytkownika, który istniał w systemie, odtwarzane razem z nim hasła do produktu nie będą poprawne, chyba że dla komendy RSTUSRPRF podano parametr SECDTA(*PWDGRP).

- Jeśli w systemie odtwarzane są wszystkie profile, wszystkie pola tych profili, które już istnieją w systemie, są odtwarzane z nośnika składowania (w tym także hasło).

  Uwaga: Profile użytkowników zeskładowane w systemie z innym poziomem haseł (wartość systemowa QPWDLVL), niż w systemie, w którym są odtwarzane, mogą mieć nieprawidłowe hasła. Na przykład jeśli zeskładowany profil użytkownika pochodzi z systemu, w którym ustawiony był poziom hasła równy 2, użytkownik mógł mieć hasło typu ″To jest moje hasło″. Takie hasło nie będzie poprawne w systemie z poziomem hasła 0 lub 1.

  Uwaga: Należy zapisać hasło szefa ochrony (QSECOFR) związane z każdą wersją informacji o ochronie, która została zeskładowana, aby umożliwić wpisanie się do systemu, gdyby zaszła konieczność pełnego odtwarzania.

  Do zresetowania hasła dla profilu QSECOFR można wykorzystać narzędzia DST. Instrukcje na ten temat zawiera temat Narzędzia serwisowe w Centrum informacyjnym. Więcej informacji na temat sposobu dostępu do Centrum informacyjnego zawiera sekcja “Informacje wstępne i pokrewne” na stronie xvi.
- Jeśli profil istnieje w systemie, operacja odtwarzania nie zmienia identyfikatora uid lub gid.
- Jeśli profil nie istnieje w systemie, identyfikatory uid i gid dla profilu odtwarzane są z nośnika składowania. Jeśli identyfikator uid lub gid już istnieje w systemie, generowana jest nowa wartość oraz komunikat (CPI3810).
- Uprawnienia specjalne *ALLOBJ są usuwane z odtwarzanych profili użytkowników, jeśli system znajduje się na poziomie ochrony 30 lub wyższym, w następujących sytuacjach:
  - profil został zeskładowany w innym systemie, a użytkownik wywołujący komendę RSTUSRPRF nie ma uprawnień specjalnych *ALLOBJ i *SECADM,
  - profil został zeskładowany w tym samym systemie, ale na poziomie ochrony 10 lub 20.

  UWAGA: W celu określenia, czy obiekty odtwarzane są w tym samym systemie, czy innym, system używa numeru seryjnego komputera oraz nośnika składowania.

  Uprawnienia specjalne *ALLOBJ **nie** są usuwane z następujących profili użytkowników IBM:

  QSYS (system), profil użytkownika

  QSECOFR (szef ochrony), profil użytkownika

  QLPAUTO (instalowanie automatyczne programu licencjonowanego), profil użytkownika

  QLPINSTALL (instalowanie programu licencjonowanego), profil użytkownika

Odtwarzanie obiektów

Podczas odtwarzania obiektu system korzysta z informacji o uprawnieniach zeskładowanych razem z obiektem. Ochrony odtwarzanych obiektów dotyczą następujące zagadnienia:

Prawo własności do obiektu:

- Jeśli profil, który jest właścicielem obiektu, znajduje się w systemie, prawo własności do tego profilu jest odtwarzane.
- Jeśli profil właściciela nie istnieje w systemie, prawo własności do obiektu nadawane jest profilowi użytkownika QDFTOWN (domyślny właściciel).
- Jeśli obiekt istnieje w systemie, a właściciel jest inny niż właściciel z nośnika składowania, obiekt nie jest odtwarzany, chyba że podano parametr ALWOBJDIF(*ALL). W takim przypadku obiekt jest odtwarzany i używany jest właściciel w nowym systemie.
- Dodatkowe uwagi dotyczące odtwarzania programów zawiera sekcja “Odtwarzanie programów” na stronie 229.

Grupa podstawowa:

W przypadku gdy obiekt nie istnieje w systemie:

- Jeśli profil, który jest grupą podstawową dla obiektu, znajduje się w systemie, odtwarzana jest wartość grupy podstawowej oraz uprawnienia do obiektu.
- Jeśli profil, który jest grupą podstawową, nie istnieje:
  - grupa podstawowa dla obiektu ustawiana jest na wartość none (brak),
  - uprawnienia grupy podstawowej ustawiane są na brak uprawnień.

Gdy odtwarzany jest istniejący obiekt, operacja odtwarzania nie zmienia grupy podstawowej dla obiektu.

Uprawnienia publiczne:
- Jeśli odtwarzany obiekt nie istnieje w systemie, uprawnienia publiczne będą takie same, jak uprawnienia publiczne zeskładowanego obiektu.
- Jeśli odtwarzany obiekt istnieje, uprawnienia publiczne nie są zmieniane. Uprawnienia publiczne z zeskładowanej wersji obiektu nie są używane.
- Podczas odtwarzania obiektów do biblioteki, parametr CRTAUT dla biblioteki nie jest używany.

Lista autoryzacji:
- Jeśli obiekt, inny niż dokument lub folder, już istnieje w systemie oraz jest powiązany z listą autoryzacji, parametr ALWOBJDIF określa wynik:
  - jeśli podano ALWOBJDIF(*NONE), istniejący obiekt musi mieć taką samą listę autoryzacji, jak obiekt zeskładowany; jeśli nie ma, obiekt nie zostanie odtworzony,
  - jeśli podano ALWOBJDIF(*ALL), obiekt jest odtwarzany; obiekt powiązywany jest z listą autoryzacji związaną z istniejącym obiektem.
- Jeśli odtwarzany jest dokument lub folder, który już istnieje w systemie, używana jest lista autoryzacji związana z obiektem znajdującym się w systemie. Lista autoryzacji z zeskładowanego dokumentu lub folderu nie jest używana.
- Jeśli lista autoryzacji nie istnieje, obiekt odtwarzany jest bez powiązywania z listą autoryzacji, a uprawnienia publiczne zmieniane są na *EXCLUDE.
- Jeśli obiekt jest odtwarzany w tym samym systemie, w którym był zeskładowany, jest ponownie powiązywany z listą autoryzacji.
- Jeśli obiekt jest odtwarzany w innym systemie, do określenia, czy obiekt ma być powiązany z listą autoryzacji, używany jest parametr ALWOBJDIF komendy odtwarzania:
  - jeśli podano ALWOBJDIF(*ALL), obiekt jest powiązywany z listą autoryzacji,
  - jeśli podano If ALWOBJDIF(*NONE) obiekt nie jest powiązywany z listą autoryzacji, a jego uprawnienia publiczne ustawiane są na *EXCLUDE.

Uprawnienie prywatne:
- Uprawnienia prywatne składowane są z profilami użytkowników, a nie z obiektami.
- Jeśli profile użytkowników mają uprawnienia prywatne do odtwarzanego obiektu, te uprawnienia zazwyczaj nie są używane. Odtwarzanie pewnych typów programów może powodować odwoływanie uprawnień prywatnych. Więcej informacji na ten temat zawiera sekcja “Odtwarzanie programów” na stronie 229.
- Jeśli obiekt jest usuwany z systemu, a potem odtwarzany z zeskładowanej wersji, uprawnienia prywatne do tego obiektu już nie istnieją w systemie. Gdy obiekt jest usuwany, wszystkie uprawnienia prywatne do obiektu są usuwane z profili użytkowników.
- Jeśli trzeba odtworzyć uprawnienia prywatne, musi być użyta komenda Odtwarzanie uprawnień (Restore Authority - RSTAUT). Normalną kolejnością jest:
  1. Odtworzenie profili użytkowników
  2. Odtworzenie obiektów.
  3. Odtworzenie uprawnień.

Kontrolowanie obiektu:
- Jeśli odtwarzany obiekt nie istnieje w systemie, wartość kontrolowania obiektu (OBJAUD) jest odtwarzana.

- Jeśli odtwarzany obiekt istnieje i jest zastępowany, wartość kontrolowania obiektu nie jest zmieniana. Wartość OBJAUD zeskładowanej wersji obiektu nie jest odtwarzana.
- Jeśli odtwarzana biblioteka nie istnieje w systemie, wartość kontroli tworzenia obiektu (CRTOBJAUD) dla biblioteki jest odtwarzana.
- Jeśli odtwarzana biblioteka istnieje i jest zastępowana, wartość CRTOBJAUD nie jest odtwarzana. Użyta zostanie wartość CRTOBJAUD dla istniejącej biblioteki.

Magazyn uprawnień:
- Jeśli dla odtwarzanego zbioru istnieje magazyn uprawnień dla zbioru oraz biblioteki o takiej nazwie, zbiór jest z nim łączony.
- Informacje o uprawnieniach związane z magazynem uprawnień zastępują uprawnienia publiczne oraz informacje o właścicielu zeskładowane ze zbiorem.

Obiekty domeny użytkownika:
- W przypadku systemów w wersji 2, wydanie 3, lub późniejszych programu licencjonowanego OS/400, system ogranicza obiekty domeny użytkownika (*USRSPC, *USRIDX i *USRQ) do bibliotek podanych w wartości systemowej QALWUSRDMN. Jeśli biblioteka przenoszona jest z wartości systemowej QALWUSRDMN po zeskładowaniu obiektu domeny użytkownika typu *USRSPC, *USRIDX lub *USRQ, podczas odtwarzania obiektu system zmienia go na domenę systemu.

Informacje o zarejestrowaniu funkcji:
- Informacje o zarejestrowaniu funkcji mogą być odtwarzane przez odtwarzanie obiektu QUSEXRGOBJ *EXITRG w bibliotece QUSRSYS. Powoduje to odtworzenie wszystkich zarejestrowanych funkcji. Informacje o użyciu związane z funkcjami są odtwarzane podczas odtwarzania profili użytkowników oraz uprawnień.

Aplikacje używające rejestracji certyfikatów
- Aplikacje używające informacji o rejestrowaniu certyfikatów mogą być odtwarzane przez odtwarzanie obiektu QUSEXRGOBJ *EXITRG w bibliotece QUSRSYS. Powoduje to odtworzenie wszystkich zarejestrowanych aplikacji. Powiązanie aplikacji z jej informacją o certyfikacie może być odtworzone przed odtwarzaniem obiektu QYCDCERTI *USRIDX w bibliotece QUSRSYS.

Odtwarzanie uprawnień

Gdy odtwarzane są informacje o ochronie, trzeba odbudować uprawnienia prywatne. Gdy odtwarzany jest profil użytkownika, który ma tabelę uprawnień, ta tabela także jest odtwarzana.

Komenda Odtwarzanie uprawnień (Restore Authority - RSTAUT) odbudowuje uprawnienia prywatne profilu użytkownika, korzystając z informacji z tabeli uprawnień. Dla każdego uprawnienia prywatnego z tabeli uprawnień uruchamiana jest operacja nadawania uprawnień. Jeśli uprawnienia odtwarzane są dla wielu profili, a w tabelach uprawnień istnieje wiele uprawnień prywatnych, proces ten może znacznie się wydłużyć.

Komendy RSTUSRPRF i RSTAUT mogą być uruchomione dla pojedynczego profilu, listy profili, ogólnej nazwy profilu lub dla wszystkich profili. System przeszukuje nośnik składowania lub zbiór składowania utworzony przez komendę SAVSECDTA lub SAVSYS albo przez funkcję API QSRSAVO w celu odnalezienia profili, które mają być odtworzone.

Odtwarzanie uprawnień do pola:

W celu odtworzenia uprawnień prywatnych do pola dla zbiorów bazy danych, które jeszcze nie istnieją w systemie, wymagane jest wykonanie następujących czynności:
- odtworzenie lub utworzenie wymaganych profili użytkowników,
- odtworzenie zbiorów,
- uruchomienie komendy Odtwarzanie uprawnień (Restore Authority - RSTAUT).

Uprawnienia prywatne do pola nie będą w pełni odtworzone, dopóki uprawnienia prywatne do obiektu, które je ograniczają, nie zostaną także ustanowione.

Odtwarzanie programów

Odtwarzanie w systemie programów, które zostały pobrane z nieznanego źródła, stanowi ryzyko naruszenia ochrony. Programy mogą wykonywać operacje, które złamią wymagania ochrony. Szczególnie należy zwrócić uwagę na programy zawierające zastrzeżone instrukcje, programy adoptujące uprawnienia właściciela oraz programy, które ktoś zmieniał. Obejmuje to typy obiektów *PGM, *SRVPGM, *MODULE i *CRQD. Aby zapobiec odtwarzaniu tego typu obiektów, można użyć wartości systemowych QVFYOBJRST, QFRCCVNRST i QALWOBJRST. Więcej informacji na temat tych wartości systemowych zawiera sekcja Wartości systemowe odtwarzania związane z ochroną.

System korzysta z wartości sprawdzania podczas zabezpieczania programów. Ta wartość przechowywana jest z programem i ponownie obliczana podczas odtwarzania programu. Działania systemu określane są przez parametr ALWOBJDIF komendy odtwarzania oraz wartość systemową wymuszenia konwersji podczas odtwarzania (QFRCCVNRST).

Uwaga: Programy utworzone dla wydania 1 wersji 5 lub nowszych systemu iSeries zawierają informacje, które umożliwiają ponowne utworzenie programu podczas odtwarzania. Informacje wymagane do ponownego utworzenia programu pozostają razem z programem, nawet jeśli obserwowalność programu zostanie usunięta. Jeśli podczas odtwarzania programu powstanie błąd sprawdzania programu, program zostanie ponownie utworzony w celu poprawienia błędu sprawdzania. Ponowne tworzenie programu podczas odtwarzania nie jest nową opcją systemu iSeries w wersji 5 wydaniu 1. W poprzednich wydaniach, każdy błąd sprawdzania programu, który pojawił się podczas odtwarzania, powodował ponowne tworzenie programu, jeśli było to możliwe (jeśli w odtwarzanym programie istniała obserwowalność). Różnica między programami systemu iSeries w wersji 5 wydaniu 1 lub nowszych, polega na tym, że informacje wymagane do ponownego utworzenia programu pozostają, nawet jeśli z programu usunięta zostanie obserwowalność.

Odtwarzanie programów, które adoptują uprawnienia właściciela:

Gdy odtwarzany jest program adoptujący uprawnienia właściciela, prawo własności oraz uprawnienia do programu mogą zostać zmienione. Stosowane są następujące kryteria:

- Profil użytkownika przeprowadzającego odtwarzanie musi być właścicielem programu lub mieć uprawnienia specjalne *ALLOBJ i *SECADM.
- Profil użytkownika przeprowadzającego odtwarzanie może otrzymać uprawnienia do odtwarzania programu, jeśli:
  - jest właścicielem programu,
  - jest członkiem profilu grupowego, który jest właścicielem programu (chyba że ma uprawnienia prywatne do programu),
  - ma uprawnienia specjalne *ALLOBJ i *SECADM,
  - jest członkiem profilu grupowego, który ma uprawnienia specjalne *ALLOBJ i *SECADM,
  - działa za pomocą uprawnień adoptowanych, które spełniają jeden z wyżej wymienionych warunków.
- Jeśli odtwarzający profil nie ma odpowiednich uprawnień, wszystkie uprawnienia publiczne i prywatne do programu są odwoływane, a uprawnienia publiczne zmieniane na *EXCLUDE.
- Jeśli właściciel programu nie istnieje, prawo własności nadawane jest profilowi użytkownika QDFTOWN. Uprawnienia publiczne zmieniane są na *EXCLUDE, a lista autoryzacji jest usuwana.

Odtwarzanie programów licencjonowanych

Komenda Odtworzenie programu licencjonowanego (Restore Licensed Program - RSTLICPGM) używana jest do instalowania w systemie programów IBM. Może być użyta także do zainstalowania programów firm innych niż IBM, które zostały utworzone za pomocą programu licencjonowanego SystemView* System Manager/400*.

W nowym systemie komendy RSTLICPGM mogą używać wyłącznie użytkownicy z uprawnieniami specjalnymi *ALLOBJ. W celu zainstalowania programów, które nie są dostarczane przez IBM, procedura RSTLICPGM wywołuje program obsługi wyjścia.

Aby zabezpieczyć ochronę systemu, program obsługi wyjścia nie powinien być uruchamiany z wykorzystaniem profilu mającego uprawnienia specjalne *ALLOBJ. Do uruchomienia komendy RSTLICPGM należy używać programu adoptującego uprawnienia specjalne *ALLOBJ, a nie wykorzystywać użytkownika z uprawnieniami *ALLOBJ do bezpośredniego uruchamiania tej komendy.

Poniżej przedstawiono przykład tej techniki. Program, który ma być zainstalowany za pomocą komendy RSTLICPGM, to program CPAPP (Kontrakty i wycena).

1. Utwórz profil użytkownika z uprawnieniami wystarczającymi do pomyślnego zainstalowania aplikacji. Nie nadawaj temu profilowi uprawnień specjalnych *ALLOBJ. Na przykład może to być profil użytkownika OWNCP.
2. Napisz program do instalowania aplikacji. Na przykład program CPINST:

   ```
   PGM
   RSTLICPGM CPAPP
   ENDPGM
   ```

3. Ustaw parametry programu CPINST tak, aby adoptował uprawnienia użytkownika z uprawnieniami specjalnymi *ALLOBJ, na przykład QSECOFR, i nadaj uprawnienia do tego programu użytkownikowi OWNCP:

   ```
   CRTCLPGM QGPL/CPINST USRPRF(*OWNER) +
            AUT(*EXCLUDE)
   GRTOBJAUT OBJ(CPINST) OBJTYP(*PGM) +
             USER(OWNCP)  AUT(*USE)
   ```

4. Wpisz się jako użytkownik OWNCP i wywołaj program CPINST. Gdy program CPINST uruchomi komendę RSTLICPGM, użytkownik będzie działał z uprawnieniami użytkownika QSECOFR. Gdy program obsługi wyjścia zostanie uruchomiony do zainstalowania programów CPAPP, porzuci uprawnienia adoptowane. Programy wywoływane przez program obsługi wyjścia uruchamiane są z uprawnieniami użytkownika OWNCP.

Odtwarzanie list autoryzacji

Listy autoryzacji składowane są za pomocą komendy SAVSECDTA lub SAVSYS. Odtwarzane są przez komendę:

```
RSTUSRPRF USRPRF(*ALL)
```

Nie istnieje żadna metoda odtworzenia pojedynczej listy.

Podczas odtwarzania listy autoryzacji uprawnienia i prawo własności ustawiane jest tak samo, jak dla innych odtwarzanych obiektów. Jeśli obiekty odtwarzane są po odtworzeniu list autoryzacji, ustanawiane są powiązania między listami a obiektami. Więcej informacji na ten temat zawiera sekcja “Odtwarzanie obiektów” na stronie 226. Uprawnienia prywatne użytkownika do listy odtwarzane są za pomocą komendy RSTAUT.

Odzyskiwanie zniszczonej listy autoryzacji

Gdy obiekt zabezpieczany jest przez listę autoryzacji, która zostanie zniszczona, dostęp do obiektu ograniczany jest tylko do użytkowników mających uprawnienia specjalne *ALLOBJ.

Aby odtworzyć zniszczoną listę autoryzacji, wymagane są dwie czynności:

1. Odtwarzanie użytkowników i ich uprawnień do listy autoryzacji.
2. Odtwarzanie powiązań listy autoryzacji z obiektami.

Te czynności muszą być wykonane przez użytkownika z uprawnieniami specjalnymi *ALLOBJ.

Odzyskiwanie listy autoryzacji: Jeśli znane są uprawnienia użytkownika do listy autoryzacji, po prostu należy usunąć listę autoryzacji, utworzyć ją ponownie i następnie dodać do niej użytkowników.

Jeśli ponowne utworzenie listy autoryzacji nie jest możliwe, gdyż nie są znane wszystkie uprawnienia użytkownika, można odtworzyć listę autoryzacji i za pomocą ostatnich taśm SAVSYS lub SAVSECDTA odtworzyć użytkowników tej listy. Aby odtworzyć listę autoryzacji, należy wykonać następujące czynności:

1. Za pomocą komendy Usunięcie listy autoryzacji (Delete Authorization List - DLTAUTL) usuń zniszczoną listę autoryzacji.
2. Odtwarzając profile użytkowników odtwórz listę autoryzacji:

```
RSTUSRPRF USRPRF(*ALL)
```

3. Za pomocą komendy RSTAUT odtwórz uprawnienia prywatne użytkowników do listy.

Uwaga: Ta procedura odtwarza z nośnika składowania wartości profili użytkowników. Więcej informacji na ten temat zawiera sekcja “Odtwarzanie profili użytkowników” na stronie 225.

Odtwarzanie powiązań obiektów z listą autoryzacji: Gdy zniszczona lista autoryzacji zostanie usunięta, obiekty zabezpieczane przez taką listę muszą być dodane do nowej listy autoryzacji. Należy wtedy wykonać następujące czynności:

1. Za pomocą komendy Odzyskiwanie pamięci (Reclaim Storage - RCLSTG) odszukaj obiekty, które były związane ze zniszczoną listą autoryzacji. Komenda Odzyskiwanie pamięci (Reclaim storage) przypisuje do listy autoryzacji QRCLAUTL obiekty, które były związane ze zniszczoną listą.
2. Za pomocą komendy Wyświetlenie listy autoryzacji (Display Authorization List Objects - DSPAUTLOBJ) wyświetl obiekty związane z listą autoryzacji QRCLAUTL.
3. Za pomocą komendy Nadanie uprawnień dla obiektu (Grant Object Authority - GRTOBJAUT) zabezpiecz każdy obiekt za pomocą poprawnej listy autoryzacji:

```
GRTOBJAUT OBJ(nazwa_biblioteki/nazwa_obiektu) +
          OBJTYPE(typ_obiektu) +
          AUTL(nazwa_listy autoryzacji)
```

Uwaga: Jeśli z listą autoryzacji QRCLAUTL związana jest duża liczba obiektów, za pomocą komendy DSPAUTLOBJ należy utworzyć zbiór bazy danych podając parametr OUTPUT(*OUTFILE). Do uruchamiania komendy GRTOBJAUT dla każdego obiektu znajdującego się w zbiorze, można napisać program CL.

Odtwarzanie systemu operacyjnego

Podczas wykonywania ręcznego IPL, menu IPL lub instalowanie systemu (IPL or Install the System) udostępnia opcję instalowania systemu operacyjnego. Funkcja narzędzi DST udostępnia możliwość wymagania od każdego używającego tego menu podania hasła ochrony narzędzi DST. Można go użyć do zabezpieczenia przed odtworzeniem nieautoryzowanej kopii systemu operacyjnego.

Aby zabezpieczyć instalację systemu operacyjnego, należy wykonać następujące czynności:

1. Wykonaj ręczne IPL.
2. Z menu IPL lub instalowanie systemu (IPL or Install the System) wybierz narzędzia DST.
3. Z menu Użycie narzędzi DST (Use DST) wybierz opcję pracy w środowisku DST.
4. Wybierz opcję zmiany hasła narzędzi DST.
5. Wybierz opcję zmiany ochrony instalacji systemu operacyjnego.
6. Podaj wartość 1 (zabezpiecz).
7. Naciśnij klawisz F3 (wyjście), aż wrócisz do menu IPL lub instalowanie systemu (IPL or Install the System).
8. Zakończ ręczne IPL i ustaw blokadę w jej normalnej pozycji.

Uwagi:

1. Jeśli instalacja systemu operacyjnego nie ma być już dłużej chroniona, należy wykonać te same czynności i podać wartość 2 (nie chroniona).
2. Instalację systemu operacyjnego można zabezpieczyć także ustawiając stacyjkę w normalnej pozycji i usuwając z niej klucz.

Uprawnienia specjalne *SAVSYS

Aby składować lub odtwarzać obiekty, użytkownik musi mieć uprawnienia *OBJEXIST do obiektu lub uprawnienia specjalne *SAVSYS. Użytkownik z uprawnieniami specjalnymi *SAVSYS nie potrzebuje żadnych dodatkowych uprawnień do składowanego lub odtwarzanego obiektu.

Uprawnienia specjalne *SAVSYS dają użytkownikowi możliwość składowania obiektu i przeniesienia go do innego systemu w celu odtworzenia lub wyświetlenia (zrzutu) nośnika, w celu przeglądania danych. Daje użytkownikowi także możliwość składowania obiektu oraz zwolnienia pamięci, a zatem usunięcia danych z obiektu. Podczas składowania dokumentów użytkownik z uprawnieniami specjalnymi *SAVSYS ma możliwość usunięcia tych dokumentów. Uprawnienia specjalne *SAVSYS powinny być nadawane ze szczególną uwagą.

Kontrola operacji składowania i odtwarzania

Jeśli wartość kontroli działania (wartość systemowa QAUDLVL lub parametr AUDLVL w profilu użytkownika) ma wartość *SAVRST, dla każdej operacji odtwarzania zapisywany jest rekord kontroli. Jeśli używana jest komenda odtwarzająca dużą liczbę obiektów, taka jak RSTLIB, rekord kontroli zapisywany jest dla każdego odtwarzanego obiektu. Może to powodować problemy z wielkością dziennika kontroli, szczególnie gdy odtwarzana jest więcej niż jedna biblioteka.

Komenda RSTCFG nie tworzy rekordu kontroli dla każdego odtwarzanego obiektu. Jeśli dla tej komendy ma być zapisany rekord kontroli, kontrolę obiektu należy ustawić dla samej komendy. Za każdym razem gdy zostanie uruchomiona ta komenda, zapisany zostanie jeden rekord kontroli.

Komendy, które składują bardzo dużą liczbę obiektów, takie jak SAVSYS, SAVSECDTA i SAVCFG, nie tworzą pojedynczych rekordów kontroli dla składowanych obiektów, nawet jeśli składowane obiekty mają aktywną opcję kontroli obiektu. Aby monitorować te komendy, kontrolę obiektu należy skonfigurować dla samych komend.

Rozdział 9. Kontrolowanie ochrony na systemie iSeries

Rozdział ten opisuje techniki kontroli efektywności ochrony w systemie. Kontrolowanie ochrony systemu może mieć kilka celów:

- określenie, czy plan ochrony jest kompletny;
- sprawdzenie, czy planowane elementy sterujące ochroną są na swoim miejscu i działają poprawnie. Kontrola tego typu jest wykonywana przez szefa bezpieczeństwa w ramach codziennych zadań administrowania ochroną. Może ona także być wykonywana, czasami w sposób bardziej szczegółowy, w ramach okresowego badania ochrony przez pracowników przedsiębiorstwa lub firmy zewnętrzne;
- sprawdzenie, czy ochrona systemu nadąża za zmianami w środowisku systemu; przykładowe zmiany, które mają wpływ na ochronę:
  - nowe obiekty tworzone przez użytkowników systemu;
  - nowi użytkownicy mający uprawnienia w systemie;
  - zmiana praw własności do obiektu (nieodpowiednie uprawnienia);
  - zmiana kompetencji (grupy, do której należy użytkownik);
  - uprawnienie tymczasowe (nieunieważnione w odpowiednim momencie);
  - zainstalowanie nowych produktów.
- przygotowanie się na zdarzenie w przyszłości, jak na przykład instalację nowej aplikacji, zmianę poziomu ochrony lub instalację sieci.

Techniki opisane w tym rozdziale dotyczą wszystkich tych sytuacji. Dobór kontrolowanych elementów oraz częstotliwość kontrolowania zależą od wielkości organizacji i potrzeb związanych z ochroną. Celem tego rozdziału jest omówienie następujących kwestii: jakie informacje są dostępne, jak je uzyskać i dlaczego są potrzebne, a nie udzielenie wskazówek dotyczących częstotliwości kontroli.

Ten rozdział składa się z trzech części:

- Lista kontrolna elementów ochrony, które można planować i kontrolować.
- Informacje o konfigurowaniu i używaniu systemowej kroniki kontroli.
- Inne techniki umożliwiające zbieranie informacji o ochronie dotyczących systemu.

Kontrola ochrony obejmuje używanie komend na systemie iSeries oraz dostęp do protokołowanych i kronikowanych informacji o systemie. Warto utworzyć specjalny profil dla osoby, która będzie wykonywała kontrolę ochrony systemu. Profil ten, aby mógł zmieniać charakterystykę kontroli w systemie, wymaga uprawnienia specjalnego *AUDIT. Niektóre z zadań kontroli zalecanych w tym rozdziale wymagają profilu użytkownika z uprawnieniami specjalnymi *ALLOBJ i *SECADM. Po zakończeniu okresu kontroli należy upewnić się, że hasło tego profilu zostało ustawione na *NONE.

Lista kontrolna dla szefów ochrony i kontrolerów

Ta lista kontrolna może być użyta zarówno do planowania, jak i do kontroli ochrony systemu. Podczas planowania ochrony z listy należy wybrać te elementy, które spełniają wymagania ochrony. Podczas kontrolowania ochrony systemu listy należy użyć do określenia kontroli oraz określenia, czy konieczna jest dodatkowa kontrola.

Ta lista służy jako przegląd informacji zawartych w tej książce. Składa się z krótkiego opisu wykonania każdego elementu oraz sposobu monitorowania, czy został wykonany, ze wskazaniem, jakich pozycji należy szukać w kronice QAUDJRN. Szczegóły dotyczące każdego elementu można znaleźć w książce.

Ochrona fizyczna

Uwaga: Temat Podstawowa ochrona systemu i jej planowanie w Centrum informacyjnym zawiera pełny opis zabezpieczeń fizycznych systemu iSeries. Więcej informacji na ten temat zawiera sekcja “Informacje wstępne i pokrewne” na stronie xvi.

System i konsola są w bezpiecznym miejscu.

Nośniki składowania zabezpieczone są przed uszkodzeniem i kradzieżą.

Ustawienie stacyjki na jednostce procesora jest w pozycji Secure lub Auto. Klucz jest wyjęty. Klucze przechowywane są osobno, oba w dobrze zabezpieczonym miejscu. Więcej informacji dotyczących stacyjki znajduje się w Centrum informacyjnym (patrz “Informacje wstępne i pokrewne” na stronie xvi, aby uzyskać szczegółowe informacje).

Dostęp do publicznych stacji roboczych i konsoli jest ograniczony. Za pomocą komendy DSPOBJAUT należy sprawdzić, kto ma uprawnienia *CHANGE do stacji roboczych. Aby odszukać próby wpisania się do zastrzeżonych stacji roboczych, w kronice kontroli należy poszukać pozycji AF z polem rodzaju obiektu równym *DEVD.

Wpisywanie się użytkowników z uprawnieniami specjalnymi *ALLOBJ lub *SERVICE jest ograniczone do kilku stacji roboczych. Należy sprawdzić, czy wartość systemowa QLMTSECOFR ustawiona jest na 1. Aby sprawdzić, czy użytkownik QSECOFR ma uprawnienia *CHANGE, dla urządzeń należy użyć komendy DSPOBJAUT.

Wartości systemowe

Wartości systemowe ochrony spełniają zalecane wskazówki. Aby wydrukować wartości systemowe ochrony, należy wpisać: WRKSYSVAL *SEC OUTPUT(*PRINT). Dwie ważne wartości systemowe do kontrolowania to:

- QSECURITY, która powinna mieć wartość 40 lub większą,
- QMAXSIGN, która nie powinna być większa niż 5.

Uwaga: Jeśli funkcja kontroli jest aktywna, w kronice QAUDJRN zapisywana jest pozycja SV, za każdym razem gdy zmieniana jest wartość systemowa.

Decyzje dotyczące wartości systemowych są przeglądane okresowo, szczególnie podczas zmian środowiska systemu, takich jak instalowanie nowych aplikacji lub sieci komunikacyjnych.

Profile użytkowników dostarczane przez IBM

Hasło dla profilu użytkownika QSECOFR zostało zmienione. Hasło domyślne tego profilu ma wartość QSECOFR, aby można było zainstalować system. Hasło **musi** być zmienione podczas pierwszego wpisywania się do systemu, a także okresowo po zainstalowaniu.

Należy sprawdzić, czy hasło zostało zmienione, sprawdzając listę DSPAUTUSR pod kątem daty zmiany hasła QSECOFR oraz próbując wpisać się za pomocą hasła domyślnego.

Uwaga: Więcej informacji dotyczących profili użytkowników IBM zawiera sekcja “Profile użytkowników IBM” na stronie 110 i Dodatek B.

Hasła IBM dla narzędzi DST zostały zmienione. Profile DST nie pojawiają się na liście DSPAUTUSR. Aby sprawdzić, czy identyfikatory użytkowników oraz hasła zostały zmienione, należy uruchomić narzędzia DST i spróbować użyć wartości domyślnych. Więcej informacji na ten temat zawiera sekcja “Praca z identyfikatorami użytkowników narzędzi serwisowych” na stronie 111.

Wpisywanie się za pomocą profili użytkowników IBM, z wyjątkiem QSECOFR, nie jest zalecane. Te profile użytkowników IBM zaprojektowane zostały do posiadania obiektów lub uruchamiania funkcji systemowych. Za pomocą listy DSPAUTUSR należy sprawdzić, czy wymienione poniżej profile użytkowników IBM mają hasła o wartości *NONE:

| QAUTPROF
| QBRMS
| QCLUMGT
| QCLUSTER
| QCOLSRV
| QDBSHR
| QDBSHRDO
| QDFTOWN
| QDIRSRV
| QDLFM
| QDOC
| QDSNX
| QEJB
| QFNC
| QGATE
| QIPP
| QLPAUTO
| QLPINSTALL
| QMGTC
| QMSF
| QNETSPLF
| QNFSANON
| QNTP
| QPEX
| QPGMR
| QPM400
| QRJE
| QSNADS
| QSPL
| QSPLJOB
| QSRV
| QSRVAGT
| QSRVBAS
| QSYS
| QSYSOPR
| QTCM
| QTCP
| QTFTP
| QTMHHTP1
| QTMHHTTP
| QTSTRQS
| QUSER
| QYCMCIMOM
| QYPSJSVR

Kontrola hasła

Użytkownicy mogą zmieniać własne hasła. Umożliwienie użytkownikom definiowania własnych haseł zmniejsza potrzebę zapisywania haseł użytkowników na kartkach. Użytkownicy powinni mieć dostęp do komendy CHGPWD lub funkcji Zmiana hasła (Change Password) z menu Ochrona (GO SECURITY).

Wymagania dotyczące zmiany hasła są określone przez wytyczne dotyczące ochrony w organizacji. Wartość systemowa QPWDEXPITV ustawiana jest zgodnie z tymi zasadami ochrony.

Jeśli profil użytkownika ma okres ważności hasła inny niż wartość systemowa, spełnia wskazówki ochrony. Należy przejrzeć profile i sprawdzić, czy wartość PWDEXPITV jest inna niż *SYSVAL.

Przed trywialnymi hasłami zabezpiecza wartość systemowa oraz program zatwierdzania hasła, które ustanawiają reguły hasła. Należy użyć komendy WRKSYSVAL *SEC i sprawdzić ustawienia dla wartości rozpoczynających się od znaków QPWD.

Profile grupowe mają hasła o wartości *NONE. Do sprawdzania, czy jakieś profile grupowe mają hasła, należy użyć komendy DSPAUTUSR.

Jesli poziom obsługi haseł w systemie ma wartość inną niż 3, a użytkownicy zmieniają swoje hasło, jeśli jest to możliwe, system próbuje utworzyć równoważne hasło, którego można będzie użyć na innych poziomach obsługi haseł. Aby sprawdzić, które profile użytkowników mają hasła, których można używać na różnych poziomach obsługi haseł, należy użyć komendy PRTUSRPRF TYPE(*PWDLVL).

Uwaga: Równoważne hasło jest najlepszą próbą utworzenia hasła możliwego do użycia na innych poziomach obsługi haseł, ale po zmianie poziomu obsługi haseł może ono nie przejść przez wszystkie reguły tworzenia hasła. Na przykład jeśli na poziomie hasła 2 podano hasło BbAaA3x, system utworzy równoznaczne hasło - BBAAA3X, które może być użyte na poziomach 0 i 1. Będzie to możliwe, nawet jeśli wartość systemowa QPWDLMTCHR określa znak ″A″ jako znak zastrzeżony (na poziomie hasła 2 wartość QPWDLMTCHR nie jest narzucana) lub wartość systemowa QPWDLMTREP określa, że kolejne znaki nie mogą być takie same (ponieważ na poziomie hasła 2 jest rozróżnianie wielkości liter, ale na poziomach 0 i 1 nie).

Profile użytkowników i grupowe

Każdy użytkownik ma przypisany unikalny profil użytkownika. Wartość systemowa QLMTDEVSSN powinna być ustawiona na 1. Ograniczanie każdego użytkownika do jednej sesji urządzenia w danym momencie nie zapobiega współużytkowaniu profili użytkowników, ale ogranicza je.

Profile użytkowników z uprawnieniami specjalnymi *ALLOBJ są ograniczone i nie są używane jako profile grupowe. Komenda DSPUSRPRF może być użyta do sprawdzania uprawnień specjalnych dla profili użytkowników oraz do określania, które profile są profilami grupowymi. Temat “Drukowanie wybranych profili użytkowników” na stronie 269 opisuje sposób używania w tym celu zbioru wyjściowego oraz zapytania.

Pole *Ograniczenie możliwości* ma wartość *YES w profilach użytkowników, którzy powinni być ograniczeni do zestawu menu. Sposób określania, czy tak jest, opisuje temat “Drukowanie wybranych profili użytkowników” na stronie 269.

Programiści nie mają dostępu do bibliotek produkcyjnych. Za pomocą komendy DSPOBJAUT można określić uprawnienia publiczne oraz prywatne do bibliotek produkcyjnych oraz obiektów krytycznych w bibliotekach.

Więcej informacji dotyczących ochrony oraz środowiska programistycznego zawiera sekcja “Planowanie ochrony dla programistów” na stronie 220.

Gdy zmieniają się obowiązki zadań, zmieniane jest członkostwo w profilu grupowym. Aby sprawdzić członkostwo w grupie, należy użyć jednej z następujących komend:

```
DSPAUTUSR SEQ(*GRPPRF)
DSPUSRPRF nazwa_profilu *GRPMBR
```

Dla profili grupowych powinna być używana konwencja nazewnictwa. Dzięki temu po wyświetleniu uprawnień można łatwo rozpoznać profil grupowy.

Administracja profilami użytkowników jest zorganizowana odpowiednio. Żaden z profili użytkowników nie ma dużej liczby uprawnień prywatnych. Omówienie odszukiwania oraz sprawdzania dużych profili użytkowników w systemie zawiera temat “Badanie dużych profili użytkowników” na stronie 270.

Pracownicy usuwani są z systemu natychmiast po ich przeniesieniu lub zwolnieniu. Listę DSPAUTUSR należy przeglądać regularnie, aby upewnić się, że dostęp do systemu mają jedynie aktywni pracownicy. Aby upewnić się, że profile użytkowników są usuwane natychmiast po odejściu pracowników, można przejrzeć pozycję DO (usunięcie obiektu) w kronice kontroli.

Menedżerowie regularnie sprawdzają uprawnienia użytkowników do systemu. Aby uzyskać te informacje, należy użyć komendy DSPAUTUSR.

Hasło dla nieaktywnego pracownika ustawione jest na *NONE. Aby sprawdzić, czy nieaktywne profile użytkowników nie mają haseł, należy użyć komendy DSPAUTUSR.

Menedżerowie regularnie sprawdzają użytkowników z uprawnieniami specjalnymi, a w szczególności z uprawnieniami *ALLOBJ, *SAVSYS i *AUDIT. Sposób określania, czy tak jest, opisuje temat “Drukowanie wybranych profili użytkowników” na stronie 269.

Kontrola autoryzacji

Właściciele danych rozumieją swoje zobowiązanie do autoryzowania użytkowników na podstawie wiedzy.

Właściciele obiektów regularnie sprawdzają uprawnienia do używania obiektów, także uprawnienia publiczne. Komenda WRKOBJOWN udostępnia ekran do pracy z uprawnieniami do wszystkich obiektów, których właścicielem jest profil użytkownika.

Wrażliwe dane nie są publiczne. Za pomocą komendy DSPOBJAUT należy sprawdzić uprawnienia dla użytkownika *PUBLIC do obiektów krytycznych.

Uprawnienia do profili użytkowników są kontrolowane. Uprawnienia publiczne do profili użytkowników powinny mieć wartość *EXCLUDE. Zapobiega to wprowadzaniu zadań, które uruchamiane są pod kontrolą innego profilu użytkownika.

Kontrolowane są opisy zadań:

– Opisy zadań z uprawnieniami publicznymi *USE lub większymi zostały określone jako USER(*RQD). Oznacza to, że zadania wprowadzone za pomocą opisu zadania muszą być uruchamiane za pomocą profilu wprowadzającego.
– Opisy zadań podające użytkownika mają uprawnienia publiczne *EXCLUDE. Autoryzacja do korzystania z tych opisów zadań jest kontrolowana. Zapobiega to wprowadzaniu zadań, które działają z uprawnieniami innego profilu, przez nieuprawnionych użytkowników.

Aby sprawdzić, jakie opisy zadań znajdują się w systemie, należy wpisać:

```
DSPOBJD OBJ(*ALL/*ALL) OBJTYPE(*JOBD) ASPDEV(*ALLAVL) OUTPUT(*PRINT)
```

Aby sprawdzić parametr *Użytkownik* w opisie zadania, należy użyć komendy Wyświetlenie opisu zadania (Display Job Description - DSPJOBD). Aby sprawdzić uprawnienia do opisu zadania, należy użyć komendy DSPOBJAUT.

Uwaga: Na poziomie ochrony 40 lub 50, użytkownik wprowadzający opis zadania, w którym podano nazwę profilu, musi mieć uprawnienia *USE zarówno do opisu zadania, jak i do profilu użytkownika. Na wszystkich poziomach ochrony, próba wprowadzenia lub ustalenia harmonogramu zadania bez uprawnień *USE do użytkownika podanego w opisie zadania, powoduje powstanie w kronice kontroli pozycji AF z typem naruszenia J.

Użytkownicy nie są uprawnieni do wpisywania się przez naciśnięcie klawisza Enter na ekranie Wpisanie Się (Sign On). Należy upewnić się, że żadna pozycja stacji roboczej w opisach podsystemów nie podaje opisu zadania, w którym dla parametru USER podano nazwę profilu użytkownika.

Domyślnie wpisanie się jest zablokowane na poziomie ochrony 40 lub 50, nawet jeśli opis podsystemu zezwala na takie działanie. Na wszystkich poziomach ochrony, próba domyślnego wpisania się, gdy zezwala na to opis podsystemu, powoduje zapisanie w kronice kontroli pozycji AF z typem naruszenia S.

Lista bibliotek aplikacji jest kontrolowana w celu zapobiegnięcia dołączeniu biblioteki, która zawiera podobny program, przed bibliotekami produkcyjnymi. Metody kontrolowania listy bibliotek omawia temat “Listy bibliotek” na stronie 187.

Programy adoptujące uprawnienia używane są tylko wtedy, gdy są wymagane, i są uważnie kontrolowane. Wyjaśnienie sposobu użycia funkcji adoptowania zawiera temat “Analizowanie programów adoptujących uprawnienia” na stronie 270.

Interfejsy API zostały zabezpieczone.

W celu uniknięcia problemów związanych z wydajnością, używane są dobre techniki ochrony.

Dostęp bez uprawnień

Gdy aktywna jest funkcja kontroli, w kronice kontroli ochrony (QAUDJRN) protokołowane są zdarzenia związane z ochroną. Aby kontrolować błędy uprawnień, należy użyć następujących wartości systemowych oraz ustawień:

- wartość QAUDCTL musi być ustawiona na *AUDLVL,
- wartość QAUDLVL musi zawierać wartości *PGMFAIL i *AUTFAIL.

Najlepszą metodą wykrywania nieautoryzowanych prób dostępu do informacji jest regularne przeglądanie pozycji w kronice kontroli.

Wartość systemowa QMAXSIGN ogranicza liczbę kolejnych niepoprawnych prób wpisywania się do pięciu lub mniej. Wartość systemowa QMAXSGNACN ustawiona jest na 2 lub 3.

Utworzona została kolejka komnikatów QSYSMSG, która jest monitorowana.

Kronika kontroli kontrolowana jest pod kątem powtórzonych prób użytkownika. (Błędy autoryzacji powodują zapisanie w kronice kontroli pozycji typu AF.)

Podczas próby dostępu do obiektów za pomocą nieobsługiwanych interfejsów działanie programu nie powiedzie się. (Wartość systemowa QSECURITY ustawiona jest na 40 lub 50.)

Do wpisania się wymagany jest identyfikator użytkownika i hasło. Narzucają to poziomy ochrony 40 i 50. Na poziomie 20 lub 30, użytkownik musi zapewnić, że żadne opisy podsystemów nie mają pozycji stacji roboczej, które używają opisu zadania z podaną nazwą profilu użytkownika.

Nieautoryzowane programy

Wartość systemowa QALWOBJRST ustawiona jest na *NONE, aby zapobiec odtwarzaniu w systemie programów wrażliwych na ochronę.

Komenda Sprawdzenie integralności obiektu (Check Object Integrity - CHKOBJITG) uruchamiana jest okresowo w celu wykrywania nieautoryzowanych zmian w obiektach programu. Ta komenda została opisana w sekcji “Sprawdzanie obiektów, które zostały zmienione” na stronie 271.

Komunikacja

Komunikacja telefoniczna zabezpieczana jest przez procedury oddzwaniania.

Dla wrażliwych danych stosowane jest szyfrowanie.

Zdalne wpisywanie się jest kontrolowane. Wartość systemowa QRMTSIGN ustawiona jest na *FRCSIGNON lub używany jest program sprawdzania tranzytu.

Dostęp do danych z innych systemów, także z komputerów osobistych, kontrolowany jest za pomocą atrybutów sieciowych JOBACN, PCSACC i DDMACC. Atrybut sieciowy JOBACN powinien mieć wartość *FILE.

Używanie kroniki kontroli ochrony

Kronika kontroli ochrony jest podstawowym źródłem informacji o kontroli dotyczących systemu. Kontroler ochrony w lub poza organizacją może użyć funkcji kontroli udostępnianej przez system, aby zebrać informacje dotyczące zdarzeń związanych z ochroną, które wystąpiły w systemie.

Kontrolę systemu można zdefiniować na trzech różnych poziomach:

- kontrola systemu, która dotyczy wszystkich użytkowników,
- kontrola, która dotyczy określonych obiektów,
- kontrola, która dotyczy określonych użytkowników.

Do definiowania kontroli używane są wartości systemowe, parametry profilu użytkownika oraz parametry obiektu. Sekcja “Planowanie kontroli ochrony” opisuje sposób wykonania tego zadania.

Gdy wystąpi zdarzenie związane z ochroną, które może być kontrolowane, system sprawdza, czy użytkownik wybrał, że to zdarzenie ma być kontrolowane. Jeśli tak, w bieżącym dzienniku dla kroniki kontroli ochrony (kronika QAUDJRN w bibliotece QSYS) zapisuje pozycję kroniki.

Aby przeanalizować informacji kontroli zebrane w kronice QAUDJRN, należy użyć komendy Wyświetlenie kroniki (Display Journal - DSPJRN). Za pomocą tej komendy, informacje z kroniki QAUDJRN można zapisać w zbiorze bazy danych. Do przeanalizowania danych można użyć programu lub narzędzia zapytań.

Funkcja kontroli ochrony jest opcjonalna. Aby skonfigurować kontrolę ochrony, należy wykonać kilka określonych czynności.

Przedstawione poniżej sekcje opisują sposób planowania, konfigurowania i zarządzania kontrolą ochrony oraz informują, jakie informacje są zapisywane i jak je przeglądać. Dodatek F pokazuje układy rekordów dla pozycji kroniki kontroli. Dodatek E opisuje, jakie operacje są kontrolowane dla każdego rodzaju obiektu.

Planowanie kontroli ochrony

Aby zaplanować użycie kontroli ochrony, należy:

- określić, jakie zdarzenia związane z ochroną mają być zapisywane dla wszystkich użytkowników systemu; kontrola zdarzeń związanych z ochroną nazywana jest **kontrolą działania**,
- sprawdzić, czy dla określonych użytkowników potrzebna jest dodatkowa kontrola,
- zadecydować, czy ma być kontrolowane użycie określonych obiektów,
- określić, czy kontrolowanie obiektu powinno być przeprowadzane dla wszystkich użytkowników, czy dla niektórych.

Planowanie kontroli działania

Wartość systemowa QAUDCTL (sterowanie kontrolą), wartość systemowa QAUDLVL (poziom kontroli), wartość systemowa QAUDLVL2 (rozszerzenie poziomu kontroli) oraz parametr AUDLVL (kontrola działania) w profilu użytkownika, współpracują ze sobą w celu sterowania kontrolą działania:

- wartość systemowa QAUDLVL określa, które działania kontrolowane są dla wszystkich użytkowników w systemie,
- wartość systemowa QAUDLVL2 także określa, które działania kontrolowane są dla wszystkich użytkowników w systemie i jest używana, gdy wymaganych jest więcej niż 16 wartości kontroli,
- parametr AUDLVL w profilu użytkownika określa, które działania są kontrolowane w przypadku danego użytkownika; wartości dla parametru AUDLVL stosowane są *dodatkowo*, oprócz wartości systemowych QAUDLVL i QAUDLVL2,
- wartość systemowa QAUDCTL uruchamia i zatrzymuje kontrolę działania.

To, które zdarzenia zostaną wybrane do protokołowania, zależy od celów ochrony i potencjalnego ryzyka. Tabela 125 opisuje możliwe wartości poziomu kontroli oraz sposób ich użycia. Informuje także, czy są to wartości systemowe, parametry profilu użytkownika, czy oba jednocześnie.

Tabela 126 na stronie 243 udostępnia więcej informacji dotyczących pozycji kroniki, które zapisywane są dla wartości kontroli działania, podanych dla wartości systemowych QAUDLVL i QAUDLVL2 oraz w profilu użytkownika. Pokazuje:

- typ pozycji zapisywanej w kronice QAUDJRN,
- modelowy zbiór wyjściowy bazy danych, który może być użyty do definiowania rekordu podczas tworzenia zbioru wyjściowego za pomocą komendy DSPJRN; pełny układ dla modelowych zbiorów wyjściowych bazy danych zawiera Dodatek F,
- szczegółowy typ pozycji; niektóre typy pozycji używane są do protokołowania więcej niż jednego typu zdarzeń; szczegółowe pole typu pozycji w pozycji kroniki definiuje typ zdarzenia,
- identyfikator komunikatu, który może być użyty do definiowania informacji specyficznych dla pozycji w pozycji kroniki.

Tabela 125. Wartości kontroli działania

Możliwa wartość	Dostępna dla wartości systemowych QAUDLVL i QAUDLVL2	Dostępna dla komendy CHGUSRAUD	Opis
*NONE	Tak	Tak	Jeśli wartość systemowa QAUDLVL ma wartość *NONE, nie są protokołowane żadne działania dla całego systemu. Działania protokołowane są dla pojedynczych użytkowników w oparciu o wartość parametru AUDLVL w ich profilach użytkowników. Jeśli wartość parametru AUDLVL dla profilu użytkownika jest równa *NONE, dla tego użytkownika nie jest przeprowadzana żadna dodatkowa kontrola działania. Dla tego użytkownika protokołowane są wszystkie działania podane w wartości systemowej QAUDLVL.
*AUTFAIL	Tak	Nie	**Błędy uprawnień**: protokołowane są nieudane próby wpisania się do systemu oraz przy dostępie do obiektów. Wartość *AUTFAIL może być używana regularnie do monitorowania użytkowników próbujących wykonać w systemie nieautoryzowane funkcje. Może być użyta także do asystowania podczas migracji do wyższego poziomu ochrony oraz testowania ochrony zasobów dla nowych aplikacji.
*CMD	Nie	Tak	**Komendy**: system protokołuje łańcuchy komend uruchamiane przez użytkownika. Jeśli komenda uruchamiana jest z poziomu programu CL, który utworzony został z parametrem LOG(*NO) i ALWRTVSRC(*NO), protokołowana jest jedynie nazwa komendy oraz biblioteki. Wartość *CMD może być używana do zapisywania działań poszczególnych użytkowników, takich jak szef ochrony.
*CREATE	Tak	Tak	**Tworzenie obiektów**: system zapisuje pozycję kroniki, gdy tworzony jest nowy lub zastępujący obiekt. Wartość *CREATE może być użyta do monitorowania, gdy programy są tworzone lub ponownie kompilowane.
*DELETE	Tak	Tak	**Usuwanie obiektów**: system zapisuje pozycję kroniki, gdy usuwany jest obiekt.

Tabela 125. Wartości kontroli działania (kontynuacja)

Możliwa wartość	Dostępna dla wartości systemowych QAUDLVL i QAUDLVL2	Dostępna dla komendy CHGUSRAUD	Opis
*JOBDTA	Tak	Tak	**Zadania**: protokołowane są działania wpływające na zadanie, takie jak uruchomienie lub zatrzymanie zadania, wstrzymanie go, zwolnienie, anulowanie lub zmiana. Wartość *JOBDTA może być użyta do monitorowania, kto uruchamia zadania wsadowe.
*NETBAS,	Tak	Nie	**Podstawowe funkcje sieci**: działania dla reguł IP, połączenia przez gniazda, filtru przeszukiwania katalogów APPN, filtr zakończenia APPN.
*NETCLU,	Tak	Nie	**Działania klastra lub grupy zasobów klastra**: pozycja kroniki kontroli jest zapisywana, gdy wystąpią następujące zdarzenia: • dodawanie, tworzenie lub usuwanie węzła klastra lub grupy zasobów klastra, • uruchamianie, kończenie, aktualizowanie lub usuwanie węzła klastra lub grupy zasobów klastra, • wystąpi automatyczna awaria systemu, która przełącza dostęp do innego systemu, • dostęp przełączany jest ręcznie z jednego systemu w klastrze do innego.
*NETCMN	Tak	Nie	**Kontrola komunikacji sieciowej**: naruszenia wykryte przez obsługę filtru APPN są protokołowane w kronice kontroli ochrony, gdy są kontrolowane: filtr wyszukiwania ktalogu i filtr punktu końcowego. Parametr *NETCMN składa się z kilku wartości umożliwiających lepsze dostosowanie kontroli. Na parametr *NETCMN składają się następujące wartości: *NETBAS, *NETCLU, *NETFAIL, *NETSCK.
*NETFAIL,	Tak	Nie	**Awarie sieci**: pozycja kroniki kontroli zapisywana jest, gdy następuje próba połączenia z portem TCP/IP, który nie istnieje lub następuje próba wysłania informacji do portu TCP/IP, który nie jest otwarty lub dostępny.
*NETSCK.	Tak	Nie	**Zadania gniazda**: pozycja kroniki kontroli zapisywana jest, gdy wystąpią następujące zdarzenia: • zaakceptowane zostanie przychodzące połączenie przez gniazdo TCP/IP, • ustanowione zostanie wychodzące połączenie przez gniazdo TCP/IP, • adres IP zostanie przypisany przez protokół DHCP (Dynamic Host Configuration Protocol), • adres IP nie może być przypisany przez protokół DHCP, ponieważ wszystkie adresy IP są używane, • poczta została przefiltrowana lub odrzucona.
*OBJMGT	Tak	Tak	**Zadania zarządzania obiektem**: protokołowane jest przenoszenie obiektu do innej biblioteki lub zmiana jego nazwy. Wartość *OBJMGT może być użyta do wykrywania kopiowania poufnych informacji przez przenoszenie obiektu do innej biblioteki.

Tabela 125. Wartości kontroli działania (kontynuacja)

Możliwa wartość	Dostępna dla wartości systemowych QAUDLVL i QAUDLVL2	Dostępna dla komendy CHGUSRAUD	Opis
*OPTICAL	Tak	Tak	**Funkcje optyczne**: kontrolowane są wszystkie funkcje optyczne, w tym funkcje związane ze zbiorami optycznymi, katalogami optycznymi, woluminami optycznymi oraz kasetami optycznymi. Wartość *OPTICAL może być użyta do wykrywania prób utworzenia lub usunięcia katalogu optycznego.
*PGMADP	Tak	Tak	**Adoptowanie uprawnień**: system zapisuje pozycję kroniki, gdy przy dostępie do obiektu używane są uprawnienia adoptowane. Wartość *PGMADP może być użyta do testowania, gdzie i jak nowa aplikacja używa uprawnień adoptowanych.
*PGMFAIL	Tak	Nie	**Awarie programu**: system zapisuje pozycję kroniki, gdy program powoduje błąd integralności. Wartość *PGMFAIL może być użyta do asystowania podczas migracji do wyższego poziomu ochrony lub do testowania nowej aplikacji.
*PRTDTA	Tak	Nie	**Funkcje drukowania**: protokołowane jest drukowanie zbioru buforowego, drukowanie bezpośrednio z programu lub wysyłanie zbioru buforowego do zdalnej drukarki. Wartość *PRTDTA może być użyta wykrywania drukowania poufnych informacji.
*SAVRST	Tak	Tak	**Operacje odtwarzania**: wartość *SAVRST może być użyta do wykrywania prób odtwarzania nieautoryzowanych obiektów.
*SECCFG,	Tak	Nie	**Konfiguracja ochrony**: pozycja kroniki kontroli jest zapisywana, gdy wystąpią następujące zdarzenia: • tworzenie, zmiana, usuwanie lub odtwarzanie profilu użytkownika, • Wprowadzanie zmian w programach, wartościach systemowych, routingu podsystemu lub atrybutach kontroli, • resetowanie hasła użytkownika QSECOFR do wartości domyślnej, • ustawienie hasła szefa ochrony narzędzi serwisowych na wartość domyślną.
*SECDIRSRV,	Tak	Nie	**Funkcje usług katalogowych**: pozycja kroniki kontroli zapisywana jest, gdy wystąpią następujące zdarzenia: • w kontroli, uprawnieniach, hasłach i prawie własności wprowadzane są zmiany, • następuje pomyślne konsolidowanie i odłączanie.
*SECIPC,	Tak	Nie	**Komunikacja międzyprocesorowa**: pozycja kroniki kontroli zapisywana jest, gdy wystąpią następujące zdarzenia: • wprowadzanie zmian w prawach własności lub uprawnieniach obiektu IPC, • tworzenie, usuwanie lub pobieranie obiektu IPC, • podłączanie pamięci współużytkowanej.

Tabela 125. Wartości kontroli działania (kontynuacja)

Możliwa wartość	Dostępna dla wartości systemowych QAUDLVL i QAUDLVL2	Dostępna dla komendy CHGUSRAUD	Opis
*SECNAS,	Tak	Nie	**Działania usługi uwierzytelniania sieciowego**: pozycja kroniki kontroli zapisywana jest, gdy wystąpią następujące zdarzenia: • Niepoprawny bilet usług. • Niezgodne jednostki główne usługi. • Niezgodne jednostki główne klienta • Niezgodność adresu IP biletu. • deszyfrowanie biletu nie powiedzie się, • deszyfrowanie uwierzytelniania nie powiedzie się, • dziedzina nie znajduje się w kliencie i dziedzinach lokalnych, • bilet jest próbą utworzenia odpowiedzi, • bilet nie jest jeszcze ważny, • niezgodny jest zdalny lub lokalny adres IP, • wystąpi błąd sumy kontrolnej deszyfrowania KRB_AP_PRIV lub KRB_AP_SAFE, • w przypadku KRB_AP_PRIV lub KRB_AP_SAFE wystąpi: błąd datownika, błąd odpowiedzi lub błąd kolejności sekwencji, • w przypadku akceptacji GSS wystąpią: wygasłe uprawnienia, błąd sumy kontrolnej lub konsolidacje kanału, • w przypadku odpakowania lub weryfikacji GSS wystąpią: wygasły kontekst, odszyfrowanie/dekodowanie, błąd sumy kontrolnej lub błąd kolejności.
*SECRUN,	Tak	Nie	**Funkcje wykonawcze ochrony**: w kronice kontroli zapisywane są zmiany praw własności, uprawnień oraz grup podstawowych.
*SECSCKD,	Tak	Nie	**Opisy gniazda**: pozycja kroniki kontroli zapisywana jest, gdy wystąpią następujące zdarzenia: • deskryptor gniazda nadany zostanie innemu zadaniu, • odebrany zostanie deskryptor gniazda, • deskryptor gniazda jest nie do użycia.
*SECVFY,	Tak	Nie	**Funkcje sprawdzania**: pozycja kroniki kontroli zapisywana jest, gdy wystąpią następujące zdarzenia: • wygenerowany zostanie uchwyt profilu lub znacznik, • Wszystkie znaczniki profilu zostały unieważnione. • wygenerowana zostanie maksymalna liczba znaczników profilu, • Wszystkie znaczniki profilu dla użytkownika zostały usunięte. • profil użytkownika zostanie uwierzytelniony, • podczas sesji tranzytu zostanie zmieniony profil docelowy.

Tabela 125. Wartości kontroli działania (kontynuacja)

Możliwa wartość	Dostępna dla wartości systemowych QAUDLVL i QAUDLVL2	Dostępna dla komendy CHGUSRAUD	Opis
*SECVLDL.	Tak	Nie	**Operacje listy sprawdzania**: pozycja kroniki kontroli zapisywana jest, gdy wystąpią następujące zdarzenia: • pozycja listy sprawdzania zostanie dodana, zmieniona, usunięta lub odnaleziona, • weryfikacja pozycji listy sprawdzania powiedzie się lub nie powiedzie.
*SECURITY	Tak	Tak	**Zadania ochrony**: protokołowane są zdarzenia dotyczące ochrony, takie jak zmiana profilu użytkownika lub wartości systemowej. Wartość *SECURITY może być użyta do zapisywania całej aktywności ochrony. Parametr *SECURITY składa się z kilku wartości umożliwiających lepsze dostosowanie kontroli. Na parametr *SECURITY składają się następujące wartości: *SECCFG, *SECDIRSRV, *SECIPC, *SECNAS, *SECRUN, *SECSCKD, *SECVFY, *SECVLDL.
*SERVICE	Tak	Tak	**Zadania serwisu**: protokołowane jest użycie narzędzi serwisowych, takich jak DMPOBJ (Zrzut obiektu - Dump Object) i STRCPYSCN (Uruchomienie kopiowania ekranu - Start Copy Screen). Wartość *SERVICE może być użyta do wykrywania prób obejścia ochrony za pomocą narzędzi serwisowych.
*SPLFDTA	Tak	Tak	**Operacje na zbiorach buforowych**: protokołowane są działania wykonywane na zbiorach buforowych, takie jak tworzenie, kopiowanie lub wysyłanie. Wartość *SPLFDTA może być użyta do wykrywania prób drukowania lub wysyłania poufnych danych.
*SYSMGT	Tak	Tak	**Zadania zarządzania systemem**: system zapisuje pozycję kroniki dla czynności zarządzania systemem, jak zmienianie listy odpowiedzi lub harmonogramu wł./wył. Wartość *SYSMGT może być używana do wykrycia prób użycia funkcji zarządzania systemem w celu obejścia kontroli ochrony.

Tabela 126. Pozycje kroniki kontroli ochrony

Działanie lub wartość kontroli obiektu	Typ pozycji kroniki	Plik zewnętrzny bazy danych modelu	Pozycja szczegółowa	Opis
Kontrola działania:				

Tabela 126. Pozycje kroniki kontroli ochrony (kontynuacja)

Działanie lub wartość kontroli obiektu	Typ pozycji kroniki	Plik zewnętrzny bazy danych modelu	Pozycja szczegółowa	Opis
*AUTFAIL [1]	AF	QASYAFJE/J4/J5	A	Próba dostępu do obiektu lub wykonania działania, do którego użytkownik nie był uprawniony.
	X1	QASYX1J5	F	Delegowanie znacznika tożsamości nie powiodło się
			U	Pobranie użytkownika z znacznika tożsamości nie powiodło się
			F	Błąd autoryzacji ICAPI
			G	Błąd uwierzytelniania ICAPI
			H	Skanowanie programu obsługi wyjścia
			J	Próba wprowadzenia lub ustalenia harmonogramu dla zadania z opisu zadania, w którym podano profil użytkownika. Użytkownik wprowadzający nie miał uprawnień *USE.
			N	znacznik profilu nie jest znacznikiem możliwym do regeneracji
			P	Próba użycia uchwytu profilu, który nie jest poprawny dla funkcji API QWTSETP.
			S	Próba wpisania się bez podawania identyfikatora użytkownika lub hasła.
			T	Brak uprawnień do portu TCP/IP
			U	Żądanie uprawnień użytkownika nie było poprawne.
			V	znacznik profilu nie jest poprawny do generowania nowego znacznika profilu
			W	znacznik profilu nie jest poprawny dla funkcji przełączania
			Y	Brak uprawnień do bieżącego pola JUID podczas wykonywania operacji usuwania zawartości pola JUID
			Z	Brak uprawnień do bieżącego pola JUID podczas wykonywania operacji ustawiania pola JUID
	CV	QASYCVJ4/J5	E	Połączenie zakończone niepoprawnie
	DI	QASYDIJ4/J5	AF	Błędy uprawnień
			PW	Błędy hasła
			R	Połączenie odrzucone
	GR	QASYGRJ4/J5	F	Działania rejestrowania funkcji.
	KF	QASYKFJ4/J5	P	Wprowadzono niepoprawne hasło.
	IP	QASYIPJE/J4/J5	F	Błąd uprawnień dla żądania IPC.
	PW	QASYPWJE/J4/J5	A	Połączenie APPC nie powiodło się.
			D	Wprowadzono niepoprawną nazwę użytkownika narzędzi DST.
			E	Wprowadzono niepoprawne hasło dla narzędzi DST.
			P	Wprowadzono niepoprawne hasło.
			U	Nazwa użytkownika jest niepoprawna
			X	Użytkownik narzędzi serwisowych został zablokowany
			Y	Użytkownik narzędzi serwisowych jest niepoprawny

Tabela 126. Pozycje kroniki kontroli ochrony (kontynuacja)

Działanie lub wartość kontroli obiektu	Typ pozycji kroniki	Plik zewnętrzny bazy danych modelu	Pozycja szczegółowa	Opis
			Z	Hasło dla narzędzi serwisowych jest niepoprawne
	VO	QASYVOJ4/J5	U	Sprawdzanie pozycji listy weryfikacji nie powiodło się.
	VC	QASYVCJE/J4/J5	R	Połączenie zostało odrzucone z powodu niepoprawnego hasła.
	VN	QASYVNJE/J4/J5	R	Logowanie w sieci zostało odrzucone z powodu utraty ważności konta, niepoprawnych godzin, niepoprawnego identyfikatora użytkownika lub niepoprawnego hasła.
	VP	QASYVPJE/J4/J5	P	Użyto niepoprawnego hasła sieciowego.
*CMD [2]	CD	QASYCDJE/J4/J5	C	Uruchomiono komendę.
			L	Uruchomiono instrukcję języka CL S/36E.
			O	Uruchomiono komendę sterowania operatora S/36E.
			P	Uruchomiono procedurę S/36E.
			S	Uruchomiono komendę po podstawieniu komendy.
			U	Uruchomiono program narzędziowy instrukcji sterującej S/36E.
*CREATE [3]	CO	QASYCOJE/J4/J5	N	Tworzenie nowego obiektu, z wyjątkiem tworzenia obiektów w bibliotece QTEMP.
			R	Wymiana istniejącego obiektu.
	DI	QASYDIJ4/J5	CO	Tworzenie obiektu
*DELETE [3]	DO	QASYDOJE/J4/J5	A	Obiekt został usunięty
			C	Zatwierdzenie usunięcia w toku
			D	Wycofanie tworzenia w toku
			P	Usuwanie w toku
			R	Wycofanie usuwania w toku
	DI	QASYDIJ4/J5	DO	Usunięcie obiektu
*JOBDTA	JS	QASYJSJE/J4/J5	A	Użyto komendy ENDJOBABN.
			B	Wprowadzono zadanie.
			C	Zmieniono zadanie.
			E	Zakończono zadanie.
			H	Wstrzymano zadanie.
			I	Odłączono zadanie.
			M	Zmiana profilu lub profilu grupowego.
			N	Użyto komendy ENDJOB.
			P	Żądanie uruchomienia programu zostało dołączone do zadania prestartu.
			Q	Zmieniono atrybuty zapytania.
			R	Zwolniono wstrzymane zadanie.
			S	Uruchomiono zadanie.
			T	Zmiana profilu lub profilu grupowego przy użyciu tokenu profilu.
			U	Komenda CHGUSRTRC
	SG	QASYSGJE/J4/J5	A	Przetwarzanie asynchronicznego sygnału OS/400.
			P	Asynchroniczny sygnał środowiska PASE (Private Address Space Environment)został przetworzony.

Tabela 126. Pozycje kroniki kontroli ochrony (kontynuacja)

Działanie lub wartość kontroli obiektu	Typ pozycji kroniki	Plik zewnętrzny bazy danych modelu	Pozycja szczegółowa	Opis
	VC	QASYVCJE/J4/J5	S	Uruchomiono połączenie.
			E	Zakończono połączenie.
	VN	QASYVNJE/J4/J5	F	Żądano wylogowania.
			O	Żądano logowania.
	VS	QASYVSJE/J4/J5	S	Uruchomiono sesję serwera.
			E	Zakończono sesję serwera.
*NETBAS,	CV	QASYCVJE/J4/J5	C	Ustanowiono połączenie
			E	Połączenie zakończone poprawnie
			R	Odrzucono połączenie
	IR	QASYIRJ4/J5	L	Reguły IP zostały załadowane z pliku.
			N	Reguły IP zostały rozładowane dla połączenia ochrony IP.
			P	Reguły IP zostały załadowane dla połączenia ochrony IP.
			R	Reguły IP zostały odczytane i skopiowane do pliku.
			U	Reguły IP zostały rozładowane (usunięte).
	IS	QASYISJ4/J5	1	Faza 1 uzgadniania.
			2	Faza 2 uzgadniania.
	ND	QASYNDJE/J4/J5	A	Obsługa filtrowania APPN wykryła naruszenie podczas kontrolowania filtru przeszukiwania katalogów.
	NE	QASYNEJE/J4/J5	A	Obsługa filtrowania APPN wykryła naruszenie podczas kontrolowania filtru punktów końcowych.
*NETCLU,	CU	QASYCUJE/J4/J5	M	Tworzenie obiektu przez operację sterowania klastrem.
			R	Tworzenie obiektu przez operację zarządzania grupą zasobów klastra (*GRP).
*NETCMN	CU	QASYCUJE/J4/J5	M	Tworzenie obiektu przez operację kontroli klastra.
			R	Tworzenie obiektu przez operację zarządzania grupą zasobów klastra (*GRP).
	CV	QASYCVJ4/J5	C	Ustanowiono połączenie.
			E	Połączenie zakończone poprawnie.
	IR	QASYIRJ4/J5	L	Reguły IP zostały załadowane z pliku.
			N	Reguła IP dla połączenia ochrony IP została rozładowana.
			P	Reguły IP dla połączenia ochrony IP zostały załadowane.
			R	Reguły IP zostały odczytane i skopiowane do pliku.
			U	Reguły IP zostały rozładowane (usunięte).
	IS	QASYISJ4/J5	1	Faza 1 uzgadniania.
			2	Faza 2 uzgadniania.
	ND	QASYNDJE/J4/J5	A	Obsługa filtrowania APPN wykryła naruszenie podczas kontrolowania filtru przeszukiwania katalogów.
	NE	QASYNEJE/J4/J5	A	Obsługa filtrowania APPN wykryła naruszenie podczas kontrolowania filtru punktów końcowych.
	SK	QASYSKJ4/J5	A	Akceptowanie

Tabela 126. Pozycje kroniki kontroli ochrony (kontynuacja)

Działanie lub wartość kontroli obiektu	Typ pozycji kroniki	Plik zewnętrzny bazy danych modelu	Pozycja szczegółowa	Opis
			C	Połączenie
			D	Przypisano adres DHCP
			F	Przefiltrowano pocztę
			P	Port jest niedostępny
			R	Odrzucenie poczty
			U	Odmówiono adresu DHCP
*NETFAIL,	SK	QASYSKJ4/J5	P	Port jest niedostępny
*NETSCK.	SK	QASYSKJ4/J5	A	Akceptowanie
			C	Połączenie
			D	Przypisano adres DHCP
			F	Przefiltrowano pocztę
			R	Odrzucenie poczty
			U	Odmówiono adresu DHCP
*OBJMGT [3]	DI	QASYDIJ4/J5	OM	Zmiana nazwy obiektu
	OM	QASYOMJE/J4/J5	M	Obiekt przeniesiono do innej biblioteki.
			R	Zmieniono nazwę obiektu.
*OFCSRV	ML	QASYMLJE/J4/J5	O	Otwarto protokół poczty.
	SD	QASYSDJE/J4/J5	S	Wprowadzono zmiany w katalogu dystrybucyjnym systemu.
*OPTICAL	O1	QASY01JE/J4/J5	R	Otwarcie pliku lub katalogu
			U	Zmiana lub wczytanie atrybutów
			D	Usunięcie katalogu pliku
			C	Tworzenie katalogu
			X	Zwolnienie zawieszonego zbioru optycznego
	O2	QASY02JE/J4/J5	C	Kopiowanie pliku lub katalogu
			R	Zmiana nazwy pliku
			B	Składowanie pliku lub katalogu
			S	Składowanie zawieszonego zbioru optycznego
			M	Przeniesienie pliku
	O3	QASY03JE/J4/J5	I	Inicjowanie woluminu
			B	Składowanie woluminu.
			N	Zmiana nazwy woluminu
			C	Przekształcanie kopii zapasowej woluminu w wolumin podstawowy
			M	Importowanie
			E	Eksportowanie
			L	Zmiana listy autoryzacji
			A	Zmiana atrybutów woluminu
			R	Odczyt bezwzględny
*PGMADP	AP	QASYAPJE/J4/J5	S	Został uruchomiony program, który adoptuje uprawnienia właściciela. Pozycja uruchomienia jest zapisywana, gdy w celu uzyskania dostępu do obiektu po raz pierwszy używane jest uprawnienie adoptowane, a nie gdy program wchodzi na stos programu.

Tabela 126. Pozycje kroniki kontroli ochrony (kontynuacja)

Działanie lub wartość kontroli obiektu	Typ pozycji kroniki	Plik zewnętrzny bazy danych modelu	Pozycja szczegółowa	Opis
			E	Program, który adoptuje uprawnienia właściciela, zakończył działanie. Kiedy program opuszcza stos programu, zapisywana jest pozycja zakończenia. Jeśli ten sam program wystąpi na stosie więcej niż jeden raz, pozycja zakończenia jest zapisywana, gdy najwyższe (ostatnie) wystąpienie programu opuści stos.
			A	Podczas aktywowania programu użyto uprawnienia adoptowanego.
*PGMFAIL [1]	AF	QASYAFJE/J4/J5	B	Program uruchomił zastrzeżone instrukcje interfejsu maszynowego.
			C	Został odtworzony program, dla którego nie powiodło się sprawdzanie czasu odtwarzania. Informacje o tej awarii znajdują się w rekordzie w polu *Validation Value Violation Type* (Rodzaj naruszenia wartości sprawdzenia).
			D	Program uzyskał dostęp do obiektu za pomocą nieobsługiwanego interfejsu lub program wywoływany nie jest wymieniony na liście wywoływalnych interfejsów API.
			E	Naruszenie ochrony pamięci sprzętowej.
			R	Próba zaktualizowania obiektu, który został zdefiniowany jako tylko do odczytu. (Zaawansowana ochrona pamięci sprzętowej protokołowana jest tylko na poziomie ochrony 40 i wyższym)
*PRTDTA [1]	PO	QASYPOJE/J4/J5	D	Zbiór wydruku został przesłany bezpośrednio do drukarki.
			R	Dane wyjściowe zostały przesłane do systemu zdalnego w celu wydrukowania.
			S	Zbiór wydruku został umieszczony w buforze i wydrukowany.
*SAVRST [3]	OR	QASYORJE/J4/J5	N	W systemie został odtworzony nowy obiekt.
			E	Odtworzony został obiekt, który zastąpił istniejący.
	RA	QASYRAJE/J4/J5	A	System zmienił uprawnienia dla odtwarzanego obiektu. [4]
	RJ	QASYRJJE/J4/J5	A	Odtworzony został opis zadania, który zawiera nazwę profilu użytkownika.
	RO	QASYROJE/J4/J5	A	Podczas odtwarzania właściciel został zmieniony na QDFTOWN. [4]
	RP	QASYRPJE/J4/J5	A	Odtworzony został program, który adoptuje uprawnienia właściciela.
	RQ	QASYRQJE/J4/J5	A	Odtworzony został obiekt *CRQD z z profilem PROFILE(*OWNER).
	RU	QASYRUJE/J4/J5	A	Za pomocą komendy RSTAUT dla profilu użytkownika zostały odtworzone uprawnienia.
	RZ	QASYRZJE/J4/J5	A	Podczas odtwarzania zmieniona została grupa podstawowa dla obiektu.
			O	Za pomocą komendy CHGOBJAUD zmieniona została kontrola obiektu.

Tabela 126. Pozycje kroniki kontroli ochrony (kontynuacja)

Działanie lub wartość kontroli obiektu	Typ pozycji kroniki	Plik zewnętrzny bazy danych modelu	Pozycja szczegółowa	Opis
			U	Za pomocą komendy CHGUSRAUD zmieniona została kontrola użytkownika.
*SECCFG,	AD	QASYADJE/J4/J5	D	Za pomocą komendy CHGDLOAUD zmieniona została kontrola biblioteki DLO.
			S	Atrybut skanowania zmieniony został za pomocą komendy CHGATR lub funkcji API Qp01SetAttr
			O	Za pomocą komendy CHGOBJAUD zmieniona została kontrola obiektu.
			U	Za pomocą komendy CHGUSRAUD zmieniona została kontrola użytkownika.
	AU	QASYAUJ5	E	Zmiana konfiguracji programu Enterprise Identity Mapping (EIM)
	CP	QASYCPJE/J4/J5	A	Podczas używania funkcji API QSYSRESPA tworzono, zmieniano lub odtwarzano profil użytkownika.
	CQ	QASYCQJE/J4/J5	A	Zmieniony został obiekt *CRQD.
	CY	QASYCYJ4/J5	A	Funkcja kontroli dostępu
			F	Funkcja kontroli narzędzia
			M	Funkcja klucza głównego
	DO	QASYDOJE/J4/J5	A	Obiekt został usunięty poza kontrolą transakcji
			C	Oczekujące usunięcie obiektu zostało zatwierdzone
			D	Oczekujące tworzenie obiektu zostało wycofane
			P	Usuwanie obiektu w toku (usuwanie zostało przeprowadzone za pomocą kontroli transakcji)
			R	Oczekujące usuwanie obiektu zostało wycofane
	DS	QASYDSJE/J4/J5	A	Żądanie wyzerowania hasła profilu QSECOFR dla narzędzi DST do wartości domyślnej.
			C	Zmieniono profil narzędzi DST.
	EV	QASYEVJ4/J5	A	Dodanie.
			C	Zmiana.
			D	Usunięcie.
	GR	QASYGRJ4/J5	A	Dodano program obsługi wyjścia
			D	Usunięto program obsługi wyjścia
			F	Rejestrowanie funkcji
			R	Zastąpiono program obsługi wyjścia
	JD	QASYJDJE/J4/J5	A	Zmieniony został parametr USER opisu zadania.
	KF	QASYKFJ4/J5	C	Operacja certyfikowania.
			K	Operacja pliku bazy kluczy.
			T	Operacja użytkownika zaufanego.
	NA	QASYNAJE/J4/J5	A	Atrybut sieciowy został zmieniony.
	PA	QASYPAJE/J4/J5	A	Program został zmieniony tak, aby adoptował uprawnienia właściciela.
	SE	QASYSEJE/J4/J5	A	Pozycja routingu podsystemu została zmieniona.
	SO	QASYSOJ4/J5	A	Dodanie pozycji.

Tabela 126. Pozycje kroniki kontroli ochrony (kontynuacja)

Działanie lub wartość kontroli obiektu	Typ pozycji kroniki	Plik zewnętrzny bazy danych modelu	Pozycja szczegółowa	Opis
			C	Zmiana pozycji.
			R	Usunięcie pozycji.
	SV	QASYSVJE/J4/J5	A	Wartość systemowa została zmieniona.
			B	Atrybuty usługi zostały zmienione.
			C	Zmiana w zegarze systemowym.
	VA	QASYVAJE/J4/J5	S	Lista kontroli dostępu została pomyślnie zmieniona.
			F	Zmiana listy kontroli dostępu nie powiodła się.
			V	Pomyślne sprawdzenie pozycji listy weryfikacji.
	VU	QASYVUJE/J4/J5	G	Rekord grupy został zmieniony.
			M	Zmieniono informacje globalne profilu użytkownika.
			U	Rekord użytkownika został zmieniony.
*SECDIRSRV,	DI	QASYADJE/J4/J5	AD	Zmiana kontroli.
			BN	Konsolidacja powiodła się
			CA	Zmiana uprawnień
			CP	Zmiana hasła
			OW	Zmiana prawa własności
			UB	Odłączanie powiodło się
*SECIPC,	IP	QASYIPJE/J4/J5	A	Zostało zmienione prawo własności lub uprawnienia obiektu IPC.
			C	Utworzenie obiektu IPC.
			D	Usunięcie obiektu IPC.
			G	Pobranie obiektu IPC.
*SECNAS,	X0	QASYX0J4/J5	1	Niepoprawny bilet usług.
			2	Niezgodne jednostki główne usługi.
			3	Niezgodne jednostki główne klienta.
			4	Niezgodność adresu IP biletu.
			5	Deszyfrowanie biletu nie powiodło się
			6	Deszyfrowanie elementu uwierzytelniającego nie powiodło się
			7	Dziedzina nie znajduje się w kliencie i dziedzinach lokalnych
			8	Bilet jest próbą utworzenia odpowiedzi
			9	Bilet nie jest jeszcze ważny
			A	Błąd sumy kontrolnej deszyfrowania KRB_AP_PRIV lub KRB_AP_SAFE
			B	Niezgodność zdalnego adresu IP
			C	Niezgodność lokalnego adresu IP
			D	Błąd datownika KRB_AP_PRIV lub KRB_AP_SAFE
			E	Błąd odpowiedzi KRB_AP_PRIV lub KRB_AP_SAFE
			F	Błąd kolejności uporządkowania KRB_AP_PRIV lub KRB_AP_SAFE
			K	Akceptacja GSS - wygasłe uprawnienia
			L	Akceptacja GSS - błąd sumy kontrolnej
			M	Akceptacja GSS - konsolidacje kanałów
			N	Odpakowanie lub weryfikacja GSS - wygasły kontekst

Tabela 126. Pozycje kroniki kontroli ochrony (kontynuacja)

Działanie lub wartość kontroli obiektu	Typ pozycji kroniki	Plik zewnętrzny bazy danych modelu	Pozycja szczegółowa	Opis
			O	Odpakowanie lub weryfikacja GSS - odszyfrowanie/dekodowanie
			P	Odpakowanie lub weryfikacja GSS - błąd sumy kontrolnej
			Q	Odpakowanie lub weryfikacja GSS - błąd kolejności
*SECRUN,	CA	QASYCAJE/J4/J5	A	Zmiany w liście autoryzacji lub uprawnieniach do obiektu.
	OW	QASYOWJE/J4/J5	A	Zmienione zostało prawo własności do obiektu.
	PG	QASYPGJE/J4/J5	A	Zmieniona została grupa podstawowa dla obiektu.
*SECSCKD,	GS	QASYGSJE/J4/J5	G	Deskryptor gniazda został nadany innemu zadaniu. (Rekord kontroli GS jest tworzony, jeśli nie został utworzony dla bieżącego zadania.)
			R	Pobrano deskryptor.
			U	Nie można użyć deskryptora.
*SECURITY	AD	QASYADJE/J4/J5	D	Za pomocą komendy CHGDLOAUD zmieniona została kontrola biblioteki DLO.
			O	Za pomocą komendy CHGOBJAUD zmieniona została kontrola obiektu.
			U	Za pomocą komendy CHGUSRAUD zmieniona została kontrola użytkownika.
			S	Atrybut skanowania zmieniony został za pomocą komendy CHGATR lub funkcji API Qp01SetAttr
	X1	QASYADJE/J4/J5	D	Delegowanie znacznika tożsamości powiodło się
			G	Pobranie użytkownika z znacznika tożsamości powiodło się
	AU	QASYAUJ5	E	Zmiana konfiguracji programu Enterprise Identity Mapping (EIM)
	CA	QASYCAJE/J4/J5	A	Zmiany w liście autoryzacji lub uprawnieniach do obiektu.
	CP	QASYCPJE/J4/J5	A	Podczas używania funkcji API QSYRESPA tworzono, zmieniano lub odtwarzano profil
	CQ	QASYCQJE/J4/J5	A	Zmieniony został obiekt *CRQD.
	CV	QASYCVJ4/J5	C	Ustanowiono połączenie.
			E	Połączenie zakończone poprawnie.
			R	Odrzucono połączenie.
	CY	QASYCYJ4/J5	A	Funkcja kontroli dostępu
			F	Funkcja kontroli narzędzia
			M	Funkcja klucza głównego
	DI	QASYDIJ4/J5	AD	Zmiana kontroli
			BN	Konsolidacja powiodła się
			CA	Zmiana uprawnień
			CP	Zmiana hasła
			OW	Zmiana prawa własności
			UB	Odłączanie powiodło się
	DO	QASYDOJE/J4/J5	A	Obiekt został usunięty poza kontrolą transakcji

Tabela 126. Pozycje kroniki kontroli ochrony (kontynuacja)

Działanie lub wartość kontroli obiektu	Typ pozycji kroniki	Plik zewnętrzny bazy danych modelu	Pozycja szczegółowa	Opis
			C	Oczekujące usunięcie obiektu zostało zatwierdzone
			D	Oczekujące tworzenie obiektu zostało wycofane
			P	Usuwanie obiektu w toku (usuwanie zostało przeprowadzone za pomocą kontroli transakcji)
			R	Oczekujące usuwanie obiektu zostało wycofane
	DS	QASYDSJE/J4/J5	A	Żądanie wyzerowania hasła profilu QSECOFR dla narzędzi DST do wartości domyślnej.
			C	Zmieniono profil narzędzi DST.
	EV	QASYEVJ4/J5	A	Dodanie.
			C	Zmiana.
			D	Usunięcie.
	GR	QASYGRJ4/J5	A	Dodano program obsługi wyjścia
			D	Usunięto program obsługi wyjścia
			F	Rejestrowanie funkcji
			R	Zastąpiono program obsługi wyjścia
	GS	QASYGSJE/J4/J5	G	Deskryptor gniazda został nadany innemu zadaniu. (Rekord kontroli GS tworzony jest jeśli nie został utworzony dla bieżącego zadania.)
			R	Pobrano deskryptor.
			U	Nie można użyć deskryptora.
	IP	QASYIPJE/J4/J5	A	Zostało zmienione prawo własności lub uprawnienia obiektu IPC.
			C	Utworzenie obiektu IPC.
			D	Usunięcie obiektu IPC.
			G	Pobranie obiektu IPC.
	JD	QASYJDJE/J4/J5	A	Zmieniony został parametr USER opisu zadania.
	KF	QASYKFJ4/J5	C	Operacja certyfikowania.
			K	Operacja pliku bazy kluczy.
			T	Operacja użytkownika zaufanego.
	NA	QASYNAJE/J4/J5	A	Atrybut sieciowy został zmieniony.
	OW	QASYOWJE/J4/J5	A	Zmienione zostało prawo własności do obiektu.
	PA	QASYPAJE/J4/J5	A	Program został zmieniony tak, aby adoptował uprawnienia właściciela.
	PG	QASYPGJE/J4/J5	A	Zmieniona została grupa podstawowa dla obiektu.
	PS	QASYPSJE/J4/J5	A	Podczas sesji tranzytu zmieniony został profil użytkownika docelowego.
			E	Użytkownik biurowy zakończył pracę w imieniu innego użytkownika.
			H	Uchwyt profilu został wygenerowany za pomocą funkcji API QSYGETPH.
			I	Wszystkie znaczniki profilu zostały unieważnione.
			M	Wygenerowano maksymalną liczbę znaczników profilu.

Tabela 126. Pozycje kroniki kontroli ochrony (kontynuacja)

Działanie lub wartość kontroli obiektu	Typ pozycji kroniki	Plik zewnętrzny bazy danych modelu	Pozycja szczegółowa	Opis
			P	Wygenerowano znacznik profilu dla użytkownika.
			R	Wszystkie znaczniki profilu dla użytkownika zostały usunięte.
			S	Użytkownik biurowy rozpoczął pracę w imieniu innego użytkownika.
			V	Profil użytkownika został uwierzytelniony.
	SE	QASYSEJE/J4/J5	A	Pozycja routingu podsystemu została zmieniona.
	SO	QASYSOJ4/J5	A	Dodanie pozycji.
			C	Zmiana pozycji.
			R	Usunięcie pozycji.
	SV	QASYSVJE/J4/J5	A	Wartość systemowa została zmieniona.
			B	Atrybuty usługi zostały zmienione.
			C	Zmiana w zegarze systemowym.
	VA	QASYVAJE/J4/J5	S	Lista kontroli dostępu została pomyślnie zmieniona.
			F	Zmiana listy kontroli dostępu nie powiodła się.
	VO		V	Pomyślne sprawdzenie pozycji listy weryfikacji.
	VU	QASYVUJE/J4/J5	G	Rekord grupy został zmieniony.
			M	Zmieniono informacje globalne profilu użytkownika.
			U	Rekord użytkownika został zmieniony.
	X0	QASYX0J4/J5	1	Niepoprawny bilet usług.
			2	Niezgodne jednostki główne usługi
			3	Niezgodne jednostki główne klienta
			4	Niezgodność adresu IP biletu
			5	Deszyfrowanie biletu nie powiodło się
			6	Deszyfrowanie elementu uwierzytelniającego nie powiodło się
			7	Dziedzina nie znajduje się w kliencie i dziedzinach lokalnych
			8	Bilet jest próbą utworzenia odpowiedzi
			9	Bilet nie jest jeszcze ważny
			A	Błąd sumy kontrolnej deszyfrowania KRB_AP_PRIV lub KRB_AP_SAFE
			B	Niezgodność zdalnego adresu IP
			C	Niezgodność lokalnego adresu IP
			D	Błąd datownika KRB_AP_PRIV lub KRB_AP_SAFE
			E	Błąd odpowiedzi KRB_AP_PRIV lub KRB_AP_SAFE
			F	Błąd kolejności uporządkowania KRB_AP_PRIV lub KRB_AP_SAFE
			K	Akceptacja GSS - wygasłe uprawnienia
			L	Akceptacja GSS - błąd sumy kontrolnej
			M	Akceptacja GSS - konsolidacje kanałów
			N	Odpakowanie lub weryfikacja GSS - wygasły kontekst

Tabela 126. Pozycje kroniki kontroli ochrony (kontynuacja)

Działanie lub wartość kontroli obiektu	Typ pozycji kroniki	Plik zewnętrzny bazy danych modelu	Pozycja szczegółowa	Opis
			O	Odpakowanie lub weryfikacja GSS - odszyfrowanie/dekodowanie
			P	Odpakowanie lub weryfikacja GSS - błąd sumy kontrolnej
			Q	Odpakowanie lub weryfikacja GSS - błąd kolejności
*SECVFY,	PS	QASYPSJE/J4/J5	A	Podczas sesji tranzytu zmieniony został profil użytkownika docelowego.
	X1	QASYX1J5	D	Delegowanie znacznika tożsamości powiodło się
			G	Pobranie użytkownika z znacznika tożsamości powiodło się
			E	Użytkownik biurowy zakończył pracę w imieniu innego użytkownika.
			H	Uchwyt profilu został wygenerowany za pomocą interfejsu API QSYGETPH.
			I	Wszystkie znaczniki profilu zostały unieważnione.
			M	Wygenerowano maksymalną liczbę znaczników profilu.
			P	Wygenerowano znacznik profilu dla użytkownika.
			R	Wszystkie znaczniki profilu dla użytkownika zostały usunięte.
			S	Użytkownik biurowy rozpoczął pracę w imieniu innego użytkownika.
			V	Profil użytkownika został uwierzytelniony.
*SECVLDL.	VO		V	Pomyślne sprawdzenie pozycji listy weryfikacji.
*SERVICE	ST	QASYSTJE/J4/J5	A	Użyte zostało narzędzie usługi.
	VV	QASYVVJE/J4/J5	C	Zmieniony został status usługi.
			E	Serwer został zatrzymany.
			P	Serwer został wstrzymany.
			R	Serwer został zrestartowany.
			S	Serwer został uruchomiony.
*SPLFDTA	SF	QASYSFJE/J4/J5	A	Zbiór buforowy został odczytany przez kogoś innego niż właściciel.
			C	Zbiór buforowy został utworzony.
			D	Zbiór buforowy został usunięty.
			H	Zbiór buforowy został wstrzymany.
			I	Utworzony został zbiór wstawiany.
			R	Zbiór buforowy został zwolniony.
			U	Zbiór buforowy został zmieniony.
*SYSMGT	DI	QASYDIJ4/J5	CF	Zmiany konfiguracji
	SM	QASYSMJE/J4/J5	B	Za pomocą serwera xxxxxxxxxx zmienione zostały opcje składowania.
			C	Za pomocą serwera xxxxxxxxxx zmienione zostały opcje automatycznego czyszczenia.
			D	Dokonano zmiany DRDA*.
			F	Zmieniony został system plików HFS.
			N	Przeprowadzona została operacja na pliku sieciowym.

Tabela 126. Pozycje kroniki kontroli ochrony (kontynuacja)

Działanie lub wartość kontroli obiektu	Typ pozycji kroniki	Plik zewnętrzny bazy danych modelu	Pozycja szczegółowa	Opis
			O	Za pomocą serwera xxxxxxxxxx zmieniona została lista składowania.
			P	Za pomocą serwera xxxxxxxxxx zmieniony został harmonogram włączania/wyłączania.
			S	Zmieniona została lista odpowiedzi systemu.
			T	Zmieniony został czas odtworzenia ścieżki dostępu.
	VL	QASYVLJE/J4/J5	A	Konto wygasło.
			D	Konto zostało zablokowane.
			L	Zostały przekroczone godziny logowania.
			U	Nieznane lub niedostępne.
			W	Stacja robocza nie jest poprawna.
Kontrolowanie obiektu:				
*CHANGE	DI	QASYDIJ4/J5	IM	Importowanie katalogu LDAP
	ZC	QASYZCJ4/J5	C	Zmiany obiektu
			U	Aktualizowanie dostępu otwartego do obiektu
	AD	QASYADJEJ4/J5	D	Za pomocą komendy CHGOBJAUD zmieniona została kontrola obiektu.
			O	Za pomocą komendy CHGOBJAUD zmieniona została kontrola obiektu.
			S	Atrybut skanowania zmieniony został za pomocą komendy CHGATR lub funkcji API Qp01SetAttr
			U	Za pomocą komendy CHGUSRAUD zmieniona została kontrola użytkownika.
	AU	QASYAUJ5	E	Zmiana konfiguracji programu Enterprise Identity Mapping (EIM)
	CA	QASYCAJE/J4/J5	A	Zmiany w liście autoryzacji lub uprawnieniach do obiektu.
	OM	QASYOMJE/J4/J5	M	Obiekt przeniesiono do innej biblioteki.
			R	Zmieniono nazwę obiektu.
	OR	QASYORJE/J4/J5	N	W systemie został odtworzony nowy obiekt.
			E	Odtworzony został obiekt, który zastąpił istniejący.
	OW	QASYOWJE/J4/J5	A	Zmienione zostało prawo własności do obiektu.
	PG	QASYPGJE/J4/J5	A	Zmieniona została grupa podstawowa dla obiektu.
	RA	QASYRAJE/J4/J5	A	System zmienił uprawnienia dla odtwarzanego obiektu.
	RO	QASYROJE/J4/J5	A	Podczas odtwarzania właściciel został zmieniony na QDFTOWN.
	RZ	QASYRZJE/J4/J5	A	Podczas odtwarzania zmieniona została grupa podstawowa dla obiektu.
	GR	QASYGRJ4/J5	F	Działania rejestrowania funkcji [6]
	LD	QASYLDJE/J4/J5	L	Dowiązanie katalogu.
			U	Usunięcie dowiązania katalogu.
			K	Wyszukiwanie katalogu.
	VF	QASYVFJE/J4/J5	A	Plik został zamknięty z powodu odłączenia administracyjnego.

Tabela 126. Pozycje kroniki kontroli ochrony (kontynuacja)

Działanie lub wartość kontroli obiektu	Typ pozycji kroniki	Plik zewnętrzny bazy danych modelu	Pozycja szczegółowa	Opis
			N	Plik został zamknięty z powodu normalnego odłączenia klienta.
			S	Plik został zamknięty z powodu odłączenia sesji.
	VO	QASYVOJ4/J5	A	Dodanie pozycji listy weryfikacji.
			C	Zmiana pozycji listy weryfikacji.
			F	Szukanie pozycji listy weryfikacji.
			R	Usunięcie pozycji listy weryfikacji.
	VR	QASYVRJE/J4/J5	F	Dostęp do zasobu nie powiódł się.
			S	Dostęp do zasobu powiódł się.
	YC	QASYYCJE/J4/J5	C	Obiekt biblioteki dokumentów został zmieniony.
	ZC	QASYZCJE/J4/J5	C	Obiekt został zmieniony.
			U	Aktualizowanie dostępu otwartego do obiektu.
*ALL [5]	CD	QASYCDJ4/J5	C	Uruchomiono komendę
	DI	QASYDIJ4/J5	EX	Eksportowanie katalogu LDAP
			ZR	Odczytano obiekt
	GR	QASYGRJ4/J5	F	Działania rejestrowania funkcji [6]
	YR	QASYYRJE/J4/J5	R	Obiekt biblioteki dokumentów został odczytany.
	ZR	QASYZRJE/J4/J5	R	Obiekt został odczytany.

1 Ta wartość może być podana tylko dla wartości systemowej QAUDLVL. Nie jest to wartość dla parametru AUDLVL profilu użytkownika.

2 Ta wartość może być podana tylko dla parametru AUDLVL profilu użytkownika. Nie jest to wartość dla wartości systemowej QAUDLVL.

3 Jeśli dla obiektu aktywna jest opcja kontrolowania obiektu, rekord kontroli zapisywany jest dla operacji tworzenia, usuwania, zarządzania obiektem lub odtwarzania, nawet jeśli te działania nie są włączone do poziomu kontroli.

4 Informacje na temat zmian uprawnień, które mogą występować kiedy obiekt jest odtwarzany, zawiera temat “Odtwarzanie obiektów” na stronie 226.

5 W przypadku ustawienia *ALL pozycje zapisywane są dla opcji *CHANGE i *ALL.

6 Kiedy kontrolowany jest obiekt QUSRSYS/QUSEXRGOBJ *EXITRG.

Planowanie kontroli dostępu do obiektu

System zapewnia możliwość protokołowania w kronice kontroli ochrony dostępu do obiektu. Nazywane to jest **kontrolowaniem obiektu**. Wartość systemowa QAUDCTL, wartość OBJAUD dla obiektu oraz wartość OBJAUD dla profilu użytkownika używane są razem, w celu sterowania kontrolowaniem obiektu. Wartość OBJAUD dla obiektu oraz wartość OBJAUD dla użytkownika, który używa obiektu, określają, czy dany dostęp powinien być protokołowany. Wartość systemowa QAUDCTL uruchamia i zatrzymuje funkcję kontrolowania obiektu.

Tabela 127 pokazuje, w jaki sposób współpracują ze sobą wartości OBJAUD dla obiektu i dla profilu użytkownika.

Tabela 127. Sposób współpracy kontrolowania obiektu i użytkownika

Wartość OBJAUD dla obiektu	Wartość OBJAUD dla użytkownika		
	*NONE	*CHANGE	*ALL
*NONE	Brak	Brak	Brak
*USRPRF	Brak	Zmiana	Zmiana i użycie

Tabela 127. Sposób współpracy kontrolowania obiektu i użytkownika (kontynuacja)

Wartość OBJAUD dla obiektu	Wartość OBJAUD dla użytkownika		
	***NONE**	***CHANGE**	***ALL**
*CHANGE	Zmiana	Zmiana	Zmiana
*ALL	Zmiana i użycie	Zmiana i użycie	Zmiana i użycie

Kontrolowanie obiektu można wykorzystać do śledzenia każdego dostępu użytkowników do krytycznych obiektów w systemie. Kontrolowania obiektu można także używać do śledzenia całego dostępu przez danego użytkownika. Kontrolowanie obiektu to elastyczne narzędzie, które umożliwia monitorowanie dostępu do tych obiektów, które są ważne dla organizacji.

Skorzystanie z możliwości kontrolowania obiektu wymaga uważnego planowania. Źle zaprojektowana kontrola może spowodować generowanie wielu rekordów kontroli, które użytkownik będzie musiał analizować; może również mieć negatywny wpływ na wydajność systemu. Na przykład ustawienie wartości OBJAUD na *ALL dla biblioteki powoduje powstawanie pozycji kontroli za każdym razem, gdy system przeszukuje daną bibliotekę. W przypadku często używanej biblioteki w obciążonym systemie, spowoduje to generowanie bardzo dużej ilości pozycji kroniki kontroli.

Poniżej przedstawiono kilka przykładów użycia funkcji kontrolowania obiektu.

- Jeśli pewne zbiory krytyczne używane są w całym przedsiębiorstwie, za pomocą poniższej techniki okresowo można przeglądać, kto uzyskuje dostęp do tych obiektów:
  1. Za pomocą komendy Zmiana kontroli obiektu (Change Object Auditing) dla każdego zbioru krytycznego, wartość OBJAUD ustaw na *USRPRF:

```
                    Zmiana kontroli obiektu
                (Change Object Auditing - CHGOBJAUD)

Wpisz i naciśnij Enter.
Obiekt . . . . . . . . . . . . . . nazwa_zbioru
  Biblioteka . . . . . . . . . . .   nazwa_biblioteki
Typ obiektu  . . . . . . . . . . .  *FILE
Urządzenie ASP . . . . . . . . . . *
Wartość kontroli obiektu . . . . . *USRPRF
```

  2. Za pomocą komendy CHGUSRAUD dla każdego użytkownika wartość OBJAUD ustaw na *CHANGE lub *ALL.
  3. Upewnij się, że wartość systemowa QAUDCTL obejmuje wartość *OBJAUD.
  4. Po upłynięciu czasu wymaganego do zebrania odpowiedniej próbki, wartość OBJAUD w profilu użytkownika ustaw na *NONE lub z wartości systemowej QAUDCTL usuń *OBJAUD.
  5. Korzystając z techniki opisanej w sekcji “Analizowanie pozycji kroniki kontroli za pomocą programu Query lub programu użytkownika” na stronie 265 przeanalizuj pozycje kroniki kontroli.
- Jeśli ważne są informacje o tym, kto używa danego zbioru, można zebrać informacje dotyczące całego dostępu do tego zbioru w określonym czasie:
  1. Kontrolowanie obiektu dla zbioru ustaw niezależnie od wartości profilu użytkownika:

```
CHGOBJAUD OBJECT(nazwa_biblioteki/nazwa_zbioru)
          OBJTYPE(*FILE)  OBJAUD(*CHANGE lub *ALL)
```

  2. Upewnij się, że wartość systemowa QAUDCTL obejmuje wartość *OBJAUD.
  3. Po upłynięciu czasu wymaganego do zebrania odpowiedniej próbki, wartość OBJAUD w obiekcie ustaw na *NONE.

4. Korzystając z techniki opisanej w sekcji “Analizowanie pozycji kroniki kontroli za pomocą programu Query lub programu użytkownika” na stronie 265 przeanalizuj pozycje kroniki kontroli.

- Aby kontrolować cały dostęp dla użytkownika, należy wykonać następujące czynności:
  1. Za pomocą komendy CHGOBJAUD, dla wszystkich obiektów wartość OBJAUD ustaw na *USRPRF:

```
                    Zmiana kontroli obiektu
                (Change Object Auditing - CHGOBJAUD)

Wpisz i naciśnij Enter.
Obiekt . . . . . . . . . . . . . .   *ALL
  Biblioteka  . . . . . . . . . . . *ALLAVL
Typ obiektu  . . . . . . . . . . . *ALL
Urządzenie ASP . . . . . . . . . . *
Wartość kontroli obiektu . . . . . *USRPRF
```

     Uwaga: W zależności od tego, jak dużo jest obiektów, uruchomienie tej komendy może zająć wiele godzin. Konfigurowanie kontroli obiektu dla wszystkich obiektów w systemie często nie jest konieczne i spowoduje znaczne obniżenie wydajności. Zalecane jest wybranie podzbioru typów obiektów oraz bibliotek do kontrolowania.
  2. Za pomocą komendy CHGUSRAUD, wartość OBJAUD dla określonego profilu użytkownika ustaw na *CHANGE lub *ALL.
  3. Upewnij się, że wartość systemowa QAUDCTL obejmuje wartość *OBJAUD.
  4. Po zebraniu określonej próbki, wartość OBJAUD dla profilu użytkownika ustaw na *NONE.

Wyświetlanie kontrolowania obiektu: Aby wyświetlić bieżący poziom kontrolowania dla obiektu, należy użyć komendy DSPOBJD. Aby wyświetlić bieżący poziom kontrolowania obiektu dla obiektu biblioteki dokumentów, należy użyć komendy DSPDLOAUD.

Ustawianie domyślnego kontrolowania dla obiektów: Za pomocą wartości systemowej QCRTOBJAUD i wartości CRTOBJAUD dla bibliotek i katalogów, można ustawić kontrolowanie obiektu dla nowo tworzonych obiektów. Na przykład jeśli wszystkie nowe obiekty w bibliotece INVLIB mają mieć wartość kontroli *USRPRF, należy użyć następującej komendy:

```
CHGLIB LIB(INVLIB) CRTOBJAUD(*USRPRF)
```

Wpłynie to na wartość kontroli tylko nowych obiektów. Nie zmienia wartości kontroli obiektów, które już istnieją w bibliotece.

Domyślnych wartości kontroli należy używać ostrożnie. Nieprawidłowe użycie może powodować powstawanie w kronice kontroli ochrony wielu niechcianych pozycji. Efektywne używanie możliwości kontrolowania obiektu wymaga ostrożnego planowania.

Zapobieganie utracie informacji o kontrolowaniu

Do kontrolowania czynności systemu, gdy warunki błędu mogą spowodować utratę pozycji kroniki kontroli, służą dwie wartości systemowe.

Poziom narzucenia kontroli: Wartość systemowa QAUDFRCLVL określa, jak często system zapisuje pozycje kroniki kontroli z pamięci do pamięci dyskowej. Wartość ta działa w taki sam sposób, jak poziom narzucenia dla zbiorów bazy danych. Podczas określania odpowiedniego poziomu narzucenia dla instalacji użytkownika należy zastosować się do podobnych wskazówek.

Jeśli system sam będzie określał, kiedy zapisywać pozycje w pamięci dyskowej, wybierze takie parametry, aby zminimalizować pogorszenie wydajności systemu przy jednoczesnym zabezpieczeniu przed utratą informacji w wypadku przerwy w zasilaniu. Domyślnym i zalecanym wyborem jest *SYS.

Ustawienie niskiej wartości poziomu wymuszenia powoduje zminimalizowanie możliwości utraty rekordów kontroli, ale może negatywnie wpływać na wydajność systemu. Jeśli instalacja użytkownika wymaga, aby podczas awarii zasilania nie został utracony żaden rekord, wartość QAUDFRCLVL należy ustawić na 1.

Działanie zakończenia kontroli: Wartość systemowa QAUDENDACN określa co system zrobi, jeśli nie może zapisać w kronice kontroli kolejnej pozycji. Wartością domyślną jest *NOTIFY. Jeśli system nie może zapisać pozycji kroniki kontroli, a wartość QAUDENDACN ustawiona jest na *NOTIFY, wykonane zostaną następujące czynności:

1. Wartość systemowa QAUDCTL zostanie ustawiona na *NONE, aby zapobiec dodatkowym próbom zapisu pozycji.
2. Co godzinę, do czasu pomyślnego zrestartowania kontroli, do kolejki komunikatów QSYSOPR i kolejki QSYSMSG (jeśli istnieje) wysyłany jest komunikat CPI2283.
3. Kontynuowane jest zwykłe przetwarzanie.
4. Jeśli jest wykonywane IPL, podczas IPL do kolejek komunikatów QSYSOPR i QSYSMSG wysyłany jest komunikat CPI2284.

   Uwaga: W większości przypadków wykonanie IPL rozwiązuje problem, który spowodował awarię kontroli. Po zrestartowaniu systemu, wartość systemową QAUDCTL należy ustawić na poprawną wartość. System próbuje zapisać rekord kroniki kontroli, kiedy tylko ta wartość systemowa zostanie zmieniona.

Istnieje możliwość ustawienia wartości systemowej QAUDENDACN tak, aby system był wyłączany w przypadku niepowodzenia kontroli (*PWRDWNSYS). Tej wartości należy użyć tylko wtedy, gdy do działania instalacji wymagana jest aktywna funkcja kontroli. Jeśli system nie może zapisać pozycji kroniki kontroli, a wartość systemowa QAUDENDACN ustawiona jest na *PWRDWNSYS, mają miejsce następujące zdarzenia:

1. System natychmiast się wyłącza (jest to równoznaczne z wywołaniem komendy PWRDWNSYS *IMMED).
2. Wyświetlany jest kod SRC B900 3D10.

Następnie należy wykonać następujące czynności:

1. Z jednostki systemowej rozpocznij IPL. Należy sprawdzić, czy urządzenie określone w wartości systemowej konsoli (QCONSOLE) jest włączone.
2. Aby zakończyć IPL, na konsoli musi być wpisany użytkownik z uprawnieniami specjalnymi *ALLOBJ i *AUDIT.
3. System uruchamia się w stanie zastrzeżonym z komunikatem wskazującym, że zatrzymanie systemu spowodował błąd kontroli.
4. Wartość systemowa QAUDCTL ustawiona jest na *NONE.
5. Aby odtworzyć normalne działanie systemu, wartość systemową QAUDCTL należy ustawić na wartość inną niż *NONE. Po zmianie wartości systemowej QAUDCTL system próbuje zapisać pozycję kroniki kontroli. Jeśli próba będzie pomyślna, system powraca do normalnego stanu.

   Jeśli system nie powrócił do normalnego stanu, za pomocą protokołu zadania należy określić, dlaczego zawiodła kontrola. Problem należy poprawić i ponownie spróbować zresetować wartość QAUDCTL.

Ustawianie braku kontroli obiektów QTEMP

Wartość *NOQTEMP, może być podana jako wartość dla wartości systemowej QAUDCTL. Jeśli zostanie podana, należy także podać wartość *OBJAUD lub *AUDLVL. Gdy kontrola jest aktywna i podana została wartość *NOQTEMP, NIE będą kontrolowane następujące działania na obiektach w bibliotece QTEMP:

zmiana lub odczyt obiektów z biblioteki QTEMP (typy pozycji kroniki ZC, ZR),

zmiana uprawnień, właściciela lub grupy podstawowej dla obiektów z biblioteki QTEMP (typy pozycji kroniki CA, OW, PG).

Używanie komendy CHGSECAUD do konfigurowania kontroli ochrony

Przegląd:

Przeznaczenie:

Konfiguruje system do zbierania zdarzeń ochrony w kronice QAUDJRN.

Sposób używania:
CHGSECAUDDSPSECAUD

Uprawnienia:
Użytkownik musi mieć uprawnienia specjalne *ALLOBJ i *AUDIT.

Pozycja kroniki:
CO (tworzenie obiektu),
SV (zmiana wartości systemowej),
AD (zmiany kontroli obiektu i użytkownika).

Uwagi:
Komenda CHGSECAUD tworzy kronikę oraz dziennik, jeśli nie istnieją. Następnie ustawia wartości systemowe QAUDCTL, QAUDLVL i QAUDLVL2.

Konfigurowanie kontroli ochrony

Przegląd:

Przeznaczenie:
Konfiguruje system do zbierania zdarzeń ochrony w kronice QAUDJRN.

Sposób używania:
CRTJRNRCVCRTJRN QSYS/QAUDJRN
WRKSYSVAL *SEC
CHGOBJAUDCHGDLOAUD
CHGUSRAUD

Uprawnienia:
Uprawnienie *ADD do biblioteki QSYS i dziennika
Uprawnienia specjalne *AUDIT

Pozycja kroniki:
CO (tworzenie obiektu),
SV (zmiana wartości systemowej),
AD (zmiany kontroli obiektu i użytkownika).

Uwaga:
Zanim wartość QAUDCTL zostanie zmieniona, musi istnieć kronika QSYS/QAUDJRN.

Aby skonfigurować kontrolę ochrony, należy wykonać następujące czynności. Konfigurowanie kontroli wymaga uprawnień specjalnych *AUDIT.

1. Za pomocą komendy Tworzenie dziennika (Create Journal Receiver - CRTJRNRCV) w wybranej bibliotece utwórz dziennik. Ten przykład korzysta z biblioteki JRNLIB.

```
CRTJRNRCV  JRNRCV(JRNLIB/AUDRCV0001) +
           THRESHOLD(100000) AUT(*EXCLUDE)   +
           TEXT('Dziennik kontroli')
```

   - Umieść dziennik w bibliotece, która jest regularnie składowana. Dziennika **nie** należy umieszczać w bibliotece QSYS, nawet jeśli jest to miejsce docelowe kroniki.
   - Podaj nazwę dziennika, która ma być użyta do utworzenia konwencji nazewnictwa dla przyszłych dzienników, na przykład AUDRCV0001. W celu kontynuowania konwencji nazewnictwa można użyć opcji *GEN podczas zmieniania dzienników. Użycie tego typu konwencji jest przydatne, gdy system ma zarządzać zmianami dzienników.
   - Podaj próg dziennika odpowiedni dla wielkości systemu oraz jego aktywności. Wybrana wielkość powinna opierać się na liczbie transakcji w systemie oraz liczbie czynności wybranych do kontrolowania. Jeśli używana jest obsługa zarządzania zmianami kroniki przez system, próg dziennika musi mieć przynajmniej 100 000 kB. Więcej informacji dotyczących progu dziennika znajduje się w temacie Zarządzanie kronikami.
   - Aby ograniczyć dostęp do informacji przechowywanych w kronice, dla parametru AUT należy podać wartość *EXCLUDE.

2. Za pomocą komendy Tworzenie kroniki (Create Journal - CRTJRN) utwórz kronikę QSYS/QAUDJRN:

```
CRTJRN  JRN(QSYS/QAUDJRN) +
        JRNRCV(JRNLIB/AUDRCV0001) +
        MNGRCV(*SYSTEM) DLTRCV(*NO) +
        AUT(*EXCLUDE) TEXT('Kronika kontroli')
```

   - Nazwa QSYS/QAUDJRN musi być użyta.
   - Podaj nazwę dziennika utworzonego w poprzednim kroku.
   - Aby ograniczyć dostęp do informacji przechowywanych w kronice, dla parametru AUT należy podać wartość *EXCLUDE. Aby utworzyć kronikę, użytkownik musi mieć uprawnienia do dodawania obiektów do biblioteki QSYS.
   - Aby system zmienił dziennik i podłączył nowy, gdy podłączony dziennik przekroczy podany próg, należy użyć parametru *Zarządzanie dziennikiem* (MNGRCV). Po wybraniu tej opcji do ręcznego odłączania dzienników oraz tworzenia i przyłączania nowych dzienników nie będzie konieczne użycie komendy CHGJRN.
   - System nie może usuwać odłączonych dzienników. Podaj parametr DLTRCV(*NO), który jest domyślny. Dzienniki kroniki QAUDJRN są zapisami kontrolnymi ochrony. Przed usunięciem ich z systemu należy się upewnić, że zostały odpowiednio zeskładowane.

   Więcej informacji dotyczących pracy z kronikami oraz dziennikami zawiera temat Zarządzanie kroniką.
3. Za pomocą komendy WRKSYSVAL ustaw wartość systemową poziomu kontroli (QAUDLVL) lub wartość systemową rozszerzenia poziomu kontroli (QAUDLVL2). Wartości systemowe QAUDLVL i QAUDLVL2 określają, jakie działania użytkowników systemu protokołowane są w kronice kontroli. Patrz “Planowanie kontroli działania” na stronie 238.
4. Jeśli to konieczne, za pomocą komendy CHGUSRAUD ustaw kontrolę działania dla pojedynczych użytkowników. Patrz “Planowanie kontroli działania” na stronie 238.
5. Jeśli to konieczne, za pomocą komend CHGOBJAUD i CHGDLOAUD ustaw kontrolowanie obiektu dla określonych obiektów. Patrz “Planowanie kontroli dostępu do obiektu” na stronie 256.
6. Jeśli to konieczne, za pomocą komendy CHGUSRAUD ustaw kontrolowanie obiektu dla określonych użytkowników.
7. Ustaw wartość systemową QAUDENDACN, aby kontrolować, co się stanie, jeśli system nie będzie miał dostępu do kroniki kontroli. Patrz “Działanie zakończenia kontroli” na stronie 259.
8. Ustaw wartość systemową QAUDFRCLVL, aby kontrolować, jak często w pamięci dyskowej zapisywane są rekordy kontroli. Patrz “Zapobieganie utracie informacji o kontrolowaniu” na stronie 258.
9. Ustawiając wartość systemową QAUDCTL na wartość inną niż *NONE rozpocznij kontrolowanie.

Przed zmianą wartości systemowej QAUDCTL na wartość inną niż *NONE, musi istnieć kronika QSYS/QAUDJRN. Gdy kontrola jest uruchamiana, system próbuje zapisać rekord w kronice kontroli. Jeśli próba się nie powiedzie, użytkownik otrzyma komunikat, a kontrola nie zostanie uruchomiona.

Zarządzanie kroniką kontroli oraz dziennikami

Kronika kontroli, QSYS/QAUDJRN, służy wyłącznie do kontroli ochrony. Nie należy kronikować w niej obiektów. Również kontrola transakcji nie powinna korzystać z kroniki kontroli. Nie należy też wysyłać do niej pozycji użytkowników za pomocą komendy Wysłanie pozycji do kroniki (Send Journal Entry - SNDJRNE) ani funkcji API Send Journal Entry (QJOSJRNE).

Aby system mógł zapisywać pozycje kontroli do kroniki kontroli, używana jest specjalna blokada. Kiedy kontrola jest aktywna (wartość systemowa QAUDCTL jest różna od *NONE), zadanie arbitra systemowego (QSYSARB) blokuje kronikę QSYS/QAUDJRN. Gdy kronika kontroli jest aktywna, nie można wykonywać na niej takich czynności, jak:

- komenda DLTJRN,
- komenda ENDJRNxxx (Zakończenie kronikowania - End Journaling),
- komenda APYJRNCHG,
- komenda RMVJRNCHG,
- komenda DMPOBJ lub DMPSYSOBJ,

- przenoszenie kroniki,
- odtwarzanie kroniki,
- operacje na uprawnieniach, na przykład komenda GRTOBJAUT,
- komenda WRKJRN.

Informacje zapisane w pozycjach kroniki ochrony opisano w sekcji Dodatek F. Wszystkie pozycje dotyczące ochrony w kronice kontroli mają kod kroniki T. W kronice QAUDJRN, obok pozycji dotyczących ochrony, znajdują się pozycje systemowe. Mają one kod kroniki J i dotyczą ładowania programu początkowego (IPL) i ogólnych działań wykonywanych na dziennikach (na przykład składowania).

Jeśli kronika lub jej bieżący dziennik zostanie uszkodzona i pozycje kontroli nie będą kronikowane, wartość systemowa QAUDENDACN będzie określać, jakie czynności powinien podjąć system. Odzyskiwanie zniszczonej kroniki lub dziennika wykonuje się tak samo, jak w przypadku innych kronik.

Można skonfigurować system tak, aby sam zarządzał zmianami dzienników. Podczas tworzenia kroniki QAUDJRN należy podać parametr MNGRCV(*SYSTEM) lub zmienić go w istniejącej kronice. Po podaniu wartości MNGRCV(*SYSTEM) system automatycznie odłączy dziennik, gdy osiągnie on wielkość progową, a następnie utworzy i przyłączy nowy dziennik. Jest to tak zwane **systemowe zarządzanie zmianą kroniki**.

Jeśli dla wartości QAUDJRN podano MNGRCV(*USER), po osiągnięciu progu pamięci, do kolejki komunikatów progu, podanej dla kroniki, wysyłany jest komunikat. Komunikat informuje, że dziennik osiągnął swój próg. Za pomocą komendy CHGJRN należy odłączyć ten dziennik i podłączyć nowy. Zapobiega to powstaniu warunku błędu *pozycja nie została zakronikowana*. Jeśli zostanie otrzymany taki komunikat, należy użyć komendy CHGJRN, aby kontynuować kontrolę ochrony.

Domyślną kolejką komunikatów dla kroniki jest kolejka QSYSOPR. Jeśli w kolejce komunikatów QSYSOPR przechowywana jest duża liczba komunikatów, z kroniką kontroli QAUDJRN można powiązać inną kolejkę komunikatów, taką jak AUDMSG. Do monitorowania kolejki komunikatów AUDMSG można użyć programu obsługi komunikatów. Gdy otrzymane zostanie ostrzeżenie progu kroniki (CPF7099), nowy dziennik może zostać automatycznie podłączony. Jeśli używane jest systemowe zarządzanie zmianą kroniki, po zakończeniu zamiany kroniki, do kolejki komunikatów kroniki wysyłany jest komunikat CPF7020. Ten komunikat można monitorować w celu określenia, kiedy należy zeskładować odłączone dzienniki kontroli.

Uwaga: Funkcja automatycznego usuwania zawartości udostępniana przez menu Asysty Operacyjnej, nie usuwa zawartości dzienników QAUDJRN. Aby uniknąć problemów związanych z przestrzenią dyskową, dzienniki QAUDJRN należy regularnie odłączać, składować i usuwać.

Sekcja Zarządzanie kroniką zawiera więcej szczegółowych informacji o zarządzaniu kronikami i dziennikami.

Uwaga: Podczas przeprowadzania IPL tworzona jest kronika QAUDJRN, jeśli nie istnieje, a wartość systemowa QAUDCTL ustawiana jest na wartość inną niż *NONE. Następuje to jedynie w przypadku nadzwyczajnej sytuacji, takiej jak zastąpienie urządzenia dyskowego lub czyszczenie zawartości puli pamięci dyskowej.

Składowanie i usuwanie dzienników kontroli

Przegląd:

Przeznaczenie:

Do podłączania nowego dziennika kontroli; do składowania i usunięcia poprzedniego dziennika

Sposób używania:

- CHGJRN QSYS/QAUDJRN
- JRNRCV(*GEN) SAVOBJ (do składowania poprzedniego dziennika)
- DLTJRNRCV (do usunięcia poprzedniego dziennika)

Uprawnienia:
Uprawnienia *ALL do dziennika, uprawnienia *USE do kroniki

Pozycja kroniki:
J (pozycja systemowa w kronice QAUDJRN)

Uwaga:
Należy wybrać moment, gdy system nie jest zajęty.

Odłączanie bieżącego dziennika kontroli i podłączanie nowego należy wykonywać z dwóch powodów:

- analizowanie pozycji kroniki jest łatwiejsze, jeśli każdy dziennik zawiera pozycje dla określonego, możliwego do określenia okresu,
- duże dzienniki mogą wpływać na wydajność systemu, oprócz zajmowania cennej przestrzeni pamięci dyskowej.

Zalecanym podejściem jest ustawienie automatycznego zarządzania dziennikami przez system. Można to określić przez podanie parametru *Zarządzanie dziennikami* podczas tworzenia kroniki.

Jeśli kontrola działania i obiektu została skonfigurowana do protokołowania wielu różnych zdarzeń, konieczne może być podanie dużej wartości progu dla dziennika. Jeśli użytkownik zarządza dziennikami ręcznie, konieczna może okazać się codzienna zmiana dzienników. Jeśli protokołowanych jest tylko kilka zdarzeń, zmiana dzienników może odpowiadać harmonogramowi składowania dla biblioteki zawierającej dziennik.

Za pomocą komendy CHGJRN można odłączyć i podłączyć nowy dziennik.

Dzienniki zarządzane przez system: Jeśli dziennikami zarządza system, aby zeskładować wszystkie podłączone dzienniki QAUDJRN oraz je usunąć, należy wykonać następującą procedurę:

1. Wpisz WRKJRNA QAUDJRN. Na ekranie zostanie wyświetlony aktualnie podłączony dziennik. Nie należy go składować ani usuwać.
2. Aby pracować z katalogiem dziennika, użyj klawisza F15. Spowoduje to wyświetlenie wszystkich dzienników, które były związane z kroniką oraz ich status.
3. Za pomocą komendy SAVOBJ zeskładuj każdy dziennik, z wyjątkiem aktualnie podłączonego, który nie został jeszcze zapisany.
4. Za pomocą komendy DLTJRNRCV usuń każdy zeskładowany dziennik.

Uwaga: Alternatywą dla powyższej procedury może być użycie kolejki komunikatów kroniki, w celu odszukania komunikatu CPF7020, który wskazuje, że systemowa zmiana kroniki została zakończona pomyślnie. Więcej informacji dotyczących tej obsługi znajduje się w temacie *Składowanie i odtwarzanie*.

Dzienniki zarządzane przez użytkownika: Jeśli dzienniki kontroli mają być zarządzane ręcznie, do odłączania, składowania i usuwania dziennika należy użyć następującej procedury:

1. Wpisz CHGJRN JRN(QAUDJRN) JRNRCV(*GEN). Ta komenda:
   a. odłącza aktualnie podłączony dziennik,
   b. tworzy nowy dziennik z następnym numerem kolejnym,
   c. podłącza nowy dziennik do kroniki.

   Na przykład jeśli aktualnym dziennikiem jest dziennik AUDRCV0003, system utworzy i podłączy nowy dziennik AUDRCV0004.

   Komenda Praca z atrybutami kroniki (Work with Journal Attributes - WRKJRNA) informuje, który dziennik jest aktualnie podłączony: WRKJRNA QAUDJRN.
2. Za pomocą komendy Składowanie obiektu (Save Object - SAVOBJ) zeskładuj odłączony dziennik. Jako typ obiektu podaj *JRNRCV.
3. Za pomocą komendy Usunięcie dziennika (Delete Journal Receiver - DLTJRNRCV) usuń dziennik. Jeśli nastąpi próba usunięcia dziennika bez jego składowania, pojawi się komunikat ostrzegawczy.

Zatrzymywanie funkcji kontroli

Użytkownik może chcieć korzystać z funkcji kontroli jedynie okresowo, a nie przez cały czas. Na przykład można jej używać podczas testowania nowej aplikacji. Lub podczas wykonywania kwartalnej kontroli ochrony.

Aby zatrzymać funkcję kontroli, należy wykonać następujące czynności:

1. Za pomocą komendy WRKSYSVAL zmień wartość systemową QAUDCTL na *NONE. Zatrzyma to protokołowanie przez system zdarzeń ochrony.
2. Za pomocą komendy CHGJRN odłącz bieżący dziennik.
3. Za pomocą komend SAVOBJ i DLTJRNRCV zeskładuj i usuń odłączony dziennik.
4. Kronikę QAUDJRN można usunąć po zmianie wartości QAUDCTL na *NONE. Jeśli planowane jest wznowienie kontroli ochrony w przyszłości, kronikę QAUDJRN można pozostawić. Jeśli kronika QAUDJRN została skonfigurowana przy użyciu wartości MNGRCV(*SYSTEM), to przy każdym wykonaniu IPL system będzie odłączał dziennik i przyłączał nowy, gdy kontrola ochrony jest aktywna. Te dzienniki należy usunąć. Składowanie ich przed usunięciem nie jest konieczne, ponieważ nie zawierają one żadnych pozycji kontroli.

Analizowanie pozycji kroniki kontroli

Po skonfigurowaniu funkcji kontroli ochrony do analizowania protokołowanych zdarzeń można użyć kilku różnych metod:

- przeglądanie wybranych pozycji na stacji roboczej,
- używanie narzędzia do tworzenia zapytań lub programu do analizowania pozycji,
- używanie komendy Wyświetlenie pozycji kroniki kontroli (Display Audit Journal Entries - DSPAUDJRNE).

Uwaga: IBM wstrzymał udostępnianie rozszerzeń komendy DSPAUSJRNE. Komenda ta nie obsługuje wszystkich typów rekordów kontroli ochrony i nie wyświetla wszystkich pól dla rekordów, które obsługuje.

W celu pobrania pozycji w zapisanej postaci, dla kroniki QAUDJRN można także użyć komendy Pobranie pozycji kroniki (Receive Journal Entry - RCVJRNE).

Przeglądanie pozycji kroniki kontroli

Przegląd:

Przeznaczenie:
Przeglądanie pozycji QAUDJRN

Sposób używania:
Komenda DSPJRN (Wyświetlenie kroniki - Display Journal)

Uprawnienia:
Uprawnienia *USE do QSYS/QAUDJRN, uprawnienia *USE do dziennika

Komenda Wyświetlenie kroniki (Display Journal - DSPJRN) umożliwia przeglądanie wybranych pozycji kroniki na stacji roboczej. Aby przeglądać pozycje kroniki, należy wykonać następujące czynności:

1. Wpisz DSPJRN QAUDJRN i naciśnij klawisz F4. Na ekranie podpowiedzi można wprowadzić zakres pozycji, które mają być pokazane. Na przykład można wybrać wszystkie pozycje w określonym zakresie dat lub można wybrać jedynie pewien typ pozycji, takie jak nieprawidłowe próby wpisania się (typ pozycji kroniki PW).

   Wartością domyślną jest wyświetlanie pozycji tylko z podłączonego dziennika. Za pomocą parametru RCVRNG(*CURCHAIN) można zobaczyć pozycje ze wszystkich dzienników, które znajdują się w łańcuchu dzienników dla kroniki QAUDJRN, łącznie z dziennikiem, który jest aktualnie podłączony.
2. Po naciśnięciu klawisza Enter pojawi się ekran Wyświetlenie pozycji kroniki (Display Journal Entries):

```
                  Wyświetlenie pozycji kroniki
                   (Display Journal Entries)
 Kronika. . . . . . . :   QAUDJRN        Biblioteka . . . . . :   QSYS
 Największy numer kolejny na tym ekranie . . . . . :00000000000000000012
Wpisz opcje i naciśnij klawisz Enter.
   5=Wyświetlenie całej pozycji


 Opcja  Kolejność Kod   Typ   Obiekt    Biblioteka    Zadanie   Godzina
              1   J     PR                          SCPF      10:24:55
              2   T     CA                          SCPF      10:24:55
              3   T     CO                          SCPF      10:24:55
              4   T     CA                          SCPF      10:24:55
              5   T     CO                          SCPF      10:24:55
              6   T     CA                          SCPF      10:24:55
              7   T     CO                          SCPF      10:24:55
              8   T     CA                          SCPF      10:24:56
              9   T     CO                          SCPF      10:24:56
             10   T     CA                          SCPF      10:24:57
             11   T     CO                          SCPF      10:24:57
             12   T     CA                          SCPF      10:24:57
                                                              Więcej...
F3=Wyjście      F12=Anuluj
```

3. Aby zobaczyć informacje dotyczące konkretnej pozycji, należy użyć opcji 5 (Wyświetlenie całej pozycji):

```
                  Wyświetlenie pozycji kroniki
                    (Display Journal Entry)
 Obiekt . . . . . . . :   NEWESTAREA      Biblioteka . . . . . :LEVERING
 Podzbiór . . . . . . :
 Niekompletne dane. . :   Nie             Min danych pozycji   :Nie
 Kolejność. . . . . . :   3
 Kod. . . . . . . . . :   E  - Operacja na obszarze danych
 Typ. . . . . . . . . :   EG - Uruchomienie kronikowania
                            dla obszaru danych

            Dane specyficzne dla pozycji
 Kolumna    *...+....1....+....2....+....3....+....4....+....5
 00001     '0'
```

4. Dla pozycji z dużą ilością danych można użyć klawisza F6 (Display only entry specific data - Wyświetlenie tylko danych dotyczących pozycji). Można także wybrać szesnastkową wersję tego ekranu. Za pomocą klawisza F10 można wyświetlić szczegółowe informacje dotyczące pozycji kroniki, bez informacji specyficznych dla pozycji.

   Dodatek F zawiera układ dla każdego typu pozycji kroniki QAUDJRN.

Analizowanie pozycji kroniki kontroli za pomocą programu Query lub programu użytkownika

Przegląd:

Przeznaczenie:
Wyświetlanie lub drukowanie wybranych informacji z pozycji kroniki.

Sposób używania:
Komenda DSPJRN OUTPUT(*OUTFILE), tworzenie zapytania lub programu, uruchomienie zapytania lub programu

Uprawnienia:

Uprawnienia *USE do kroniki QSYS/QAUDJRN, uprawnienia *USE do dziennika lub uprawnienia *ADD do biblioteki dla zbioru wyjściowego

Za pomocą komendy Wyświetlenie kroniki (Display Journal - DSPJRN) w zbiorze wyjściowym można zapisać wybrane pozycje z dzienników kontroli. Do przeglądania informacji ze zbioru wyjściowego można użyć programu lub zapytania.

Jako parametr wyjściowy komendy DSPJRN należy podać *OUTFILE. Pojawią się dodatkowe parametry, dla których należy podać informacje dotyczące zbioru wyjściowego:

```
                Wyświetlenie kroniki
              (Display Journal - DSPJRN)

Wpisz i naciśnij Enter.
   :
Wyjście  . . . . . . . . . . . . > *OUTFILE
Format zbioru wyjściowego  . . . *TYPE5
Zbiór wyjściowy do zapisania . . dspjrnout
  Biblioteka . . . . . . . . . .   mylib
Opcje podzbioru wyjściowego:
  Podzbiór wyjściowy . . . . . . *FIRST
  Zastąpienie lub dod. rekordów. *REPLACE
Długość pozycji:
  Format danych pola . . . . . . *OUTFILFMT
  Długość pola o zmiennej dług .
  Przydzielona długość . . . . .
```

Wszystkie pozycje związane z ochroną z kroniki kontroli zawierają te same informacje nagłówkowe, takie jak typ pozycji, datę pozycji oraz zadanie, które spowodowało zapisanie pozycji. Wartość QADSPJR5 (z formatem rekordu QJORDJE5) udostępniona została do definiowania tych pól, podczas podawania wartości *TYPE5 jako parametr formatu zbioru wyjściowego. Więcej informacji na ten temat zawiera Tabela 152 na stronie 505.

Więcej informacji na temat innych rekordów i ich formatu zbioru wyjściowego znajduje się w dodatku F.

Jeśli ma być przeprowadzona szczegółowa analiza danego typu pozycji, należy użyć jednego z udostępnionych modelowych zbiorów wyjściowych bazy danych. Na przykład, aby w bibliotece QGPL utworzyć zbiór wyjściowy AUDJRNAF, który obejmuje jedynie pozycje błędów uprawnień:

1. Utwórz pusty zbiór wyjściowy o formacie zdefiniowanym dla pozycji AF kroniki:
   ```
   CRTDUPOBJ OBJ(QASYAFJ5) FROMLIB(QSYS) +
     OBJTYPE(*FILE) TOLIB(QGPL) NEWOBJ(AUDJRNAF5)
   ```
2. Za pomocą komendy DSPJRN zapisz w nim wybrane pozycje kroniki:
   ```
   DSPJRN JRN(QAUDJRN) ... +
      JRNCDE(T) ENTTYP(AF) OUTPUT(*OUTFILE) +
      OUTFILFMT(*TYPE5) OUTFILE(QGPL/AUDJRNAF5)
   ```
3. Za pomocą programu Query lub programu do analizowania, przeanalizuj informacje ze zbioru AUDJRNAF.

Tabela 126 na stronie 243 opisuje nazwę modelowego zbioru wyjściowego bazy danych dla każdego typu pozycji. Dodatek F opisuje układy zbioru dla każdego modelowego zbioru wyjściowego bazy danych.

Poniżej przedstawiono kilka przykładów wykorzystania informacji z kroniki QAUDJRN:

- Jeśli istnieje podejrzenie, że ktoś próbuje włamać się do systemu:
  1. Upewnij się, że wartość systemowa QAUDLVL obejmuje wartość *AUTFAIL.
  2. Za pomocą komendy CRTDUPOBJ utwórz pusty zbiór wyjściowy z formatem QASYPWJ5.

3. Gdy ktoś próbuje wprowadzić na ekranie Wpisanie się (Sign On) nieprawidłowy identyfikator użytkownika lub hasło, protokołowana jest pozycja PW. Za pomocą komendy DSPJRN zapisz w zbiorze wyjściowym pozycje PW kroniki.
4. Utwórz program zapytania, który wyświetla lub drukuje datę, godzinę oraz stację roboczą dla każdej pozycji kroniki. Te informacje powinny pomóc określić, gdzie i kiedy nastąpiła taka próba.

- Jeśli użytkownik chce przetestować ochronę zasobów, która została zdefiniowana dla nowej aplikacji:
  1. Upewnij się, że wartość systemowa QAUDLVL obejmuje wartość *AUTFAIL.
  2. Uruchom testy aplikacji z innymi identyfikatorami użytkowników.
  3. Za pomocą komendy CRTDUPOBJ utwórz pusty zbiór wyjściowy z formatem QASYAFJ5.
  4. Za pomocą komendy DSPJRN zapisz w zbiorze wyjściowym pozycje AF kroniki.
  5. Utwórz program zapytania, który wyświetla lub drukuje informacje dotyczące obiektu, zadania i użytkownika. Te informacje powinny pomóc określić, którzy użytkownicy oraz które funkcje aplikacji powodują błędy uprawnień.
- Jeśli użytkownik planuje migrację do poziomu ochrony 40:
  1. Upewnij się, że wartość systemowa QAUDLVL obejmuje wartości *PGMFAIL i *AUTFAIL.
  2. Za pomocą komendy CRTDUPOBJ utwórz pusty zbiór wyjściowy z formatem QASYAFJ5.
  3. Za pomocą komendy DSPJRN zapisz w zbiorze wyjściowym pozycje AF kroniki.
  4. Utwórz program zapytania, który wybiera typ naruszeń pojawiający się podczas testowania i drukowania informacji dotyczących zadania i pozycji, które powodują powstanie każdej pozycji.

     Uwaga: Tabela 126 na stronie 243 pokazuje, jakie pozycje kroniki są zapisywane dla każdego komunikatu o naruszeniu uprawnień.

Inne techniki monitorowania ochrony

Kronika kontroli ochrony (QAUDJRN) jest podstawowym źródłem informacji związanych ze zdarzeniami dotyczącymi ochrony w systemie. Przedstawione poniżej sekcje omawiają inne sposoby obserwowania zdarzeń dotyczących ochrony oraz wartości systemowych w systemie.

Dodatkowe informacje zawiera Dodatek G, “Komendy i menu dla komend ochrony”, na stronie 619. Ten dodatek obejmuje przykłady użycia komend oraz informacje dotyczące menu dla narzędzi serwisowych.

Monitorowanie komunikatów ochrony

Niektóre zdarzenia związane z ochroną, takie jak nieprawidłowe próby wpisania się, powodują powstanie komunikatu w kolejce komunikatów QSYSOPR. W bibliotece QSYS można także utworzyć oddzielną kolejkę komunikatów QSYSMSG.

Jeśli kolejka komunikatów QSYSMSG została utworzona w bibliotece QSYS, komunikaty dotyczące krytycznych zdarzeń systemowych wysyłane są do niej oraz do kolejki QSYSOPR. Kolejka komunikatów QSYSMSG może być monitorowana oddzielnie przez program lub operatora systemu. Zapewnia to dodatkową ochronę zasobów systemu. Krytyczne komunikaty systemowe w kolejce QSYSOPR są czasem pomijane z powodu ilości komunikatów wysyłanych do tej kolejki.

Korzystanie z protokołu historii

Niektóre zdarzenia związane z ochroną, takie jak przekroczenie ilości nieprawidłowych prób wpisania się, określonych w wartości systemowej QMAXSIGN, powodują powstanie komunikatu wysyłanego do protokołu QHST (historia). Komunikaty ochrony mają zakres od 2200 do 22FF. Mają przedrostki CPI, CPF, CPC, CPD i CPA.

Począwszy od Wersji 2 Wydanie 3 programu licencjonowanego OS/400, niektóre komunikaty błędów uprawnień i naruszenia integralności nie są już wysyłane do protokołu QHST (historii). Wszystkie informacje, które były dostępne w protokole QHST, można uzyskać z kroniki kontroli ochrony. Protokołowanie informacji w kronice kontroli zapewnia

lepszą wydajność systemu oraz pełniejsze informacje dotyczące tych zdarzeń związanych z ochroną, niż protokół QHST. Protokół QHST nie powinien być traktowany, jak pełne źródło informacji o naruszeniach ochrony. Zamiast niego należy używać funkcji kontroli ochrony.

W protokole QHST już nie są zapisywane następujące komunikaty:

- CPF2218. Te zdarzenia mogą być przechwycone w kronice kontroli, przez podanie parametru *AUTFAIL dla wartości systemowej QAUDLVL.
- CPF2240. Te zdarzenia mogą być przechwycone w kronice kontroli, przez podanie parametru *AUTFAIL dla wartości systemowej QAUDLVL.

Używanie kronik do monitorowania aktywności obiektu

Jeśli dla kontroli działania systemu (wartość systemowa QAUDLVL) podany zostanie parametr *AUTFAIL, system zapisuje pozycję kroniki kontroli dla każdej niepomyślnej próby dostępu do zasobu. W przypadku krytycznych obiektów, można także ustawić kontrolę obiektu, tak że system będzie zapisywał pozycję kroniki kontroli dla każdego pomyślnego dostępu.

Kronika kontroli zapisuje jedynie, że uzyskano dostęp do obiektu. Nie protokołuje każdej transakcji dla obiektu. W przypadku krytycznych obiektów, wymagane są bardziej szczegółowe informacje, dotyczące danych, do których uzyskano dostęp oraz które zostały zmienione. Kronikowanie obiektu może udostępnić takie szczegóły. Podstawową funkcją kronikowania obiektu jest zapewnienie jego integralności oraz możliwości odzyskania. Listę typów obiektów, które mogą być kronikowane, oraz oraz wykaz informacji są kronikowane dla każdego typu obiektu zawiera sekcja Zarządzanie kroniką w Centrum informacyjnym. W celu przeglądania zmian obiektu, te pozycje kroniki mogą być używane także przez szefa ochrony lub kontrolera. Obiektów nie należy kronikować w kronice QAUDJRN.

Pozycje kroniki obejmują:

- identyfikację zadania, użytkownika oraz godziny dostępu,
- obrazy wszystkich zmian obiektu przed i po,
- rekordy informujące o tym, kiedy obiekt został otwarty, zamknięty, zmieniony, zeskładowany, itp.

Pozycja kroniki nie może być zmieniona przez żadnego użytkownika, nawet przez szefa ochrony. Cała kronika lub dziennik może zostać usunięta, ale jest to łatwe do wykrycia.

Jeśli kronikowane są zbiory, a użytkownik chce wydrukować wszystkie informacje dotyczące danego zbioru, należy wpisać następującą komendę:

```
DSPJRN JRN(biblioteka/kronika) +
       FILE(biblioteka/zbiór) OUTPUT(*PRINT)
```

Na przykład jeśli do zapisywania informacji dotyczących zbioru CUSTFILE (z biblioteki CUSTLIB) wykorzystywana jest kronika JRNCUST z biblioteki CUSTLIB, komenda będzie wyglądała następująco:

```
DSPJRN JRN(CUSTLIB/JRNCUST) +
       FILE(CUSTLIB/CUSTFILE) OUTPUT(*PRINT)
```

Jeśli kronikowane są inne typy obiektów, a użytkownik chce przejrzeć informacje na temat danego obiektu, należy wpisać:

```
DSPJRN JRN(biblioteka/kronika)
       OUTPUT(*OUTFILE)
       OUTFILEFMT(*TYPE5)
       OUTFILE(biblioteka/zbiór_wyjściowy)
       ENTDTALEN(*CALC)
```

Następnie można użyć zapytania lub programu SQL, aby wybrać wszystkie rekordy z tego zbioru wyjściowego dotyczące konkretnego obiektu.

Aby dowiedzieć się, jakie kroniki znajdują się w systemie, należy użyć komendy Praca z kroniką (Work with Journals - WRKJRN). Aby dowiedzieć się, jakie obiekty są kronikowane przez daną kronikę, należy użyć komendy Praca z atrybutami kroniki (Work with Journal Attributes - WRKJRNA).

Pełne informacje dotyczące kronikowania zawiera temat Zarządzanie kroniką.

Analizowanie profili użytkowników

Komenda Wyświetlenie uprawnionych użytkowników (Display Authorized Users - DSPAUTUSR) umożliwia wyświetlenie lub wydrukowanie pełnej listy wszystkich użytkowników w systemie. Lista może być posortowana według nazwy profilu lub profilu grupowego. Poniższy przykład przedstawia listę posortowaną według profili grupowych:

```
                    Wyświetlenie uprawnionych użytkowników
                          (Display Authorized Users)

                         Hasło -
Profil       Profil      Ostatnia    Brak
grupowy      użytkownika zmiana      Hasła   Tekst
DPTSM
             ANDERSOR    08/04/0x            Roger Anders
             VINCENTM    09/15/0x            Mark Vincent
DPTWH
             ANDERSOR    08/04/0x            Roger Anders
             WAGNERR     09/06/0x            Rose Wagner
QSECOFR
             JONESS      09/20/0x            Sharon Jones
             HARRISOK    08/29/0x            Ken Harrison
*NO GROUP
             DPTSM       09/05/0x    X       Sales and Marketing
             DPTWH       08/13/0x    X       Warehouse
             RICHARDS    09/05/0x            Janet Richards
             SMITHJ      09/18/0x            John Smith
```

Drukowanie wybranych profili użytkowników

Utworzony za pomocą komendy Wyświetlenie profilu użytkownika (Display User Profile - DSPUSRPRF) zbiór wyjściowy można przetwarzać za pomocą narzędzia zapytań.

```
DSPUSRPRF USRPRF(*ALL) +
          TYPE(*BASIC) OUTPUT(*OUTFILE)
```

Narzędzie zapytań pozwala utworzyć wiele różnych raportów z analizy zbioru wyjściowego, na przykład:

- listę wszystkich użytkowników mających uprawnienia specjalne *ALLOBJ i *SPLCTL,
- listę wszystkich użytkowników posortowaną według dowolnego pola w profilu użytkownika, na przykład według programów początkowych lub klas użytkowników.

Można tworzyć programy zapytań generujące na podstawie utworzonego zbioru wyjściowego różne raporty. Na przykład:

- wyświetlić wszystkie profile użytkowników z uprawnieniami specjalnymi, wybierając rekordy, w których pole UPSPAU jest różne od *NONE,
- wyświetlić wszystkich użytkowników, którzy mogą uruchamiać komendy, wybierając rekordy, w których pole *Ograniczenie możliwości* (o nazwie UPLTCP w modelowym zbiorze wyjściowym bazy danych) ma wartość *NO lub *PARTIAL,
- wyświetlać wszystkich użytkowników z określonym menu lub programem początkowym,
- wyświetlać użytkowników nieaktywnych na podstawie pola z datą ostatniego wpisania się,

- wyświetlać wszystkich użytkowników, którzy nie mają haseł działających na poziomach 0 i 1, wybierając rekordy, dla których pole Hasło obecne dla poziomu 0 lub 1 (nazywanego UPENPW w modelowym zbiorze wyjściowym) jest równe N,
- wyświetlać wszystkich użytkowników, którzy mają hasła działające na poziomach 2 i 3, wybierając rekordy, dla których pole Hasło obecne dla poziomu 2 lub 3 (nazywanego UPENPH w modelowym zbiorze wyjściowym) jest równe Y,

Badanie dużych profili użytkowników

Przypadkowo rozmieszczone w systemie profile użytkowników o dużej liczbie uprawnień są oznaką źle zaplanowanej ochrony. Poniżej opisano jedną z metod odnajdywania dużych profili użytkowników i ich oceny:

1. Użyj komendy Wyświetlenie opisu obiektu (Display Object Description - DSPOBJD), aby utworzyć zbiór wyjściowy zawierający informacje o wszystkich profilach użytkowników w systemie:

   ```
   DSPOBJD OBJ(*ALL) OBJTYPE(*USRPRF) +
           DETAIL(*BASIC) OUTPUT(*OUTFILE)
   ```

2. Utwórz program z zapytaniem wyświetlający nazwę i wielkość każdego profilu użytkownika w kolejności malejącej.
3. Wydrukuj szczegółowe informacje o największych profilach użytkowników i oceń uprawnienia oraz obiekty należące do tych profili:

   ```
   DSPUSRPRF USRPRF(nazwa_profilu_użytkownika) +
             TYPE(*OBJAUT) OUTPUT(*PRINT)
   DSPUSRPRF USRPRF(nazwa_profilu_użytkownika) +
             TYPE(*OBJOWN) OUTPUT(*PRINT)
   ```

   Niektóre profile użytkowników IBM są bardzo duże, ponieważ są właścicielami wielu obiektów. Wyświetlanie ich listy i analizowanie ich nie jest konieczne. Należy jednak sprawdzić, czy w systemie nie ma programów adoptujących uprawnienia profili użytkowników IBM z uprawnieniem specjalnym *ALLOBJ, takich jak QSECOFR i QSYS. Patrz “Analizowanie programów adoptujących uprawnienia”.

   Dodatek B udostępnia informacje dotyczące wszystkich profili użytkowników IBM oraz ich funkcji.

Analizowanie uprawnień do obiektu

Aby określić, kto ma uprawnienia do bibliotek w systemie, można użyć poniższej metody:

1. Za pomocą komendy DSPOBJD wyświetl wszystkie biblioteki w systemie:

   ```
   DSPOBJD OBJ(QSYS/*ALL) OBJTYPE(*LIB) ASPDEV(*ALLAVL) OUTPUT(*PRINT)
   ```

2. Aby wyświetlić uprawnienia do określonej biblioteki, można użyć komendy Wyświetlenie uprawnień dla obiektu (Display Object Authority - DSPOBJAUT).

   ```
   DSPOBJAUT OBJ(nazwa_biblioteki) OBJTYPE(*LIB) +
             ASPDEV(nazwa_urządzenia_asp) OUTPUT(*PRINT)
   ```

3. Aby wyświetlić obiekty w bibliotece, użyj komendy Wyświetlenie biblioteki (Display Library - DSPLIB):

   ```
   DSPLIB LIB(nazwa_biblioteki) ASPDEV(nazwa_urządzenia_asp) OUTPUT(*PRINT)
   ```

Za pomocą tych raportów można określić, co zawiera biblioteka i kto ma do niej dostęp. W razie potrzeby można użyć komendy DSPOBJAUT, aby dodatkowo wyświetlić uprawnienia do wybranych obiektów w bibliotece.

Analizowanie programów adoptujących uprawnienia

Programy, które adoptują uprawnienie specjalne *ALLOBJ, stanowią zagrożenie ochrony. Za pomocą poniższej metody można wyszukać i sprawdzić te programy:

1. Dla każdego użytkownika z uprawnieniem specjalnym *ALLOBJ użyj komendy Wyświetlenie programów, które adoptują uprawnienia (Display Programs That Adopt - DSPPGMADP), aby wyświetlić programy, które adoptują uprawnienia użytkownika:

   ```
   DSPPGMADP USRPRF(nazwa_profilu_użytkownika) +
             OUTPUT(*PRINT)
   ```

   Uwaga: Sekcja “Drukowanie wybranych profili użytkowników” na stronie 269 pokazuje, jak wyświetlić użytkowników z uprawnieniem *ALLOBJ.

2. Za pomocą komendy DSPOBJAUT określ, kto ma uprawnienia do używania każdego programu adoptującego uprawnienia, i jakie są publiczne uprawnienia do programu:

   ```
   DSPOBJAUT OBJ(nazwa_biblioteki/nazwa_programu) +
             OBJTYPE(*PGM) ASPDEV(nazwa_urządzenia_asp) OUTPUT(*PRINT)
   ```

3. Sprawdź kod źródłowy i opis programu, aby oszacować, czy:
   - Użytkownik programu uruchamianego z adoptowanym profilem nie ma dostępu do zbyt dużej ilości funkcji, takich jak wiersz komend.
   - Program adoptuje minimalny poziom uprawnień potrzebny do realizacji zamierzonych zadań. Istnieje możliwość napisania aplikacji, które wykorzystują błędy w programie, używające tego samego profilu właściciela dla obiektów i programów. W sytuacji, gdy uprawnienia właściciela programu są adoptowane, użytkownik ma uprawnienie *ALL do obiektów aplikacji. W wielu przypadkach profil właściciela nie wymaga uprawnień specjalnych.
4. Za pomocą komendy DSPOBJD sprawdź datę ostatniej modyfikacji programu:

   ```
   DSPOBJD OBJ(nazwa_biblioteki/nazwa_programu) +
           OBJTYPE(*PGM) ASPDEV(nazwa_urządzenia_asp) DETAIL(*FULL)
   ```

Sprawdzanie obiektów, które zostały zmienione

Za pomocą komendy Sprawdzenie integralności obiektu (Check Object Integrity - CHKOBJITG) można wyszukać obiekty, które zostały zmodyfikowane. Zmodyfikowany obiekt często wskazuje, że jakiś użytkownik próbował zmienić dane w systemie. Komendę tę warto uruchomić po:

- odtwarzaniu programów w systemie,
- użyciu dedykowanych narzędzi serwisowych (DST).

Po uruchomieniu komendy system tworzy zbiór bazy danych zawierający informacje o potencjalnych problemach związanych z integralnością danych. Można sprawdzić obiekty należące do jednego lub więcej profili, obiekty, które znajdują się w danej ścieżce, lub wszystkie obiekty w systemie. Można wyszukać obiekty, których domena została zmieniona, oraz obiekty, które zmieniano. Można ponownie obliczyć wartości sprawdzania programu, aby wyszukać obiekty typu *PGM, *SRVPGM, *MODULE i *SQLPKG, które zostały zmienione. Można sprawdzić podpisy obiektów, które zostały podpisane cyfrowo. Można sprawdzić, czy manipulowano w bibliotekach i komendach. Można także uruchomić skanowanie lub sprawdzanie zintegrowanego systemu plików, jeśli obiekty nie przeszły poprzedniego skanowania systemu plików.

Uruchomienie programu CHKOBJITG wymaga uprawnienia specjalnego *AUDIT. Czas wykonania komendy może być długi ze względu na ilość skanowania i obliczeń, jakie są wykonywane. Dlatego należy ją uruchamiać przy małym obciążeniu systemu. Większość komend IBM zduplikowanych z wydań wcześniejszych niż V5R2 będzie protokołowanych jako naruszenia. Te komendy powinny zostać usunięte i utworzone ponownie za pomocą komendy CRTDUPOBJ (Tworzenie duplikatu obiektu - Create duplicate object) za każdym razem, gdy ładowane jest nowe wydanie.

Sprawdzanie systemu operacyjnego

Za pomocą funkcji API Check System (QYDOCHKS) można sprawdzić, czy jakiś kluczowy obiekt systemu operacyjnego został zmieniony od czasu jego podpisania. Każdy obiekt, który nie był podpisany lub został zmieniony od czasu ostatniego podpisania, będzie raportowany jako mający błąd Only signatures (Tylko podpisy) z poprawnego zaufanego źródła systemowego.

Uruchomienie funkcji API QYDOCHKS wymaga uprawnień specjalnych *AUDIT. Działanie funkcji API może zająć długi czas, z powodu wykonywanych obliczeń. Dlatego należy ją uruchamiać przy małym obciążeniu systemu.

Kontrola działań szefa ochrony

Istnieje możliwość zapisywania wszystkich działań wykonywanych przez użytkowników z uprawnieniami specjalnymi *ALLOBJ i *SECADM. Aby to zrobić, można użyć wartości kontroli działania w profilu użytkownika:

1. Dla każdego użytkownika z uprawnieniami specjalnymi *ALLOBJ i *SECADM należy użyć komendy CHGUSRAUD, aby ustawić parametr AUDLVL na wartości, których nie obejmują wartości systemowe

QAUDLVL lub QAUDLVL2. Na przykład jeśli wartość systemowa QAUDLVL ustawiona jest na *AUTFAIL, *PGMFAIL, *PRTDTA i *SECURITY, za pomocą poniższej komendy, należy ustawić parametr AUDLVL dla profilu użytkownika szefa ochrony:

```
CHGUSRAUD USER((SECUSER)
          AUDLVL(*CMD *CREATE *DELETE +
                 *OBJMGT *OFCSRV *PGMADP +
                 *SAVRST *SERVICE, +
                 *SPLFDTA *SYSMGT)
```

Uwaga: Tabela 125 na stronie 239 opisuje wszystkie możliwe wartości dla kontroli działania.

2. Profilom użytkowników z uprawnieniami *ALLOBJ i *SECADM należy usunąć uprawnienia specjalne *AUDIT. Zapobiega to zmienianiu przez takich użytkowników parametrów kontroli we własnych profilach.

   Uwaga: Nie można usunąć uprawnień specjalnych profilu QSECOFR. Dlatego nie można zapobiec, aby użytkownicy wpisani jako QSECOFR, nie mogli zmieniać parametrów kontroli w takim profilu. Jednak jeśli użytkownik wpisany jako QSECOFR do zmiany parametrów kontroli korzysta z komendy CHGUSRAUD, w kronice kontroli zapisywana jest pozycja AD.

   Zalecane jest, aby szefowie ochrony (użytkownicy z uprawnieniami specjalnymi *ALLOBJ lub *SECADM) używali własnych profili dla lepszej kontroli. Hasło profilu QSECOFR nie powinno być rozpowszechniane.
3. Należy upewnić się, że wartość systemowa QAUDCTL obejmuje wartość *AUDLVL.
4. Za pomocą komendy DSPJRN należy przejrzeć pozycje w kronice kontroli, korzystając z technik opisanych w sekcji “Analizowanie pozycji kroniki kontroli za pomocą programu Query lub programu użytkownika” na stronie 265.

Dodatek A. Komendy ochrony

Ten dodatek zawiera komendy systemowe związane z ochroną. Można ich używać zamiast menu systemowych, wpisując je w wierszu komend. Komendy podzielone zostały na grupy według zadań.

Więcej szczegółowych informacji na temat zaprezentowanych tutaj komend zawiera temat CL w Centrum informacyjnego. Więcej informacji na ten temat zawiera sekcja “Informacje wstępne i pokrewne” na stronie xvi. Tabele w sekcji Dodatek D prezentują uprawnienia wymagane do korzystania z tych komend.

Tabela 128. Komendy do pracy z magazynami uprawnień

Nazwa komendy	Nazwa opisowa	Funkcja
CRTAUTHLR	Tworzenie magazynu uprawnień (Create Authority Holder)	Umożliwia zabezpieczenie zbioru przed jego powstaniem. Magazyny uprawnień są poprawne tylko dla zbiorów bazy danych opisanych przez program.
DLTAUTHLR	Usunięcie magazynu uprawnień (Delete Authority Holder)	Umożliwia usunięcie magazynu uprawnień. Jeśli zbiór istnieje, informacje magazynu uprawnień kopiowane są do zbioru.
DSPAUTHLR	Wyświetlenie magazynu uprawnień (Display Authority Holder)	Umożliwia wyświetlenie wszystkich magazynów uprawnień w systemie.

Tabela 129. Komendy do pracy z listami autoryzacji

Nazwa komendy	Nazwa opisowa	Funkcja
ADDAUTLE	Dodanie pozycji listy autoryzacji (Add Authorization List Entry)	Umożliwia dodawanie użytkownika do listy autoryzacji. Należy podać uprawnienia użytkownika do wszystkich obiektów na liście.
CHGAUTLE	Zmiana pozycji listy autoryzacji (Change Authorization List Entry)	Umożliwia zmianę uprawnień użytkowników do obiektów znajdujących się na liście autoryzacji.
CRTAUTL	Tworzenie listy autoryzacji (Create Authorization List)	Umożliwia tworzenie listy autoryzacji.
DLTAUTL	Usunięcie listy autoryzacji (Delete Authorization List)	Umożliwia usunięcie całej listy autoryzacji.
DSPAUTL	Wyświetlenie listy autoryzacji (Display Authorization List)	Umożliwia wyświetlenie listy użytkowników oraz ich uprawnień do listy autoryzacji.
DSPAUTLOBJ	Wyświetlenie obiektów listy autoryzacji (Display Authorization List Objects)	Umożliwia wyświetlenie listy obiektów chronionych przez listę autoryzacji.
EDTAUTL	Edycja listy autoryzacji (Edit Authorization List)	Umożliwia dodawanie, zmienianie i usuwanie użytkowników oraz ich uprawnień do listy autoryzacji.
RMVAUTLE	Usunięcie pozycji listy autoryzacji (Remove Authorization List Entry)	Umożliwia usunięcie użytkownika z listy autoryzacji.
RTVAUTLE	Odtworzenie pozycji listy autoryzacji (Retrieve Authorization List Entry)	Używana w programach CL do pobierania jednej lub więcej wartości związanych z użytkownikiem znajdującym się na liście autoryzacji. Ta komenda może być użyta razem z komendą CHGAUTLE w celu dodania użytkownikowi nowych uprawnień do tych, które już ma.
WRKAUTL	Praca z listami autoryzacji (Work with Authorization Lists)	Umożliwia pracę z listami autoryzacji na ekranie listy.

Tabela 130. Komendy do pracy z uprawnieniami do obiektu oraz kontrolą

Nazwa komendy	Nazwa opisowa	Funkcja
CHGAUD	Zmiana kontroli (Change Auditing)	Umożliwia zmianę wartości kontroli dla obiektu.
CHGAUT	Zmiana uprawnień (Change Authority)	Umożliwia zmianę uprawnień do obiektów dla użytkowników.
CHGOBJAUD	Zmiana kontroli obiektu (Change Object Auditing)	Umożliwia określenie, czy dostęp do obiektu ma być kontrolowany.
CHGOBJOWN	Zmiana właściciela obiektu (Change Object Owner)	Umożliwia przeniesienie prawa własności do obiektu z jednego użytkownika na innego.
CHGOBJPGP	Zmiana grupy podstawowej obiektu (Change Object Primary Group)	Umożliwia zmianę grupy podstawowej dla obiektu na innego użytkownika lub na inną grupę podstawową.
CHGOWN	Zmiana właściciela (Change Owner)	Umożliwia przeniesienie prawa własności do obiektu z jednego użytkownika na innego.
CHGPGP	Zmiana grupy podstawowej (Change Primary Group)	Umożliwia zmianę grupy podstawowej dla obiektu na innego użytkownika lub na inną grupę podstawową.
DSPAUT	Wyświetlenie uprawnień (Display Authority)	Umożliwia wyświetlenie uprawnień użytkowników do obiektu.
DSPOBJAUT	Wyświetlenie uprawnień dla obiektu (Display Object Authority)	Wyświetla właściciela obiektu, uprawnienia publiczne oraz prywatne do obiektu i nazwę listy autoryzacji używanej do zabezpieczania obiektu.
DSPOBJD	Wyświetlenie opisu obiektu (Display Object Description)	Wyświetla poziom kontroli obiektu.
EDTOBJAUT	Edycja uprawnień dla obiektu (Edit Object Authority)	Umożliwia dodawanie, zmianę lub usuwanie uprawnień użytkownika do danego obiektu.
GRTOBJAUT	Nadanie uprawnień dla obiektu (Grant Object Authority)	Umożliwia jawne nadanie uprawnień dla wymienionych użytkowników, wszystkich użytkowników (*PUBLIC) lub użytkowników obiektu odniesienia do obiektów wymienionych w tej komendzie.
RVKOBJAUT	Odwołanie uprawnień dla obiektu (Revoke Object Authority)	Umożliwia usunięcie jednego lub więcej (lub wszystkich) uprawnień nadanych użytkownikowi dla wymienionych obiektów.
WRKAUT	Praca z uprawnieniami (Work with Authority)	Umożliwia pracę z uprawnieniami do obiektu przez wybieranie opcji na ekranie listy.
WRKOBJ	Praca z obiektami (Work with Objects)	Umożliwia pracę z uprawnieniami do obiektu przez wybieranie opcji na ekranie listy.
WRKOBJOWN	Praca z obiektami wg właścicieli (Work with Objects by Owner)	Umożliwia pracę z obiektami, których właścicielem jest profil użytkownika.
WRKOBJPGP	Praca z obiektami wg grupy podstawowej (Work with Objects by Primary Group)	Umożliwia pracę z obiektami, dla których profil jest grupą podstawową, korzystając z opcji ekranu listy.

Tabela 131. Komendy do pracy z hasłami

Nazwa komendy	Nazwa opisowa	Funkcja
CHGDSTPWD	Zmiana hasła narzędzi DST (Change Dedicated Service Tools Password)	Umożliwia zresetowanie możliwości zabezpieczania narzędzi DST do domyślnego hasła.
CHGPWD	Zmiana hasła (Change Password)	Umożliwia użytkownikowi zmianę własnego hasła.
CHGUSRPRF	Zmiana profilu użytkownika (Change User Profile)	Umożliwia zmianę wartości podanych w profilu użytkownika, łącznie z hasłem użytkownika.
CHKPWD	Sprawdzenie hasła (Check Password)	Umożliwia sprawdzenie hasła użytkownika. Na przykład jeśli użytkownik chce ponownie wprowadzić hasło w celu uruchomienia danej aplikacji, w programie CL można użyć komendy CHKPWD do sprawdzenia hasła.
CRTUSRPRF[1]	Tworzenie profilu użytkownika (Create User Profile)	Podczas dodawania nowego użytkownika należy mu przypisać hasło.

1 Uruchamiając komendę CRTUSRPRF, nie można określić, że profil *USRPRF ma być utworzony w niezależnej puli dyskowej (ASP). Jednak jeśli użytkownik ma uprawnienia prywatne do obiektu w niezależnej puli dyskowej, jest właścicielem obiektu w niezależnej puli dyskowej lub jest w grupie podstawowej obiektu w niezależnej puli dyskowej, to nazwa profilu przechowywana jest w niezależnej puli dyskowej. Jeśli niezależna pula dyskowa przenoszona jest do innego systemu, uprawnienia prywatne, prawa własności do obiektu oraz pozycji grupy podstawowej będą dołączone w systemie docelowym do profilu o tej samej nazwie. Jeśli w systemie docelowym dany profil nie istnieje, to zostanie utworzony. Użytkownik nie będzie miał żadnych uprawnień specjalnych, a jego hasło będzie miało wartość *NONE.

Tabela 132. Komendy do pracy z profilami użytkowników

Nazwa komendy	Nazwa opisowa	Funkcja
CHGPRF	Zmiana profilu (Change Profile)	Umożliwia użytkownikowi zminę niekórych atrybutów własnego profilu użytkownika.
CHGUSRAUD	Zmiana kontroli użytkownika (Change User Audit)	Umożliwia podanie działania i kontrolowania obiektu dla profilu użytkownika.
CHGUSRPRF	Zmiana profilu użytkownika (Change User Profile)	Umożliwia zmianę wartości podanych w profilu użytkownika, takich jak hasło użytkownika, uprawnienia specjalne, menu początkowe, biblioteka bieżąca oraz limit priorytetu.
CHKOBJITG	Sprawdzanie integralności obiektu (Check Object Integrity)	Sprawdzenie obiektów, których właścicielem jest co najmniej jeden profil użytkownika, lub sprawdzenie obiektów pasujących do nazwy ścieżki w celu określenia, czy nikt ich nie zmieniał.
CRTUSRPRF	Tworzenie profilu użytkownika (Create User Profile)	Umożliwia dodanie użytkownika do systemu oraz podanie wartości takich jak hasło użytkownika, uprawnienia specjalne, menu początkowe, biblioteka bieżąca oraz limit priorytetu.
DLTUSRPRF	Usunięcie profilu użytkownika (Delete User Profile)	Umożliwia usunięcie z systemu profilu użytkownika. Ta komenda udostępnia opcję usunięcia lub zmiany prawa własności do obiektu, którego właścicielem jest inny profil użytkownika.
DSPAUTUSR	Wyświetlenie uprawnionych użytkowników (Display Authorized Users)	Wyświetla lub drukuje następujące dane dla wszystkich profili użytkowników w systemie: powiązany profil grupowy (jeśli jest), czy profil użytkownika ma hasło, które może być używane na dowolnym poziomie hasła, czy profil użytkownika ma hasło, które może być używane na różnych poziomach haseł, czy profil użytkownika ma hasło, którego można używać z serwerem NetServer, datę ostatniej zmiany hasła i tekst profilu użytkownika.
DSPUSRPRF	Wyświetlenie profilu użytkownika (Display User Profile)	Umożliwia wyświetlenie profilu użytkownika w kilku różnych formatach.
GRTUSRAUT	Nadanie uprawnień użytkownika (Grant User Authority)	Umożliwia kopiowanie uprawnień prywatnych z jednego profilu użytkownika do innego.
PRTPRFINT	Drukowanie wewnętrznych danych profilu (Print Profile Internals)	Umożliwia wydrukowanie raportu, zawierającego wewnętrzne informacje dotyczące liczby pozycji.
PRTUSRPRF	Drukowanie profilu użytkownika (Print User Profile)	Umożliwia analizowanie profili użytkowników, które spełniają podane kryteria.
RTVUSRPRF	Odtwarzanie profilu użytkownika (Retrieve User Profile)	Używana w programach CL do pobierania i korzystania z jednej lub więcej wartości przechowywanych i związanych z profilem użytkownika.
WRKUSRPRF	Praca z profilami użytkowników (Work with User Profiles)	Umożliwia pracę z profilami użytkowników przez wprowadzanie opcji na ekranie listy.

Tabela 133. Pokrewne komendy dotyczące profili użytkownika

Nazwa komendy	Nazwa opisowa	Funkcja
DSPPGMADP	Wyświetlenie programów, które adoptują uprawnienia (Display Programs That Adopt)	Umożliwia wyświetlenie listy programów i pakietów SQL, które adoptują podany profil użytkownika.
RSTAUT	Odtwarzanie uprawnień (Restore Authority)	Umożliwia odtwarzanie uprawnień dla obiektów wstrzymanych przez profil użytkownika, gdy był on składowany. Te uprawnienia mogą być odtworzone tylko po odtworzeniu profilu użytkownika za pomocą komendy Odtworzenie profili użytkowników (Restore User Profile - RSTUSRPRF).
RSTUSRPRF	Odtworzenie profili użytkowników (Restore User Profiles)	Umożliwia odtwarzanie profilu użytkownika oraz jego atrybutów. Odtwarzanie podanych uprawnień do obiektów jest przeprowadzane za pomocą komendy RSTAUT po odtworzeniu profilu użytkownika. Jeśli podano parametr RSTUSRPRF(*ALL), komenda RSTUSRPRF odtwarza także wszystkie listy autoryzacji oraz magazyny uprawnień.
SAVSECDTA	Składowanie danych ochrony (Save Security Data)	Składuje wszystkie profile użytkowników, listy autoryzacji oraz magazyny uprawnień bez korzystania z systemu, który znajduje się w stanie zastrzeżonym.
SAVSYS	Składowanie systemu (Save System)	Składuje wszystkie profile użytkowników, listy autoryzacji i magazyny uprawnień znajdujące się w systemie. Do korzystania z tej funkcji wymagany jest system dedykowany.

Tabela 134. Komendy do pracy z kontrolą

Nazwa komendy	Nazwa opisowa	Funkcja
CHGAUD	Zmiana kontroli (Change Auditing)	Umożliwia określenie kontroli dla obiektu.
CHGDLOAUD	Zmiana kontroli DLO (Change Document Library Object Auditing)	Umożliwia określenie, czy dostęp do obiektu biblioteki dokumentów jest kontrolowany.
CHGOBJAUD	Zmiana kontroli obiektu (Change Object Auditing)	Umożliwia określenie kontroli dla obiektu.
CHGUSRAUD	Zmiana kontroli użytkownika (Change User Audit)	Umożliwia podanie działania i kontrolowania obiektu dla profilu użytkownika.

Tabela 135. Komendy do pracy z obiektami DLO.

Nazwa komendy	Nazwa opisowa	Funkcja
ADDDLOAUT	Dodanie uprawnienia dla DLO (Add Document Library Object Authority)	Umożliwia nadanie użytkownikowi dostępu do dokumentu lub folderu lub zabezpieczenie dokumentu lub folderu za pomocą listy autoryzacji lub kodu dostępu.
CHGDLOAUD	Zmiana kontroli DLO (Change Document Library Object Auditing)	Umożliwia określenie poziomu kontroli obiektu dla obiektu DLO.
CHGDLOAUT	Zmiana uprawnienia dla DLO (Change Document Library Object Authority)	Umożliwia zmianę uprawnienia do dokumentu lub folderu.
CHGDLOOWN	Zmiana właściciela obiektu DLO (Change Document Library Object Owner)	Przenosi prawo własności do dokumentu lub folderu z jednego użytkownika na innego.
CHGDLOPGP	Zmiana grupy podstawowej dla DLO (Change Document Library Object Primary)	Umożliwia zmianę grupy podstawowej dla obiektu biblioteki dokumentów.
DSPAUTLDLO	(Wyświetlenie listy autoryzacji DLO - Display Authorization List Document Library Objects)	Umożliwia wyświetlenie dokumentów i folderów, które zabezpieczane są przez podaną listę autoryzacji.
DSPDLOAUD	Wyświetlenie kontroli obiektu DLO (Display Document Library Object Auditing)	Wyświetla poziom kontroli obiektu dla obiektu biblioteki dokumentów.

Tabela 135. Komendy do pracy z obiektami DLO (kontynuacja).

Nazwa komendy	Nazwa opisowa	Funkcja
DSPDLOAUT	Wyświetlenie uprawnienia dla DLO (Display Document Library Object Authority)	Umożliwia wyświetlenie informacji o uprawnieniach do dokumentu lub folderu.
EDTDLOAUT	Edycja uprawnienia dla DLO (Edit Document Library Object Authority)	Używana do dodawania, zmiany lub usuwania uprawnień użytkownika do dokumentu lub folderu.
GRTUSRPMN	Nadanie uprawnień specjalnych użytkowników (Grant User Permission)	Nadaje uprawnienia użytkownikowi do obsługi dokumentów i folderów lub do zadań biurowych wykonywanych w imieniu innego użytkownika.
RMVDLOAUT	Usuwanie uprawnienia dla DLO (Remove Document Library Object Authority)	Używana do usuwania uprawnień użytkownika do dokumentów lub folderów.
RVKUSRPMN	Odwołanie uprawnień specjalnych użytkowników (Revoke User Permission)	Odbiera uprawnienia do dokumentu jednemu użytkownikowi (lub wszystkim) w celu uzyskania dostępu do dokumentu w imieniu innego użytkownika.

Tabela 136. Komendy do pracy z pozycjami uwierzytelniania serwera

Nazwa komendy	Nazwa opisowa	Funkcja
ADDSVRAUTE	Dodanie pozycji uwierzytelniania serwera (Add Server Authentication Entry)	Umożliwia dodawanie informacji uwierzytelniania serwera dla profilu użytkownika.
CHGSVRAUTE	Zmiana pozycji uwierzytelniania serwera (Change Server Authentication Entry)	Umożliwia zmianę istniejących pozycji uwierzytelniania serwera dla profilu użytkownika.
DSPSVRAUTE	Wyświetlenie pozycji uwierzytelniania serwera (Display Server Authentication Entries)	Umożliwia wyświetlenie pozycji uwierzytelniania serwera dla profilu użytkownika.
RMVSVRAUTE	Usuwanie pozycji uwierzytelniania serwera (Remove Server Authentication Entry)	Umożliwia usuwanie pozycji uwierzytelniania serwera z podanego profilu użytkownika.

Te komendy umożliwiają użytkownikowi podanie nazwy użytkownika, hasła oraz nazwy zdalnego serwera. Dostęp do rozproszonej relacyjnej bazy danych (Distributed Relational Database Access - DRDA) korzysta z tych pozycji w celu uruchomienia żądań dostępu do bazy danych, tak jak podany użytkownik serwera zdalnego.

Tabela 137. Komendy do pracy z katalogiem dystrybucyjnym systemu

Nazwa komendy	Nazwa opisowa	Funkcja
ADDDIRE	Dodanie pozycji katalogu (Add Directory Entry)	Dodaje nowe pozycje do katalogu dystrybucyjnego systemu. Katalog zawiera informacje dotyczące użytkowników, takie jak identyfikator użytkownika i adres, nazwę systemu, nazwę profilu użytkownika, adres pocztowy oraz numer telefonu.
CHGDIRE	Zmiana pozycji katalogu (Change Directory Entry)	Zmienia dane dla podanej pozycji w katalogu dystrybucyjnym systemu. Administrator systemu ma uprawnienia do aktualizowania wszystkich danych zawartych w pozycji katalogu, poza identyfikatorem użytkownika i jego opisem. Użytkownicy mogą aktualizować własne pozycje katalogu, ale są ograniczeni jedynie do pewnych pól.
RMVDIRE	Usuwanie pozycji katalogu (Remove Directory Entry)	Usuwa z katalogu dystrybucyjnego systemu podaną pozycję. Gdy identyfikator użytkownika i adres usuwane są z katalogu, to usuwane są także ze wszystkich list dystrybucyjnych.
WRKDIRE	Praca z katalogiem (Work with Directory)	Udostępnia zestaw ekranów umożliwiających użytkownikowi przeglądanie, dodawanie, zmienianie o usuwanie pozycji z katalogu dystrybucyjnego systemu.

Tabela 138. Komendy do pracy z listami sprawdzania

Nazwa komendy	Nazwa opisowa	Funkcja
CRTVLDL	Tworzenie listy sprawdzania (Create Validation List)	Umożliwia tworzenie obiektu listy sprawdzania zawierającego pozycje składające się z identyfikatora, danych, które będą szyfrowane przez system podczas składowania oraz dane w dowolnym formacie.
DLTVLDL	Usunięcie listy sprawdzania (Delete Validation List)	Umożliwia usunięcie z biblioteki podanej listy sprawdzania.

Tabela 139. Komendy do pracy z informacjami o używaniu funkcji

Nazwa komendy	Nazwa opisowa	Funkcja
CHGFCNUSG	Zmiana użycia funkcji (Change function usage)	Umożliwia zmianę informacji o używaniu dla zarejestrowanej funkcji.
DSPFCNUSG	Wyświetlenie użycia funkcji (Display function usage)	Umożliwia wyświetlenie listy identyfikatorów funkcji oraz szczegółowych informacji o używaniu dla podanej funkcji.
WRKFCNUSG	Praca z użyciem funkcji (Work with function usage)	Umożliwia wyświetlenie listy identyfikatorów funkcji oraz zmianę lub wyświetlenie informacji o użyciu funkcji.

Przedstawione poniżej tabele opisują kilka różnych rodzajów narzędzi ochrony. Więcej informacji o narzędziach ochrony zawiera sekcja Dodatek G, “Komendy i menu dla komend ochrony”.

Tabela 140. Narzędzia ochrony do pracy z kontrolą

Nazwa komendy	Nazwa opisowa	Funkcja
CHGSECAUD	Zmiana kontroli ochrony (Change Security Auditing)	Umożliwia konfigurowanie kontroli ochrony oraz zmianę wartości systemowych, które sterują kontrolą ochrony.
DSPAUDJRNE	Wyświetlenie pozycji kroniki kontroli (Display Audit Journal Entries)	Umożliwia wyświetlenie lub drukowanie informacji o pozycjach w kronice kontroli ochrony. Można wybrać określone typy pozycji, użytkowników i przedział czasu.
DSPSECAUD	Wyświetlenie wartości kontroli ochrony (Display Security Auditing Values)	Umożliwia wyświetlenie informacji o kronice kontroli ochrony i wartościach systemowych, które sterują kontrolą ochrony.

Tabela 141. Narzędzia ochrony do pracy z uprawnieniami

Nazwa komendy	Nazwa opisowa	Funkcja
PRTJOBDAUT	Drukowanie uprawnień opisu dla zadania (Print Job Description Authority)	Umożliwia drukowanie listy opisów zadań, których uprawnienia publiczne nie mają wartości *EXCLUDE. Tej komendy można użyć do drukowania informacji dotyczących opisów zadań określających profil użytkownika, do którego ma dostęp każdy użytkownik w systemie.
PRTPUBAUT	Drukowanie obiektów z uprawnieniami publicznymi (Print Publicly Authorized Objects)	Umożliwia drukowanie listy obiektów podanego typu, których uprawnienia publiczne są inne niż *EXCLUDE.
PRTPVTAUT	Drukowanie uprawnień prywatnych (Print Private Authorities)	Umożliwia drukowanie listy uprawnień prywatnych dla obiektów podanego typu.
PRTQAUT	Drukowanie uprawnień dla kolejki (Print Queue Authoriy)	Umożliwia drukowanie ustawień ochrony dla kolejek wyjściowych oraz kolejek zadań w systemie. Ustawienia te określają, kto może przeglądać i zmieniać pozycje w kolejce wyjściowej lub kolejce zadań.
PRTSBSDAUT	Drukowanie uprawnień opisu podsystemu (Print Subsystem Description Authority)	Umożliwia drukowanie listy opisów podsystemów w bibliotece, które zawierają użytkownika domyślnego w pozycji podsystemu.

Tabela 141. Narzędzia ochrony do pracy z uprawnieniami (kontynuacja)

Nazwa komendy	Nazwa opisowa	Funkcja
PRTTRGPGM	Drukowanie programów wyzwalaczy (Print Trigger Programs)	Umożliwia drukowanie listy programów wyzwalaczy, które są powiązane ze zbiorami bazy danych w systemie.
PRTUSROBJ	Drukowanie obiektów użytkownika (Print User Objects)	Umożliwia drukowanie listy obiektów użytkowników (obiektów, które nie są dostarczane przez IBM), które znajdują się w bibliotece.

Tabela 142. Narzędzia ochrony do pracy z ochroną systemu

Nazwa komendy	Nazwa opisowa	Funkcja
CHGSECA [1]	Zmiana atrybutów ochrony (Change Security Attributes)	Umożliwia ustawienie nowych wartości początkowych do generowania numerów ID użytkownika lub numerów ID grupy. Użytkownicy mogą podać początkowy numer ID użytkownika oraz początkowy numer ID grupy.
CFGSYSSEC	Konfigurowanie ochrony systemu (Configure System Security)	Umożliwia ustawienie wartości systemowych dotyczących ochrony do ich zalecanych ustawień. Komenda ta konfiguruje również kontrolę ochrony w systemie.
CLRSVRSEC	Usuwanie zawartości danych ochrony serwera (Clear Server Security Data)	Umożliwia usunięcie możliwych do rozszyfrowania informacji uwierzytelniania, które są związane z profilami użytkowników oraz pozycjami list sprawdzających (*VLDL). **Uwaga:** Są to te same informacje, które były usuwane w wydaniach wcześniejszych niż V5R2, gdy wartość systemowa QRETSVRSEC była zmieniana z '1' na '0'.
DSPSECA	Wyświetlenie atrybutów ochrony (Display Security Attributes)	Umożliwia wyświetlenie bieżących i oczekujących wartości niektórych atrybutów ochrony systemu.
PRTCMNSEC	Drukowanie ochrony komunikacji (Print Communications Security)	Umożliwia drukowanie atrybutów ochrony obiektów *DEVD, *CTL i *LIND.
PRTSYSSECA	Drukowanie atrybutów ochrony systemu (Print System Security Attributes)	Umożliwia drukowanie listy wartości systemowych dotyczących ochrony oraz atrybutów sieciowych. Raport zawiera wartość bieżącą i zalecaną.
RVKPUBAUT	Odwołanie uprawnień publicznych (Revoke Public Authority)	Umożliwia ustawienie uprawnień publicznych na wartość *EXCLUDE dla zestawu komend istotnych dla ochrony.

[1] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *SECADM.

Szczegółowe informacje na temat narzędzi oraz sugestie dotyczące używania narzędzi znajdują się w podręczniku *Tips for Making Your iSeries 400 Secure*, GC41-0615.

Dodatek B. Profile użytkowników dostarczane przez IBM

Ten dodatek zawiera informacje dotyczące profili użytkowników, które są dostarczane razem z systemem. Te profile używane są jako właściciele obiektów przez różne funkcje systemowe. Niektóre funkcje systemowe działają także tylko pod kontrolą profili użytkowników dostarczanych przez IBM.

Tabela 143 opisuje wartości domyślne, które są używane przez wszystkie profile użytkowników IBM oraz przez komendę Tworzenie profilu użytkownika (Create User Profile - CRTUSRPRF). Parametry są ułożone według kolejności ich pojawiania się na ekranie Tworzenie profilu użytkownika (Create User Profile).

Tabela 144 opisuje listę profili użytkowników IBM, ich przeznaczenie oraz wartości, które są inne niż domyślne dla profili użytkowników IBM.

Uwaga:

> Tabela 144 obejmuje teraz dodatkowe profile użytkowników, które dostarczane są razem z programami licencjonowanymi. Tabela zawiera tylko **niektóre** profile użytkowników dla programów licencjonowanych, dlatego lista nie jest pełna.

Uwaga:

- Hasło dla profilu SECOFR

  Po zainstalowaniu systemu **należy** zmienić hasło dla profilu QSECOFR. To hasło jest takie samo dla każdego systemu iSeries i do czasu jego zmiany powoduje ryzyko naruszenia ochrony. Jednak **nie** należy zmieniać żadnych innych wartości profili użytkowników IBM. Zmiana tych profili może spowodować nieprawidłowe działanie funkcji systemowych.
- Uprawnienia dla profili użytkowników IBM

  Usuwając uprawnienia do obiektów profili IBM dostarczonych z systemem operacyjnym, należy zachować **ostrożność**. Niektóre profile użytkowników IBM mają nadane uprawnienia prywatne do obiektów dostarczanych razem z systemem operacyjnym. Usunięcie tych uprawnień może spowodować nieprawidłowe działanie funkcji systemowych.

Tabela 143. Wartości domyślne dla profili użytkowników

	Wartości domyślne	
Parametr profilu użytkownika	**Profile użytkowników IBM**	**Ekran Tworzenie profilu użytkownika (Create User Profile)**
Hasło (PASSWORD)	*NONE	*USRPRF[4]
Ustawienie hasła jako wygasłe (PWDEXP)	*NO	*NO
Status (STATUS)	*ENABLED	*ENABLED
Klasa użytkownika (USRCLS)	*USER	*USER
Poziom asysty (ASTLVL)	*SYSVAL	*SYSVAL
Biblioteka bieżąca (CURLIB)	*CRTDFT	*CRTDFT
Program początkowy (INLPGM)	*NONE	*NONE
Menu początkowe (INLMNU)	MAIN	MAIN
Biblioteka menu początkowego	*LIBL	*LIBL
Ograniczone możliwości (LMTCPB)	*NO	*NO
Tekst (TEXT)	*BLANK	*BLANK
Uprawnienia specjalne (SPCAUT)	*ALLOBJ[1] *SAVSYS[1]	*USRCLS[2]
Środowisko specjalne (SPCENV)	*SYSVAL	*SYSVAL
Wyświetlenie informacji wpisania (DSPSGNINF)	*SYSVAL	*SYSVAL

Tabela 143. Wartości domyślne dla profili użytkowników (kontynuacja)

	Wartości domyślne	
Parametr profilu użytkownika	**Profile użytkowników IBM**	**Ekran Tworzenie profilu użytkownika (Create User Profile)**
Okres ważności hasła (PWDEXPITV)	*SYSVAL	*SYSVAL
Ograniczenie sesji urządzeń (LMTDEVSSN)	*SYSVAL	*SYSVAL
Buforowanie klawiatury (KBDBUF)	*SYSVAL	*SYSVAL
Pamięć maksymalna (MAXSTG)	*NOMAX	*NOMAX
Limit priorytetu (PTYLMT)	0	3
Opis zadania (JOBD)	QDFTJOBD	QDFTJOBD
Biblioteka opisu zadania	QGPL	*LIBL
Profil grupowy (GRPPRF)	*NONE	*NONE
Właściciel (OWNER)	*USRPRF	*USRPRF
Uprawnienie grupowe (GRPAUT)	*NONE	*NONE
Typ uprawnień grupowych (GRPAUTTYP)	*PRIVATE	*PRIVATE
Grupy dodatkowe (SUPGRPPRF)	*NONE	*NONE
Kod rozliczeniowy (ACGCDE)	*SYS	*BLANK
Hasło do dokumentu (DOCPWD)	*NONE	*NONE
Kolejka komunikatów (MSGQ)	*USRPRF	*USRPRF
Dostarczenie (DLVRY)	*NOTIFY	*NOTIFY
Ważność (SEV)	00	00
Drukarka (PRTDEV)	*WRKSTN	*WRKSTN
Kolejka wyjściowa (OUTQ)	*WRKSTN	*WRKSTN
Program obsługi klawisza ATTN (ATNPGM)	*NONE	*SYSVAL
Kolejność sortowania (SRTSEQ)	*SYSVAL	*SYSVAL
Identyfikator języka (LANGID)	*SYSVAL	*SYSVAL
Identyfikator kraju lub regionu (CNTRYID)	*SYSVAL	*SYSVAL
Identyfikator kodowanego zestawu znaków (CCSID)	*SYSVAL	*SYSVAL
Ustawienie atrybutów zadania (SETJOBATR)	*SYSVAL	*SYSVAL
Ustawienia narodowe (LOCALE)	*NONE	*SYSVAL
Opcje użytkownika (USROPT)	*NONE	*NONE
Numer identyfikacyjny użytkownika (UID)	*GEN	*GEN
Numer identyfikacyjny grupy (GID)	*NONE	*NONE
Katalog osobisty (HOMEDIR)	*USRPRF	*USRPRF
Uprawnienie (AUT)	*EXCLUDE	*EXCLUDE
Kontrola działania (AUDLVL) [3]	*NONE	*NONE
Kontrolowanie obiektu (OBJAUD) [3]	*NONE	*NONE

1 Gdy poziom ochrony systemu jest zmieniany z poziomu 10 lub 20 na poziom 30 lub wyższy, ta wartość jest usuwana.

2 Gdy profil użytkownika jest tworzony automatycznie na poziomie ochrony 10, klasa użytkownika *USER daje uprawnienia specjalne *ALLOBJ i *SAVSYS.

3 Kontrolowanie działania i obiektu określane jest za pomocą komendy CHGUSRAUD.

4 Wykonując komendę CRTUSRPRF, nie można tworzyć profilu użytkownika (*USRPRF) w niezależnej puli dyskowej. Jednak jeśli użytkownik ma uprawnienia prywatne do obiektu na niezależnej puli dyskowej, jest właścicielem obiektu na niezależnej puli dyskowej lub jest w grupie podstawowej obiektu na niezależnej puli dyskowej, to nazwa profilu przechowywana jest na niezależnej puli dyskowej. Jeśli niezależna pula dyskowa przenoszona jest do innego systemu, uprawnienia prywatne, prawa własności do obiektu oraz pozycji grupy podstawowej będą dołączone w systemie docelowym do profilu o tej samej nazwie. Jeśli w systemie docelowym dany profil nie istnieje, to zostanie utworzony. Użytkownik nie będzie miał żadnych uprawnień specjalnych, a jego hasło będzie miało wartość *NONE.

Tabela 144. Profile użytkowników IBM

Nazwa profilu	Nazwa opisowa	Parametry inne niż wartości domyślne
QADSM	Profil użytkownika ADSM	• USERCLS: *SYSOPR • CURLIB: QADSM • TEXT: ADSM profile used by ADSM server (Profil ADSM używany przez serwer ADSM) • SPCAUT: *JOBCTL, *SAVSYS • JOBD: QADSM/QADSM • OUTQ: QADSM/QADSM
QAFOWN	Profil użytkownika APD	• USRCLS: *PGMR • SPCAUT: *JOBCTL • JOBD: QADSM/QADSM • TEXT: Internal APD User Profile (Wewnętrzny profil użytkownika APD)
QAFUSR	Profil użytkownika APD	• TEXT: Internal APD User Profile (Wewnętrzny profil użytkownika APD)
QAFDFTUSR	Profil użytkownika APD	• INLPGM: *LIBL/QAFINLPG • LMTCPB: *YES • TEXT: Internal APD User Profile (Wewnętrzny profil użytkownika APD)
QAUTPROF	Profil użytkownika uprawnień IBM	
QBRMS	Profil użytkownika BRM	
QCLUMGT	Profil zarządzania klastrem	• STATUS: *DISABLED • MSGQ: *NONE • ATNPGM: *NONE
QCLUSTER	Profil wysokiej dostępności klastra	• SPCAUT: *IOSYSCFG
QCOLSRV	Profil użytkownika usług zbierania informacji centrum zarządzania	
QDBSHR	Profil współużytkowania bazy danych	• AUT: *ADD, *DELETE
QDBSHRDO	Profil współużytkowania bazy danych	• AUT: *ADD, *DELETE
QDCEADM	Profil użytkownika DCE	• PASSWORD: *USRPRF • PWDEXP: *YES • STATUS: *DISABLED • TEXT: *NONE • SPCAUT: *JOBCTL
QDFTOWN	Profil właściciela domyślnego	• PTYLMT: 3
QDIRSRV	Profil użytkownika serwera katalogów OS/400	• LMTCPB: *YES • JOBD: QGPL/QBATCH • DSPSGNINF: *NO • LMTDEVSSN: *NO • DLVRY: *HOLD • SPCENV: *NONE • ATNPGM: *NONE

Tabela 144. Profile użytkowników IBM (kontynuacja)

Nazwa profilu	Nazwa opisowa	Parametry inne niż wartości domyślne
QDLFM	Profil menedżera zbiorów DataLink	• SRTSEQ: *HEX
QDOC	Profil dokumentu	• AUT: *CHANGE
QDSNX	Profil dystrybutora węzła systemów rozproszonych	• PTYLMT: 3 • CCSID: *HEX • SRTSEQ: *HEX
QEJBSVR	Profil użytkownika WebSphere Application Server	
QEJB	Profil użytkownika Enterprise Java	
QFNC	Profil finansowy	• PTYLMT: 3
QGATE	Profil mostu VM/MVS*	• CCSID: *HEX • SRTSEQ: *HEX
QIPP	Profil drukowania internetowego	• MSGQ: QUSRSYS/QIPP
QLPAUTO	Profil automatycznego instalowania programów licencjonowanych	• USRCLS: *SYSOPR • INLMNU: *SIGNOFF • SPCAUT: *ALLOBJ, *JOBCTL ,*SAVSYS, *SECADM, *IOSYSCFG • INLPGM: QSYS/QLPINATO • DLVRY: *HOLD • SEV: 99
QLPINSTALL	Profil instalowania programów licencjonowanych	• USRCLS: *SYSOPR • DLVRY: *HOLD • SPCAUT: *ALLOBJ, *JOBCTL ,*SAVSYS, *SECADM, *IOSYSCFG
QMGTC	Profil Centrum Zarządzania	• JOBD: QSYS/QYPSJOBD
QMSF	Profil struktury serwera poczty	• CCSID: *HEX • SRTSEQ: *HEX
QMQM	Profil użytkownika MQSeries	• USRCLS: *SECADM • SPCAUT: *NONE • PRTDEV: *SYSVAL • TEXT: MQM user which owns the QMQM library (Użytkownik MQM, który jest właścicielem biblioteki QMQM)
QNFSANON	Profil użytkownika NFS	
QNETSPLF	Profil buforowania sieciowego	
QNETWARE	Profil użytkownika ECS	• STATUS: *DISABLED • TEXT: QFPNTWE USER PROFILE (Profil użytkownika QFPNTWE)
QNTP	Profil NTP	• JOBD: QTOTNTP • JOBD LIBRARY: QSYS

Tabela 144. Profile użytkowników IBM (kontynuacja)

Nazwa profilu	Nazwa opisowa	Parametry inne niż wartości domyślne
QOIUSER	Podsystem komunikacyjny OSI	• USRCLS: *SYSOPR • SPCAUT: *JOBCTL, *SAVSYS, *IOSYSCFG • CURLIB: QOSI • MSGQ: QOSI/QOIUSER • DLVRY: *HOLD • OUTQ: *DEV • PRTDEV: *SYSVAL • ATNPGM: *NONE • CCSID: *HEX • TEXT: Internal OSI Communication Subsystem User Profile (Wewnętrzny profil użytkownika podsystemu komunikacyjnego OSI)
QOSIFS	Profil użytkownika serwera plików OSI	• USRCLS: *SYSOPR • SPCAUT: *JOBCTL, *SAVSYS • OUTQ: *DEV • CURLIB: *QOSIFS • CCSID: *HEX • TEXT: Internal OSI File Services User Profile (Wewnętrzny profil użytkownika File Services OSI)
QPGMR	Profil programisty	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1] *SAVSYS *JOBCTL • PTYLMT: 3 • ACGCDE: *BLANK
QPEX	Profil użytkownika programu Performance Explorer	• PTYLMT: 3 • ATNPGM: *SYSVAL • TEXT: IBM-supplied User Profile (Profil użytkownika dostarczany przez IBM)
QPM400	IBM Performance Management for eServer iSeries (PM iSeries)	• SPCAUT: *IOSYSCFG, *JOBCTL
QPRJOWN	Profil użytkownika właściciela części i projektów	• STATUS: *DISABLED • CURLIB: QADM • TEXT: User profile of parts and projects owner (Profil użytkownika właściciela części i projektów)
QRDARSADM	Profil użytkownika R/DARS	• INLMNU: *SIGNOFF • TEXT: R/DARS Administration Profile (Profil administracyjny R/DARS)
QRDAR	Profil właściciela R/DARS	• USRCLS: *PGMR • INLMNU: *SIGNOFF • OUTQ: *DEV • TEXT: R/DARS-400 owning profile (Profil właściciela R/DARS-400)
QRDARS4001	Profil właściciela R/DARS 1	• INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: R/DARS-400 owning profile 1 (Profil właściciela R/DARS-400 1)

Tabela 144. Profile użytkowników IBM (kontynuacja)

Nazwa profilu	Nazwa opisowa	Parametry inne niż wartości domyślne
QRDARS4002	Profil właściciela R/DARS 2	• INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: R/DARS-400 owning profile 2 (Profil właściciela R/DARS-400 2)
QRDARS4003	Profil właściciela R/DARS 3	• INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: R/DARS-400 owning profile 3 (Profil właściciela R/DARS-400 3)
QRDARS4004	Profil właściciela R/DARS 4	• INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: R/DARS-400 owning profile 4 (Profil właściciela R/DARS-400 4)
QRDARS4005	Profil właściciela R/DARS 5	• INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: R/DARS-400 owning profile 5 (Profil właściciela R/DARS-400 5)
QRMTCAL	Profil użytkownika zdalnego kalendarza	• TEXT: OfficeVision Remote Calendar User (Użytkownik zdalnego kalendarza OfficeVision)
QRJE	Profil zadania uruchamianego zdalnie	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1] *SAVSYS [1] *JOBCTL
QSECOFR	Profil szefa ochrony	• PWDEXP: *YES • USRCLS: *SECOFR • SPCAUT: *ALLOBJ, *SAVSYS, *JOBCTL, *SECADM, *SPLCTL, *SERVICE, *AUDIT, *IOSYSCFG • UID: 0 • PASSWORD: QSECOFR
QSNADS	Profil usług dystrybucyjnych SNA	• CCSID: *HEX • SRTSEQ: *HEX
QSOC	Profil użytkownika OptiConnect	• USRCLS: *SYSOPR • CURLIB: *QSOC • SPCAUT: *JOBCTL • MSGQ: QUSRSYS/QSOC
QSPL	Profil buforowania	
QSPLJOB	Profil zadania buforowania	• AUT: *USE
QSRV	Profil usługi	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1], *SAVSYS [1], *JOBCTL, *SERVICE • ASTLVL: *INTERMED • ATNPGM: QSYS/QSCATTN
QSRVAGT	Profil użytkownika aplikacji Service Agent	

Tabela 144. Profile użytkowników IBM (kontynuacja)

Nazwa profilu	Nazwa opisowa	Parametry inne niż wartości domyślne
QSRVBAS	Profil serwisu podstawowego	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1] *SAVSYS [1] *JOBCTL • ASTLVL: *INTERMED • ATNPGM: QSYS/QSCATTN
QSVCCS	Profil użytkownika CC Server	• USRCLS: *SYSOPR • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: CC Server User Profile (Profil użytkownika CC Server)
QSVCM	Profil użytkownika serwera Client Management Server	• TEXT: Client Management Server User Profile (Profil użytkownika serwera Client Management Server)
QSVSM	Profil użytkownika ECS	• USRCLS: *SYSOPR • STATUS: *DISABLED • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: SystemView System Manager User Profile (Profil użytkownika SystemView System Manager)
QSVSMSS	Profil użytkownika usług systemu zarządzanego	• STATUS: *DISABLED • USRCLS: *SYSOPR • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Managed System Service User Profile (Profil użytkownika usług systemu zarządzanego)
QSYS	Profil systemu	• USRCLS: *SECOFR • SPCAUT: *ALLOBJ, *SECADM, *SAVSYS, *JOBCTL, *AUDIT, *SPLCTL, *SERVICE, *IOSYSCFG
QSYSOPR	Profil operatora systemu	• USRCLS: *SYSOPR • SPCAUT: *ALLOBJ [1], *SAVSYS, *JOBCTL • INLMNU: SYSTEM • LIBRARY: *LIBL • MSGQ: QSYSOPR • DLVRY: *BREAK • SEV: 40
QTCM	Profil menedżera wyzwalanej pamięci podręcznej	• STATUS: *DISABLED
QTCP	Profil protokołu Transmission control protocol (TCP)	• USRCLS: *SYSOPR • SPCAUT: *JOBCTL • CCSID: *HEX • SRTSEQ: *HEX
QTFTP	Protokół Trivial File Transfer Protocol	

Tabela 144. Profile użytkowników IBM (kontynuacja)

Nazwa profilu	Nazwa opisowa	Parametry inne niż wartości domyślne
QTMPLPD	Profil obsługi drukowania Transmission control protocol/Internet protocol (TCP/IP)	• PTYLMT: 3 • AUT: *USE
QTMPLPD	Profil użytkownika zdalnego LPR	• JOBD: QGPL/QDFTJOBD • PWDEXPITV: *NOMAX • MSGQ: QTCP/QTMPLPD
QTMTWSG	Profil użytkownika bramy stacji roboczej HTML	• MSGQ: QUSRSYS/QTMTWSG • TEXT: HTML Workstation Gateway Profile (Profil bramy stacji roboczej HTML)
QTMHHTTP	Profil użytkownika bramy stacji roboczej HTML	• MSGQ: QUSRSYS/QTMHHTTP • TEXT: HTTP Server Profile (Profil serwera HTTP)
QTMHHTP1	Profil użytkownika bramy stacji roboczej HTML	• MSGQ: QUSRSYS/QTMHHTTP • TEXT: HTTP Server CGI Profile (Profil CGI serwera HTTP)
QTSTRQS	Profil żądania testu	
QUMB	Profil użytkownika Ultimedia System Facilities	
QUMVUSER	Profil użytkownika Ultimedia Business Conferencing	
QUSER	Profil użytkownika stacji roboczej	• PTYLMT: 3
QX400	Profil użytkownika OSI Messages Services File Services	• CURLIB: *QX400 • USRCLS: *SYSOPR • MSGQ: QX400/QX400 • DLVRY: *HOLD • OUTQ: *DEV • PRTDEV: *SYSVAL • ATNPGM: *NONE • CCSID: *HEX • TEXT: Internal OSI Messages Services User Profile (Wewnętrzny profil użytkownika OSI Messages Services)
QYCMCIMOM	Profil użytkownika serwera	
QYPSJSVR	Profil serwera Centrum Zarządzania Java	
QYPUOWN	Wewnętrzny profil użytkownika APU	• TEXT: Internal APU — User profile (Wewnętrzny profil użytkownika APU)

[1] Gdy poziom ochrony systemu jest zmieniany z poziomu 10 lub 20 na poziom 30 lub wyższy, ta wartość jest usuwana.

Dodatek C. Komendy z uprawnieniami publicznymi *EXCLUDE

Tabela 145 pokazuje, które komendy mają ograniczoną autoryzację (uprawnienia publiczne *EXCLUDE) ustawioną fabrycznie w dostarczanym systemie. Zawiera także informacje o tym, które profile użytkowników IBM są autoryzowane do korzystania z tych komend. Więcej informacji na temat profili użytkowników IBM zawiera temat “Profile użytkowników IBM” na stronie 110.

Tabela 145 zawiera wykaz komend, a komendy, które są zastrzeżone dla szefa ochrony oraz profilu użytkownika z uprawnieniami *ALLOBJ, oznaczono literą **R**. Komendy, do których uprawnienia ma jeden lub więcej profili użytkowników IBM, oprócz szefa ochrony, oznaczono literą **S** pod nazwą profilu, który ma odpowiednie uprawnienia).

Wszystkie komendy niewymienione tutaj są publiczne, co oznacza że mogą być używane przez wszystkich użytkowników. Jednak niektóre komendy wymagają uprawnień specjalnych, takich jak *SERVICE lub *JOBCTL. Uprawnienia specjalne wymagane dla komend zawiera Dodatek D, “Uprawnienia wymagane dla obiektów używanych przez komendy”, na stronie 299

Jeśli dla tych komend mają być nadane uprawnienia innym użytkownikom lub uprawnienia publiczne *USE, należy zaktualizować poniższą tabelę wskazując, że komendy nie są już zastrzeżone w systemie. Używanie niektórych komend może wymagać uprawnień do pewnych obiektów w systemie, a także do samych komend. Uprawnienia do obiektów wymagane dla komend zawiera Dodatek D, “Uprawnienia wymagane dla obiektów używanych przez komendy”, na stronie 299.

Tabela 145. Uprawnienia profili użytkowników IBM do komend zastrzeżonych

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
ADDCLUNODE	R					S
ADDCMDCRQA		S	S	S	S	
ADDCRGDEVE	R					S
ADDCRGNODE	R					S
ADDCRSDMNK	R					
ADDDEVDMNE	R					S
ADDDSTQ		S	S			
ADDDSTRTE		S	S			
ADDDSTSYSN		S	S			
ADDEXITPGM	R					
ADDIMGCLGE	R					
ADDMFS	R					
ADDNETJOBE	R					
ADDOBJCRQA		S	S	S	S	
ADDOPTCTG	R					
ADDOPTSVR	R					
ADDPEXDFN		S		S		
ADDPEXFTR		S		S		
ADDPRDCRQA		S	S	S	S	
ADDPTFCRQA		S	S	S	S	
ADDRPYLE		S				

Tabela 145. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
ADDRSCCRQA		S	S	S	S	
ADDTRCFTR	R					
ANSQST	R					
ANZACCGRP	R					
ANZBESTMDL	R					
ANZDBF	R					
ANZDBFKEY	R					
ANZDFTPWD	R					
ANZJVM		S	S	S	S	
ANZPFRDTA	R					
ANZPGM	R					
ANZPRB		S	S	S	S	
ANZPRFACT	R					
ANZS34OCL	R					
ANZS36OCL	R					
APYJRNCHG		S		S		
APYPTF				S		
APYRMTPTF		S	S	S	S	
CFGDSTSRV		S	S			
CFGRPDS		S	S			
CFGSYSSEC	R					
CHGACTSCDE	R					
CHGCLUCFG	R					S
CHGCLUNODE	R					
CHGCLURCY	R					S
CHGCLUVER	R					S
CHGCMDCRQA		S	S	S	S	
CHGCRG	R					S
CHGCRGDEVE	R					S
CHGCRGPRI	R					S
CHGCRSDMNK	R					
CHGDSTPWD[1]	R					
CHGDSTQ		S	S			
CHGDSTRTE		S	S			
CHGEXPSCDE	R					
CHGFCNARA	R					
CHGGPHFMT	R					
CHGGPHPKG	R					
CHGIMGCLG	R					
CHGIMGCLGE	R					

Tabela 145. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
CHGJOBTRC	R					
CHGJOBTYP	R					
CHGJRN		S	S	S		
CHGLICINF	R					
CHGMGDSYSA		S	S	S	S	
CHGMGRSRVA		S	S	S	S	
CHGMSTK	R					
CHGNETA	R					
CHGNETJOBE	R					
CHGNFSEXP	R					
CHGNWSA	R					
CHGOBJCRQA		S	S	S	S	
CHGOPTA	R					
CHGPEXDFN		S		S		
CHGPRB		S	S	S	S	
CHGPRDCRQA		S	S	S	S	
CHGPTFCRQA		S	S	S	S	
CHGPTR				S		
CHGQSTDB	R					
CHGRCYAP		S	S			
CHGRPYLE		S				
CHGRSCCRQA		S	S	S	S	
CHGSYSLIBL	R					
CHGSYSVAL		S	S	S		
CHGS34LIBM	R					
CHKASPBAL	R					
CHKCMNTRC				S		
CHKPRDOPT		S	S	S	S	
CPHDTA	R					
CPYFCNARA	R					
CPYGPHFMT	R					
CPYGPHPKG	R					
CPYPFRDTA	R					
CPYPTF		S	S	S	S	
CPYPTFGRP		S	S	S	S	
CRTAUTHLR	R					
CRTBESTMDL	R					
CRTCLS	R					
CRTCLU	R					S
CRTCRG	R					S

Tabela 145. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
CRTFCNARA	R					
CRTGPHFMT	R					
CRTGPHPKG	R					
CRTHSTDTA	R					
CRTIMGCLG	R					
CRTJOBD	R					
CRTPFRDTA	R					
CRTLASREP		S				
CRTPEXDT		S		S		
CRTQSTDB	R					
CRTQSTLOD	R					
CRTSBSD		S	S			
CRTUDFS	R					
CRTUDFS	R					
CRTVLDL	R					
CVTBASSTR	R					
CVTBASUNF	R					
CVTBGUDTA	R					
CVTDIR	R					
CVTPFRDTA	R					
CVTPFRTHD	R					
CVTS36CFG	R					
CVTS36FCT	R					
CVTS36JOB	R					
CVTS36QRY	R					
CVTS38JOB	R					
CVTTCPCL		S	S	S	S	
DLTAPARDTA		S	S	S	S	
DLTBESTMDL	R					
DLTCLU	R					S
DLTCMNTRC				S		
DLTCRGCLU	R					S
DLTFCNARA	R					
DLTGPHFMT	R					
DLTGPHPKG	R					
DLTHSTDTA	R					
DLTIMGCLG	R					
DLTLICPGM	R					
DLTPEXDTA		S		S		
DLTPFRDTA	R					

Tabela 145. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
DLTPRB		S	S	S	S	
DLTPTF		S	S	S	S	
DLTQST	R					
DLTQSTDB	R					
DLTRMTPTF		S	S	S	S	
DLTSMGOBJ		S	S	S	S	
DLTUDFS	R					
DLTVLDL	R					
DMPDLO		S	S	S	S	
DMPJOB		S	S	S	S	
DMPJOBINT		S	S	S	S	
DMPJVM		S	S	S	S	
DMPOBJ				S	S	
DMPSYSOBJ		S	S	S	S	
DMPTRC	R	S		S		
DSPACCGRP	R					
DSPDSTLOG	R					
DSPHSTGPH	R					
DSPMFSINF	R					
DSPMGDSYSA		S	S	S	S	
DSPPFRDTA	R					
DSPPFRGPH	R					
DSPPTF		S	S	S	S	
DSPSRVSTS		S	S	S	S	
DSPUDFS	R					
EDTCPCST			S			
EDTQST	R					
EDTRBDAP			S			
EDTRCYAP		S	S			
ENCCPHK	R					
ENCFRMMSTK	R					
ENCTOMSTK	R					
ENDCHTSVR	R					S
ENDCLUNOD	R					S
ENDCMNTRC	R			S		
ENDCRG	R					
ENDDBGSVR		S	S	S	S	
ENDHOSTSVR		S	S	S	S	
ENDIDXMON	R					
ENDIPSIFC		S	S	S	S	

Tabela 145. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
ENDJOBABN		S	S	S		
ENDJOBTRC	R					
ENDMGDSYS		S	S	S	S	
ENDMGRSRV		S	S	S	S	
ENDMSF			S	S	S	
ENDNFSSVR	R		S	S	S	
ENDPEX		S		S		
ENDPFRTRC	R			S		
ENDSRVJOB		S	S	S	S	
ENDSYSMGR		S	S	S	S	
ENDTCP		S	S	S	S	
ENDTCPCNN		S	S	S	S	
ENDTCPIFC		S	S	S	S	
ENDTCPSVR		S	S	S	S	
GENCPHK	R					
GENCRSDMNK	R					
GENMAC	R					
GENPIN	R					
GENS36RPT	R					
GENS38RPT	R					
GRTACCAUT	R					
HLDCMNDEV		S	S	S	S	
HLDDSTQ		S	S			
INSPTF[3]				S		
INSRMTPRD		S	S	S	S	
INZDSTQ		S	S			
INZSYS	R					
LODIMGCLG	R					
LODPTF				S		
LODQSTDB	R					
MGRS36	R					
MGRS36APF	R					
MGRS36CBL	R					
MGRS36DFU	R					
MGRS36DSPF	R					
MGRS36ITM	R					
MGRS36LIB	R					
MGRS36MNU	R					
MGRS36MSGF	R					
MGRS36QRY	R					

Tabela 145. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
MGRS36RPG	R					
MGRS36SEC	R					
MGRS38OBJ	R					
MIGRATE	R					
PKGPRDDST		S	S	S	S	
PRTACTRPT	R					
PRTCMNTRC				S		
PRTCPTRPT	R					
PRTJOBRPT	R					
PRTJOBTRC	R					
PRTLCKRPT	R					
PRTPOLRPT	R					
PRTRSCRPT	R					
PRTSYSRPT	R					
PRTTNSRPT	R					
PRTTRCRPT	R					
PRTDSKINF	R					
PRTERRLOG		S	S	S	S	
PRTINTDTA		S	S	S	S	
PRTPRFINT	R					
PWRDWNSYS	R		S			
RCLOPT	R					
RCLSPLSTG	R					
RCLSTG		S	S	S	S	
RCLTMPSTG		S	S	S	S	
RESMGRNAM	R	S	S	S	S	
RLSCMNDEV		S	S	S	S	
RLSDSTQ		S	S			
RLSIFSLCK	R					
RLSRMTPHS		S	S			
RMVACC	R					
RMVCLUNODE	R					S
RMVCRGDEVE	R					S
RMVCRGNODE	R					S
RMVCRSDMNK	R					
RMVDEVDMNE	R					S
RMVDSTQ		S	S			
RMVDSTRTE		S	S			
RMVDSTSYSN		S	S			
RMVEXITPGM	R					

Tabela 145. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
RMVIMGCLGE	R					
RMVJRNCHG		S		S		
RMVLANADP	R					
RMVMFS	R					
RMVNETJOBE	R					
RMVOPTCTG	R					
RMVOPTSVR	R					
RMVPEXDFN		S		S		
RMVPEXFTR		S		S		
RMVPTF				S		
RMVRMTPTF		S	S	S	S	
RMVRPYLE		S				
RMVTRCFTR	R					
RSTAUT	R					
RST[4]						S
RSTCFG	R					
RSTDLO	R					
RSTLIB	R					
RSTLICPGM	R					
RSTOBJ[4]						S
RSTS36F	R					
RSTS36FLR	R					
RSTS36LIBM	R					
RSTS38AUT	R					
RSTUSFCNR[5]						S
RSTUSRPRF	R					
RTVDSKINF	R					
RTVPRD		S	S	S	S	
RTVPTF		S	S	S	S	
RTVSMGOBJ		S	S	S	S	
RUNLPDA		S	S	S	S	
RUNSMGCMD		S	S	S	S	
RUNSMGOBJ		S	S	S	S	
RVKPUBAUT	R					
SAVAPARDTA		S	S	S	S	
SAVLICPGM	R					
SAVRSTCHG	R					
SAVRSTLIB	R					
SAVRSTOBJ	R					
SBMFNCJOB	R					

Tabela 145. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
SBMNWSCMD	R					
SETMSTK	R					
SNDDSTQ		S	S			
SNDPRD		S	S	S	S	
SNDPTF		S	S	S	S	
SNDPTFORD				S	S	
SNDSMGOBJ		S	S	S	S	
SNDSRVRQS				S	S	
STRBEST	R					
STRCHTSVR	R					S
STRCLUNOD	R					S
STRCMNTRC				S		
STRCRG	R					S
STRDBG		S		S	S	
STRDBGSVR		S	S	S	S	
STRHOSTSVR		S	S	S	S	
STRIDXMON	R					
STRIPSIFC		S	S	S	S	
STRJOBTRC	R					
STRMGDSYS		S	S	S	S	
STRMGRSRV		S	S	S	S	
STRMSF[2]			S	S	S	
STRNFSSVR	R					
STRPEX		S		S		
STRPFRG	R					
STRPFRT	R					
STRPFRTRC	R			S		
STRRGZIDX	R					
STRSRVJOB		S	S	S	S	
STRSST				S		
STRSYSMGR		S	S	S	S	
STRS36MGR	R					
STRS38MGR	R					
STRTCP		S	S	S	S	
STRTCPIFC		S	S	S	S	
STRTCPSVR		S	S	S	S	
STRUPDIDX	R					
TRCCPIC	R					
TRCICF	R					
TRCINT		S		S		

Tabela 145. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
TRCJOB		S	S	S	S	
TRCTCPAPP				S	S	
TRNPIN	R					
VFYCMN		S	S	S	S	
VFYIMGCLG	R					
VFYLNKLPDA		S	S	S	S	
VFYMSTK	R					
VFYPIN	R					
VFYPRT		S	S	S	S	
VFYTAP		S	S	S	S	
WRKCNTINF				S	S	
WRKDEVTBL	R					
WRKDPCQ		S	S			
WRKDSTQ		S	S			
WRKFCNARA	R					
WRKIMGCLGE	R					
WRKJRN		S	S	S		
WRKLICINF	R					
WRKORDINF			S	S		
WRKPEXDFN		S		S		
WRKPEXFTR		S		S		
WRKPGMTBL	R					
WRKPRB		S	S	S	S	
WRKPTFGRP		S	S	S	S	
WRKSRVPVD				S	S	
WRKSYSACT	R					
WRKTXTIDX	R					
WRKUSRTBL	R					

[1] Komenda CHGDSTPWD dostarczana jest z uprawnieniami publicznymi *USE, ale żeby używać tej komendy, użytkownik musi być wpisany jako użytkownik QSECOFR.

[2] Profil użytkownika QMSF także ma uprawnienia do korzystania z tej komendy.

[3] Użytkownik QSRV nie może uruchomić tej komendy podczas IPL.

[4] Oprócz użytkownika QSYS, uprawnienia ma profil użytkownika QRDARS400.

[5] Oprócz użytkownika QSYS, uprawnienia ma profil użytkownika QUMB.

[6] Te komendy są dostarczane z profilem użytkownika QSYS z uprawnieniem *ALL.

Dodatek D. Uprawnienia wymagane dla obiektów używanych przez komendy

Tabele znajdujące się w tym dodatku przedstawiają uprawnienia wymagane przez komendy do obiektów odniesienia. Na przykład w pozycji komendy Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF) w tabeli znajduje się lista wszystkich obiektów, do których użytkownik potrzebuje uprawnień, jak kolejka komunikatów użytkownika, opis zadania i program początkowy.

Tabele ułożone są w porządku alfabetycznym, według typu obiektu. Dodatkowo, dołączono tabele dla elementów, które nie są obiektami OS/400 (zadania, zbiory buforowe, atrybuty sieciowe i wartości systemowe) oraz dla niektórych funkcji (emulacji urządzeń i finansowych). Dodatkowe uwagi (jeśli są) na temat komend ujęto w przypisach do tabel.

Poniżej znajdują się opisy kolumn tabel:

Obiekt odniesienia

Obiekty wyświetlone na liście w kolumnie *Obiekt odniesienia* są obiektami, do których użytkownik potrzebuje uprawnień, używając tej komendy.

Wymagane uprawnienia do obiektu

Uprawnienia wyświetlone w tabeli określają uprawnienia do obiektów i danych wymagane dla obiektu w przypadku użycia komendy. W poniższej tabeli są opisane uprawnienia wymienione w kolumnie *Wymagane uprawnienia*. Opis zawiera przykłady użycia uprawnień. W większości przypadków dostęp do obiektu wymaga kombinacji uprawnień do obiektu i do danych.

Wymagane uprawnienia do biblioteki

W tej kolumnie wymienione są uprawnienia wymagane dla biblioteki zawierającej obiekt. Dla większości operacji, w celu odszukania obiektu wymagane są uprawnienia *EXECUTE. Aby dodać obiekt do biblioteki wymagane są uprawnienia *READ i *ADD. W poniższej tabeli są opisane uprawnienia wymienione w kolumnie *Wymagane uprawnienia*.

Tabela 146. Opis typów uprawnień

Uprawnienie	Nazwa	Dozwolone funkcje
Uprawnienia do obiektu:		
*OBJOPR	Operacyjne do obiektu	Przeglądanie opisu obiektu. Używanie obiektu zgodnie z uprawnieniami użytkownika do danych.
*OBJMGT	Zarządzanie obiektami	Określanie ochrony obiektu. Przenoszenie lub zmiana nazwy obiektu. Wszystkie funkcje zdefiniowane dla uprawnień *OBJALTER i *OBJREF.
*OBJEXIST	Istnienie obiektu	Usunięcie obiektu. Zwalnianie pamięci obiektu. Wykonywanie operacji składowania i odtwarzania obiektu [1]. Przenoszenie prawa własności.
*OBJALTER	Zmiana obiektu	Dodawanie, usuwanie zawartości, inicjowanie i reorganizowanie podzbiorów zbiorów bazy danych. Zmiana i dodawanie atrybutów zbiorów bazy danych: dodawanie i usuwanie wyzwalaczy. Zmiana atrybutów pakietów SQL. Przenoszenie biblioteki lub folderu do innej puli ASP.

Tabela 146. Opis typów uprawnień (kontynuacja)

Uprawnienie	Nazwa	Dozwolone funkcje
*OBJREF	Odniesienie do obiektu	Określanie zbioru bazy danych jako nadrzędnego w ograniczeniu referencyjnym. Na przykład można zdefiniować regułę, że rekord klienta musi istnieć w zbiorze CUSMAS, zanim zamówienie klienta będzie można dodać do zbioru CUSORD. Aby zdefiniować tę regułę, użytkownik musi mieć uprawnienia *OBJREF do zbioru CUSMAS.
*AUTLMGT	Zarządzanie listą autoryzacji	Dodawanie i usuwanie użytkowników oraz ich uprawnień z listy autoryzacji [2].
Uprawnienia do danych:		
*READ	Odczyt (Read)	Wyświetlanie zawartości obiektu - przeglądanie rekordów w zbiorze.
*ADD	Dodanie (Add)	Dodawanie pozycji do obiektu - dodawanie komunikatów do kolejki komunikatów lub rekordów do zbioru.
*UPD	Aktualizacja	Zmienianie pozycji w obiekcie - zmienianie rekordów w zbiorze.
*DLT	Usunięcie (Delete)	Usuwanie pozycji z obiektu - usuwanie komunikatów z kolejki komunikatów lub usuwanie rekordów ze zbioru.
*EXECUTE	Wykonywanie	Uruchamianie programu, programu usługowego lub pakietu SQL. Odszukiwanie obiektu w bibliotece lub katalogu.

1 Jeśli użytkownik ma uprawnienia specjalne do składowania systemu (*SAVSYS), do wykonywania operacji składowania i odtwarzania obiektu uprawnienia do istnienia obiektu nie są wymagane.

2 Więcej informacji znajduje się w podręczniku iSeries Security Reference.

Oprócz tych wartości kolumna *Wymagane uprawnienia* może zawierać zdefiniowane systemowo podzbiory tych uprawnień. W poniższej tabeli są wymienione podzbiory uprawnień do obiektów i danych.

Tabela 147. Uprawnienia zdefiniowane systemowo

Uprawnienie	*ALL	*CHANGE	*USE	*EXCLUDE
Uprawnienia do obiektu				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
Uprawnienia do danych				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X		
*DLT	X	X		
*EXECUTE	X	X	X	

W poniższej tabeli są wymienione dodatkowe podzbiory uprawnień obsługiwanych przez komendy CHGAUT i WRKAUT.

Tabela 148. Uprawnienia zdefiniowane systemowo

Uprawnienie	*RWX	*RW	*RX	*R	*WX	*W	*X
Uprawnienia do obiektu							
*OBJOPR	X	X	X	X	X	X	X
*OBJMGT							

Tabela 148. Uprawnienia zdefiniowane systemowo (kontynuacja)

Uprawnienie	*RWX	*RW	*RX	*R	*WX	*W	*X
*OBJEXIST							
*OBJALTER							
*OBJREF							
Uprawnienia do danych							
*READ	X	X	X	X			
*ADD	X	X			X	X	
*UPD	X	X			X	X	
*DLT	X	X			X	X	
*EXECUTE	X		X		X		X

Więcej informacji na temat tych uprawnień i ich opisów znajduje się w podręczniku iSeries Security Reference.

Założenia użycia komend

1. Aby można było używać dowolnej komendy wymagane są uprawnienia *USE. To uprawnienie nie jest wyraźnie zaznaczone w tabelach.
2. Aby wprowadzać dowolne komendy wyświetlania, wymagane są uprawnienia do korzystania ze zbioru ekranowego IBM, zbioru wydruku lub panelu grupowego używanego przez komendę. Te zbiory i panele grupowe dostarczane są z uprawnieniami publicznymi *USE.

Zasady ogólne dotyczące uprawnień do obiektów dla komend

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
Zmiana (Change - CHG) i klawisz F4 (podpowiedź)[7]	Wartości bieżące	Wartości bieżące są wyświetlane, jeśli użytkownik ma do nich uprawnienia.	*EXECUTE
Komenda uzyskująca dostęp do obiektu w katalogu	Katalogi w przedrostku ścieżki dla systemu plików QLANSrv	*R	
	Katalogi w przedrostku ścieżki dla wszystkich pozostałych systemów plików	*X	
	Katalog, jeśli dla systemu plików QLANSrv podano wzorzec (* lub ?)	Brak	
	Katalog, jeśli dla pozostałych systemów plików podano wzorzec (* lub ?)	*R	
Tworzenie obiektu w katalogu	Katalogi w przedrostku ścieżki	*X	
	Katalog dla nowego obiektu	*WX	

Zasady ogólne dotyczące uprawnień do obiektów dla komend

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
Kopiowanie (Copy - CPY), gdzie docelowy zbiór to zbiór bazy danych	Obiekt do skopiowania	*OBJOPR, *READ	*EXECUTE
	Komenda CRTPF, jeśli podano parametr CRTFILE (*YES)	*OBJOPR	*EXECUTE
	Docelowy zbiór, jeśli podano parametr CRTFILE (*YES) [1]		*ADD, *EXECUTE
	Docelowy zbiór, jeśli istnieje i dodawany jest nowy podzbiór	*OBJOPR, *OBJMGT, *ADD, *DLT	*ADD, *EXECUTE
	Docelowy zbiór, jeśli zbiór i podzbiór istnieją oraz podano opcję *ADD	*OBJOPR, *ADD	*EXECUTE
	Docelowy zbiór, jeśli zbiór i podzbiór istnieją oraz podano opcję *REPLACE	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Docelowy zbiór, jeśli istnieje oraz dodawany jest nowy podzbiór i podano opcję *UPDADD.[8]	*OBJOPR, *OBJMGT, *ADD, *UPD	*EXECUTE
	Docelowy zbiór, jeśli zbiór i podzbiór istnieją oraz podano opcję *UPDADD.[8]	*OBJOPR, *ADD, *UPD	*EXECUTE
Tworzenie (Create - CRT)	Obiekt do utworzenia [2]		*READ, *ADD
	Profil użytkownika, który będzie właścicielem obiektu (profil użytkownika uruchamiającego zadania lub profil grupowy)	*ADD	
Tworzenie (Create - CRT), jeśli podano parametr REPLACE(*YES) [6, 9]	Obiekt do utworzenia (i zastąpienia)[2]	*OBJMGT, *OBJEXIST, *READ[5]	*READ, *ADD
	Profil użytkownika, który będzie właścicielem obiektu (profil użytkownika uruchamiającego zadania lub profil grupowy)	*ADD	
Wyświetlenie (Display - DSP) lub inna operacja korzystająca ze zbioru wyjściowego (OUTPUT(*OUTFILE))	Obiekt do wyświetlenia	*USE	*EXECUTE
	Zbiór wyjściowy, jeśli nie istnieje [3]		*ADD, *EXECUTE
	Zbiór wyjściowy, jeśli istnieje i jest dodawany nowy członek, oraz jeśli określono opcję *REPLACE, a członek wcześniej nie istniał.	*OBJOPR, *OBJMGT lub *OBJALTER, *ADD, *DLT	*ADD, *EXECUTE
	Zbiór wyjściowy, jeśli istnieje i jest dodawany nowy członek, oraz jeśli określono opcję *ADD, a członek wcześniej nie istniał.	OBJOPR, *OBJMGT or *OBJALTER, *ADD	*ADD, *EXECUTE
	Zbiór wyjściowy, jeśli zbiór i podzbiór istnieją oraz podano opcję *ADD	*OBJOPR, *ADD	*EXECUTE
	Zbiór wyjściowy, jeśli zbiór i podzbiór istnieją oraz podano opcję *REPLACE	*OBJOPR, *OBJMGT lub *OBJALTER, *ADD, *DLT	*EXECUTE
Wyświetlenie (Display - DSP) za pomocą opcji *PRINT lub Praca (Work - WRK) za pomocą opcji *PRINT	Obiekt do wyświetlenia	*USE	*EXECUTE
	Kolejka wyjściowa [4]	*READ	*EXECUTE
	Zbiór drukarkowy (QP*xxxxx* w QSYS)	*USE	*EXECUTE
Zbiór formatu (QA*xxxxx*), jeśli zbiór wyjściowy nie istnieje	*OBJOPR		

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
Składowanie (Save - SAV) lub inna operacja korzystająca z opisu urządzenia	Opis urządzenia	*USE	*EXECUTE
	Zbiór urządzenia związany z opisem urządzenia, taki jak QSYSTAP dla opisu urządzenia TAP01	*USE	*EXECUTE

1 Profil użytkownika uruchamiający komendę kopiowania staje się właścicielem zbioru docelowego, chyba że jest członkiem profilu grupowego i ma ustawiony parametr OWNER(*GRPPRF). Jeśli profil użytkownika ma ustawiony parametr OWNER(*GRPPRF), to profil grupowy staje się właścicielem docelowego zbioru. W takim przypadku użytkownik uruchamiający komendę musi mieć uprawnienia *ADD do profilu grupowego oraz uprawnienia do dodawania podzbiorów i zapisywania danych w nowym zbiorze. Zbiór docelowy ma te same uprawnienia publiczne, uprawnienia grupy podstawowej, uprawnienia prywatne i listę autoryzacji, co zbiór źródłowy.

2 Profil użytkownika uruchamiający komendę tworzenia staje się właścicielem nowo tworzonego obiektu, chyba że jest członkiem profilu grupowego i ma ustawiony parametr OWNER(*GRPPRF). Jeśli profil użytkownika ma ustawiony parametr OWNER(*GRPPRF), to profil grupowy staje się właścicielem nowo utworzonego obiektu. Uprawnienia publiczne do obiektu kontroluje parametr AUT.

3 Profil użytkownika uruchamiający komendę wyświetlania staje się właścicielem nowo tworzonego zbioru wyjściowego, chyba że jest członkiem profilu grupowego i ma ustawiony parametr OWNER(*GRPPRF). Jeśli profil użytkownika ma ustawiony parametr OWNER(*GRPPRF), to profil grupowy staje się właścicielem zbioru wyjściowego. Uprawnienia publiczne do zbioru wyjściowego kontrolowane są przez parametr CRTAUT biblioteki zbioru wyjściowego.

4 Jeśli kolejka wyjściowa ma ustawiony parametr OPRCTL (*YES), użytkownik z uprawnieniami specjalnymi *JOBCTL nie potrzebuje żadnych uprawnień do tej kolejki. Użytkownik z uprawnieniami specjalnymi *SPLCTL nie potrzebuje żadnych uprawnień do kolejki wyjściowej.

5 Dla zbiorów urządzeń wymagane są także uprawnienia *OBJOPR.

6 W środowisku S/38 parametr REPLACE nie jest dostępny. Parametr REPLACE(*YES) odpowiada użyciu klawisza funkcyjnego z menu programisty do usunięcia bieżącego obiektu.

7 Wymagane są także uprawnienia do odpowiedniej komendy (DSP).

8 Opcja *UPDADD jest dostępna tylko dla parametru MBROPT komendy CPYF.

9 Nie ma zastosowania dla parametru REPLACE komendy CRTJVAPGM.

Wspólne komendy obiektów

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Tabela 149. Wspólne komendy obiektów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ALCOBJ [1,2,11]	Obiekt	*OBJOPR	*EXECUTE
ANZUSROBJ [20]			
CHGOBJAUD [18]	Urządzenie ASP (jeśli jest podane)	*USE	
CHGOBJD [3]	Obiekt, jeśli jest to plik	*OBJOPR, *OBJMGT	*EXECUTE
	Obiekt, jeśli nie jest to plik	*OBJMGT	*EXECUTE

Tabela 149. Wspólne komendy obiektów (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGOBJOWN [3,4]	Obiekt	*OBJEXIST	*EXECUTE
	Obiekt (jeśli jest to plik, biblioteka, opis podsystemu)	*OBJOPR, *OBJEXIST	*EXECUTE
	Obiekt (jeśli jest to *AUTL)	Prawo własności lub *ALLOBJ	*EXECUTE
	Poprzedni profil użytkownika	*DLT	*EXECUTE
	Nowy profil użytkownika	*ADD	*EXECUTE
	Urządzenie ASP (jeśli jest podane)	*USE	
CHGOBJPGP [3]	Obiekt	*OBJEXIST	*EXECUTE
	Obiekt (jeśli jest to plik, biblioteka, opis podsystemu)	*OBJOPR, *OBJEXIST	*EXECUTE
	Obiekt (jeśli jest to *AUTL)	Prawo własności i *OBJEXIST lub *ALLOBJ	*EXECUTE
	Poprzedni profil użytkownika	*DLT	
	Nowy profil użytkownika	*ADD	
	Urządzenie ASP (jeśli jest podane)	*USE	
CHKOBJ [3]	Obiekt	Uprawnienia określane przez parametr AUT [14]	*EXECUTE
CPROBJ	Obiekt	*OBJMGT	*EXECUTE
CHKOBJITG [11](Q)			
CRTDUPOBJ [3,9,11,21]	Nowy obiekt		*USE, *ADD
	Kopiowany obiekt, jeśli jest *AUTL	*AUTLMGT	*USE, *ADD
	Kopiowany obiekt, wszystkie pozostałe typy	*OBJMGT, *USE	*USE
	Komenda CRTSAVF (jeśli obiekt jest zbiorem składowania)	*OBJOPR	
	Urządzenie ASP (jeśli jest podane)	*USE	
DCPOBJ	Obiekt	*USE	*EXECUTE
DLCOBJ [1,11]	Obiekt	*OBJOPR	*EXECUTE
DMPOBJ (Q) [3]	Obiekt	*OBJOPR, *READ	*EXECUTE
DMPSYSOBJ (Q)	Obiekt	*OBJOPR, *READ	*EXECUTE
DSPOBJAUT [3]	Obiekt (aby widzieć wszystkie informacje o uprawnieniach)	Uprawnienia specjalne *OBJMGT lub *ALLOBJ albo prawo własności	*EXECUTE
	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Urządzenie ASP (jeśli jest podane)	*USE	

Tabela 149. Wspólne komendy obiektów (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
DSPOBJD [2, 28]	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Uprawnienia	Uprawnienia inne niż *EXCLUDE	*EXECUTE
	Urządzenie ASP (jeśli jest podane)	*EXECUTE	
EDTOBJAUT [3,5,6,15]	Obiekt	*OBJMGT	*EXECUTE
	Obiekt (jeśli jest to zbiór)	*OBJOPR, *OBJMGT	*EXECUTE
	*AUTL, jeśli użyte do ochrony obiektu	Nie *EXCLUDE	
	Urządzenie ASP (jeśli jest podane)	*USE	
GRTOBJAUT [3,5,6,15]	Obiekt	*OBJMGT	*EXECUTE
	Obiekt (jeśli jest to zbiór)	*OBJOPR, *OBJMGT	*EXECUTE
	*AUTL, jeśli użyte do ochrony obiektu	Nie *EXCLUDE	
	Urządzenie ASP (jeśli jest podane)	*USE	
	Urządzenie ASP odniesienia (jeśli jest podane)	*EXECUTE	
	Obiekt odniesienia	*OBJMGT lub prawo własności	*EXECUTE
MOVOBJ [3,7,12]	Obiekt	*OBJMGT	
	Obiekt (jeśli jest to *FILE)	*ADD, *DLT, *EXECUTE	
	Obiekt (jeśli nie jest to *FILE)	*DLT, *EXECUTE	
	Z biblioteki		*CHANGE
	Do biblioteki		*READ, *ADD
	Urządzenie ASP (jeśli jest podane)	*USE	
PRTADPOBJ [26](Q)			
PRTPUBAUT [26]			
PRTUSROBJ [26]			
PRTPVTAUT [26]			
RCLSTG (Q)			
RCLTMPSTG (Q)	Obiekt	*OBJMGT	*EXECUTE
RNMOBJ [3,11]	Obiekt	*OBJMGT	*UPD, *EXECUTE
	Obiekt, jeśli jest to *AUTL	*AUTLMGT	*EXECUTE
	Obiekt (jeśli jest to *FILE)	*OBJOPR, *OBJMGT	*UPD, *EXECUTE
	Urządzenie ASP (jeśli jest podane)	*USE	

Tabela 149. Wspólne komendy obiektów (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
RSTOBJ [3,13] (Q)	Obiekt, jeśli już istnieje w bibliotece	*OBJEXIST [8]	*EXECUTE, *ADD
	Obiekt, jeśli jest to *CFGL, *CNNL, *CTLD, *DEVD, *LIND lub *NWID	*CHANGE i *OBJMGT	*EXECUTE
	Definicja nośnika	*USE	*EXECUTE
	Kolejki komunikatów odtwarzane do biblioteki, w której już istnieją	*OBJOPR, *OBJEXIST [8]	*EXECUTE, *ADD
	Profil użytkownika będący właścicielem tworzonych obiektów	*ADD [8]	
	Program adoptujący uprawnienia	Właściciel lub uprawnienia specjalne *SECADM i *ALLOBJ	*EXECUTE
	Do biblioteki	*EXECUTE, *ADD [8]	
	Biblioteka do składowania obiektów, jeśli podano parametr VOL(*SAVVOL)	*USE [8]	
	Zbiór składowania	*USE	*EXECUTE
RSTOBJ [3,13] (Q)	Jednostka taśm, jednostka dyskietek lub jednostka optyczna	*USE	*EXECUTE
	Zbiór taśmowy (QSYSTAP) lub zbiór dyskietkowy (QSYSDKT)	*USE [8]	*EXECUTE
	Zbiór nośnika optycznego (OPTFILE) [22]	*R	Nie dotyczy
	Katalog nadrzędny pliku nośnika optycznego (OPTFILE) [22]	*X	Nie dotyczy
	Przedrostek ścieżki dla OPTFILE [22]	*X	Nie dotyczy
	Wolumin optyczny [24]	*USE	Nie dotyczy
	Zbiór wydruku QSYS/QPSRLDSP, jeśli określono OUTPUT(*PRINT)	*USE	*EXECUTE
	Zbiór wyjściowy, jeśli został podany	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Zbiór opisów pól QSYS/QASRRSTO dla zbioru wyjściowego, jeśli określono nieistniejący zbiór wyjściowy	*USE	*EXECUTE
	Opis urządzenia ASP [25]	*USE	
RVKPUBAUT [20]	Zbiór taśmowy (QSYSTAP) lub zbiór dyskietkowy (QSYSDKT)	*USE [8]	*EXECUTE
RTVOBJD [2, 29]	Obiekt	Uprawnienia inne niż *EXCLUDE	*EXECUTE
RVKOBJAUT [3,5,15, 27]	Przedrostek ścieżki dla OPTFILE [22]	*X	Nie dotyczy
	Wolumin optyczny [24]	*USE	Nie dotyczy
	Zbiór wydruku QSYS/QPSRLDSP, jeśli określono OUTPUT(*PRINT)	*USE	*EXECUTE
	Urządzenie ASP (jeśli jest podane)	*USE	

Tabela 149. Wspólne komendy obiektów (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
SAVCHGOBJ [3]	Obiekt (8)	*OBJEXIST	*EXECUTE
	Jednostka taśm, jednostka dyskietek, jednostka optyczna	*USE	*EXECUTE
	Zbiór składowania, jeśli jest pusty	*USE, *ADD	*EXECUTE
	Zbiór składowania, jeśli istnieją w nim rekordy	*OBJMGT, *USE, *ADD	*EXECUTE
	Kol. komunik. akt. składowania (Save active message queue)	*OBJOPR, *ADD	*EXECUTE
SAVCHGOBJ [3]	Zbiór nośnika optycznego (OPTFILE)[22]	*RW	Nie dotyczy
	Katalog nadrzędny pliku nośnika optycznego (OPTFILE) [22]	*WX	Nie dotyczy
	Przedrostek ścieżki pliku nośnika optycznego (OPTFILE) [22]	*X	Nie dotyczy
	Katalog główny (/) woluminu optycznego [22, 23]	*RWX	Nie dotyczy
	Wolumin optyczny [24]	*CHANGE	
	Zbiór wyjściowy, jeśli został podany	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Zbiór opisów pól QSYS/QASAVOBJ dla zbioru wyjściowego, jeśli określono nieistniejący zbiór wyjściowy	*USE [8]	*EXECUTE
	Zbiór wydruku QSYS/QPSAVOBJ	*USE [8]	*EXECUTE
	Opis urządzenia ASP [25]	*USE	
SAVOBJ [3]	Obiekt	*OBJEXIST [8]	*EXECUTE
	Definicja nośnika	*USE	*EXECUTE
	Jednostka taśm, jednostka dyskietek, jednostka optyczna	*USE	*EXECUTE
	Zbiór składowania, jeśli jest pusty	*USE, *ADD	*EXECUTE
	Zbiór składowania, jeśli istnieją w nim rekordy	*OBJMGT, *USE, *ADD	*EXECUTE
	Kol. komunik. akt. składowania (Save active message queue)	*OBJOPR, *ADD	*EXECUTE

Tabela 149. Wspólne komendy obiektów (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
SAVOBJ [3]	Zbiór nośnika optycznego (OPTFILE)[22]	*RW	Nie dotyczy
	Katalog nadrzędny pliku nośnika optycznego (OPTFILE) [22]	*WX	Nie dotyczy
	Przedrostek ścieżki dla OPTFILE [22]	*X	Nie dotyczy
	Katalog główny (/) woluminu optycznego [22, 23]	*RWX	Nie dotyczy
	Wolumin optyczny [24]	*CHANGE	
	Zbiór wyjściowy, jeśli został podany	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Zbiór opisów pól QSYS/QASAVOBJ dla zbioru wyjściowego, jeśli określono nieistniejący zbiór wyjściowy	*USE [8]	*EXECUTE
	Zbiór wydruku QSYS/QPSAVOBJ	*USE [8]	*EXECUTE
	Opis urządzenia ASP [25]	*USE	
SAVSTG [10]			
SAVSYS [10]	Jednostka taśm, jednostka optyczna	*USE	*EXECUTE
	Katalog główny (/) woluminu optycznego [22]	*RWX	Nie dotyczy
	Wolumin optyczny [24]	*CHANGE	Nie dotyczy
SAVRSTCHG	W systemie źródłowym są to takie same uprawnienia, jak wymagane dla komendy SAVCHGOBJ.		
	W systemie docelowym są to takie same uprawnienia, jak wymagane dla komendy RST.		
	Opis urządzenia ASP [25]	*USE	
SAVRSTLIB	W systemie źródłowym są to takie same uprawnienia, jak wymagane dla komendy SAVLIB.		
	W systemie docelowym są to takie same uprawnienia, jak wymagane dla komendy RSTLIB.		
SAVRSTOBJ	W systemie źródłowym są to takie same uprawnienia, jak wymagane dla komendy SAVOBJ.		
	W systemie docelowym są to takie same uprawnienia, jak wymagane dla komendy RST.		
	Opis urządzenia ASP [25]	*USE	
SETOBJACC	Obiekt	*OBJOPR	*EXECUTE
WRKOBJ [19]	Obiekt	Dowolne uprawnienia	*USE
WRKOBJLCK	Obiekt		*EXECUTE
	Urządzenie ASP	*EXECUTE	
WRKOBJOWN [17]	Profil użytkownika	*READ	*EXECUTE
WRKOBJPGP [17]	Profil użytkownika	*READ	*EXECUTE
WRKOBJPVT[17]	Profil użytkownika	*READ	*EXECUTE

Tabela 149. Wspólne komendy obiektów (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
[1]	Listę typów obiektów, które można przydzielić lub zwolnić, można wyświetlić za pomocą słowa kluczowego OBJTYPE komendy ALCOBJ.		
[2]	Wymagane są niektóre uprawnienia do obiektu (inne niż *EXCLUDE).		
[3]	Tej komendy nie można używać dla dokumentów lub folderów. W tym celu należy skorzystać z komendy Obiekt biblioteki dokumentu (Document Library Object - DLO).		
[4]	Aby zmienić właściciela programu, programu usługowego lub pakietu SQL, które adoptują uprawnienia, należy mieć uprawnienia specjalne *ALLOBJ i *SECADM.		
[5]	Użytkownik musi być właścicielem lub mieć uprawnienia *OBJMGT oraz uprawnienia nadawane lub odbierane.		
[6]	Aby nadać uprawnienia *OBJMGT lub *AUTLMGT, użytkownik musi być właścicielem lub mieć uprawnienia specjalne *ALLOBJ.		
[7]	Ta komenda nie może być używana dla profili użytkowników, opisów kontrolerów, opisów urządzeń, opisów linii, dokumentów, bibliotek dokumentów oraz folderów.		
[8]	Jeśli użytkownik ma uprawnienia specjalne *SAVSYS, nie potrzebuje podanych tu uprawnień.		
[9]	Jeśli użytkownik uruchamiający komendę CRTDUPOBJ w swoim profilu ma uprawnienia OWNER(*GRPPRF), właścicielem nowego obiektu będzie profil grupowy. Aby pomyślnie skopiować uprawnienia do nowego obiektu, którego właścicielem jest profil grupowy, należy zastosować następujące zasady: • Użytkownik uruchamiający komendę musi mieć uprawnienie do obiektu początkowego. Uprawnienia można uzyskać z uprawnienia adoptowanego lub za pośrednictwem profilu grupowego. • jeśli podczas kopiowania uprawnień do nowego obiektu wystąpi błąd, nowo tworzony obiekt jest usuwany,		
[10]	Użytkownik musi mieć uprawnienia specjalne *SAVSYS.		
[11]	Ta komenda nie może być używana dla kronik i dzienników.		
[12]	Ta komenda nie może być używana dla kronik i dzienników, chyba że obiektem odniesienia Z biblioteki jest QRCL, a Do biblioteki to początkowa biblioteka kroniki lub dziennika.		
[13]	Aby podać parametr ALWOBJDIF(*ALL), użytkownik musi mieć uprawnienia specjalne *ALLOBJ.		
[14]	Aby sprawdzić uprawnienia użytkownika do obiektu, użytkownik musi mieć sprawdzane uprawnienia. Na przykład, aby sprawdzić czy użytkownik ma uprawnienia *OBJEXIST do obiektu ZBIÓR_B, to użytkownik sprawdzający też musi mieć uprawnienia *OBJEXIST do tego obiektu.		
[15]	Aby zabezpieczyć obiekt za pomocą listy autoryzacji lub ją usunąć, należy: • być właścicielem obiektu, • mieć uprawnienie *ALL do tego obiektu, • mieć uprawnienie specjalne *ALLOBJ.		
[16]	Jeśli plik początkowy lub plik, którego nazwa jest zmieniana, są związane z magazynem uprawnień, do tego magazynu wymagane są uprawnienia *ALL.		
[17]	Ta komenda nie obsługuje systemu plików QOPT.		
[18]	Użytkownik musi mieć uprawnienia specjalne *AUDIT.		
[19]	Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.		
[20]	Użytkownik musi mieć uprawnienia specjalne *ALLOBJ.		

Tabela 149. Wspólne komendy obiektów (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
21	Wszystkie uprawnienia obiektu odniesienia Z obiektu są duplikowane w nowym obiekcie. Grupa podstawowa nowego obiektu określana jest przez pole rodzaju uprawnień grupowych (GRPAUTTYP) w profilu użytkownika, który uruchamia komendę. Jeśli obiekt odniesienia Z obiektu ma grupę podstawową, nowy obiekt może nie mieć tej samej grupy podstawowej, ale uprawnienia, które grupa podstawowa zyskuje od obiektu odniesienia Z obiektu, będą zduplikowane dla nowego obiektu.		
22	To sprawdzanie uprawnień przeprowadzane jest jedynie wtedy, kiedy nośnik optyczny ma format UDF (Universal Disk Format).		
23	To sprawdzanie uprawnień przeprowadzane jest jedynie wtedy, kiedy nośnik optyczny jest czyszczony.		
24	Woluminy optyczne nie są rzeczywistymi obiektami systemowymi. Dowiązanie między woluminem optycznym a listą autoryzacji używaną do ochrony obiektu jest utrzymywane przez funkcję obsługi nośników optycznych.		
25	Uprawnienie wymagane tylko, jeśli operacja składowania lub odtwarzania wymaga przełącznika przestrzeni nazw biblioteki.		
26	Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *ALLOBJ lub *AUDIT.		
27	***** Zagrożenie dla ochrony ***** Odebranie wszystkich uprawnień do obiektów nadanych użytkownikowi może spowodować, że uprawnienia tego użytkownika będą większe niż przed ich odebraniem. Jeśli użytkownik ma uprawnienie *USE do obiektu i uprawnienie *CHANGE do listy autoryzacji chroniącej ten obiekt, odebranie uprawnienia *USE spowoduje przyznanie uprawnienia *CHANGE do obiektu.		
28	Aby bieżąca wartość kontrolowania obiektu została wyświetlona, użytkownik musi mieć uprawnienie specjalne *ALLOBJ lub *AUDIT. W przeciwnym przypadku zostanie wyświetlona wartość *NOTAVL wskazująca, że wartość kontrolowania nie może być wyświetlona.		
29	Aby pobrać bieżącą wartość kontrolowania obiektu, użytkownik musi mieć uprawnienie specjalne *ALLOBJ lub *AUDIT. W przeciwnym przypadku zostanie zwrócona wartość *NOTAVL wskazująca, że wartości nie mogą być pobrane.		

Komendy odtwarzania ścieżki dostępu: wymagane uprawnienia

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Te komendy nie wymagają uprawnień do obiektu.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGRCYAP [1] (Q)	Urządzenie ASP (jeśli jest podane)	*USE	
DSPRCYAP [1]	Urządzenie ASP (jeśli jest podane)	*USE	
EDTRBDAP [2] (Q)			
EDTRCYAP [1] (Q)	Urządzenie ASP (jeśli jest podane)	*USE	
1	Aby użyć tej komendy należy mieć uprawnienia specjalne *JOBCTL.		
2	Do użycia tej komendy konieczne jest uprawnienie specjalne (*ALLOBJ).		

Komendy funkcji AFP*: wymagane uprawnienia

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDFNTTBLE	Tabela czcionek DBCS	*CHANGE	*EXECUTE
CHGCDEFNT	Zasoby czcionek	*CHANGE	*EXECUTE
CHGFNTTBLE	Tabela czcionek DBCS	*CHANGE	*EXECUTE
CRTFNTRSC	Zbiór źródłowy	*USE	*EXECUTE
	Zasób czcionki: REPLACE(*NO)		*READ, *ADD
	Zasób czcionki: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
CRTFNTTBL	Tabela czcionek DBCS		*READ, *ADD
CRTFORMDF	Zbiór źródłowy	*USE	*EXECUTE
	Definicja formularza: REPLACE(*NO)		*READ, *ADD
	Definicja formularza: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
CRTOVL	Zbiór źródłowy	*USE	*EXECUTE
	Nakładka: REPLACE(*NO)		*READ, *ADD
	Nakładka: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
CRTPAGDFN	Zbiór źródłowy	*USE	*EXECUTE
	Definicja strony: REPLACE(*NO)		*READ, *ADD
	Definicja strony: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
CRTPAGSEG	Zbiór źródłowy	*USE	*EXECUTE
	Segment strony: REPLACE(*NO)		*READ, *ADD
	Segment strony: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
DLTFNTRSC	Zasoby czcionek	*OBJEXIST	*EXECUTE
DLTFNTTBL	Tabela czcionek DBCS	*CHANGE	*EXECUTE
DLTFORMDF	Definicja formularza	*OBJEXIST	*EXECUTE
DLTOVL	Nakładka	*OBJEXIST	*EXECUTE
DLTPAGDFN	Definicja strony	*OBJEXIST	*EXECUTE
DLTPAGSEG	Segment strony	*OBJEXIST	*EXECUTE
DSPCDEFNT	Zasoby czcionek	*USE	*EXECUTE
DSPFNTRSCA	Zasoby czcionek	*USE	*EXECUTE
DSPFNTTBL	Tabela czcionek DBCS	*USE	*EXECUTE
RMVFNTTBLE	Tabela czcionek DBCS	*CHANGE	*EXECUTE
WRKFNTRSC [1]	Zasoby czcionek	*USE	*USE
WRKFORMDF [1]	Definicja formularza	*USE	*USE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
WRKOVL [1]	Nakładka	*USE	*USE
WRKPAGDFN [1]	Definicja strony	Dowolne uprawnienia	*USE
WRKPAGSEG [1]	Segment strony	*USE	Dowolne uprawnienia

1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

Komendy gniazd AF_INET przez SNA: wymagane uprawnienia

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.Te komendy nie wymagają żadnych uprawnień do obiektów:

Te komendy nie wymagają żadnych uprawnień do obiektów:			
ADDIPSIFC[1]	CHGIPSIFC[1]	CVTIPSLOC	RMVIPSLOC[1]
ADDIPSRTE[1]	CHGIPSLOC[1]	ENDIPSIFC (Q)	RMVIPSRTE[1]
ADDIPSLOC[1]	CHGIPSTOS[1]	PRTIPSCFG	STRIPSIFC (Q)
CFGIPS	CVTIPSIFC	RMVIPSIFC[1]	

1 Do użycia tej komendy konieczne jest uprawnienie specjalne (*IOSYSCFG).

Alerty: wymagane uprawnienia

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDALRD	Tabela alertów	*USE, *ADD	*EXECUTE
CHGALRD	Tabela alertów	*USE, *UPD	*EXECUTE
CHGALRTBL (Q)	Tabela alertów	*CHANGE	*EXECUTE
CRTALRTBL (Q)	Tabela alertów		*READ, *ADD
DLTALR	Zbiór fizyczny QAALERT	*USE, *DLT	*EXECUTE
DLTALRTBL (Q)	Tabela alertów	*OBJEXIST	*EXECUTE
RMVALRD	Tabela alertów	*USE, *DLT	*EXECUTE
WRKALR [1]	Zbiór fizyczny QAALERT	*USE	*EXECUTE
WRKALRD [1]	Tabela alertów	*USE	*EXECUTE
WRKALRTBL [1]	Tabela alertów	*READ	*USE

1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

Komendy projektowania aplikacji: wymagane uprawnienia

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
FNDSTRPDM	Część kodu źródłowego	*READ	*EXECUTE
MRGFORMD	Opis formularza	*READ	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
STRAPF [1]	Zbiór źródłowy	*OBJMGT, *CHANGE	*READ, *ADD
	Komendy CRTPF, CRTLF, ADDPFM, ADDLFM i RMVM	*USE	*EXECUTE
STRBGU [1]	Wykres	*OBJMGT, *CHANGE	*EXECUTE
STRDFU [1]	Program (jeśli tworzone są opcje programu)		*READ, *ADD
	Program (jeśli opcje są zmieniane lub usuwane)	*OBJEXIST	*EXECUTE
	Program (jeśli opcje danych są zmieniane lub usuwane)	*USE	*EXECUTE
	Zbiór bazy danych (jeśli opcje danych są zmieniane)	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	Zbiór bazy danych (jeśli opcje danych są wyświetlane)	*USE	*EXECUTE
	Zbiór ekranowy (jeśli opcje danych są wyświetlane lub zmieniane)	*USE	*EXECUTE
	Zbiór bazy danych (jeśli opcje programu są zmieniane)	*USE	*EXECUTE
	Zbiór bazy danych (jeśli opcje programu są usuwane)	*OBJEXIST	*EXECUTE
STRPDM [1]			
STRRLU	Zbiór źródłowy	*READ, *ADD, *UPD, *DLT	*EXECUTE
	Edytowanie, dodawanie lub zmiana podzbioru	*OBJOPR, *OBJMGT	*READ, *ADD
	Przeglądanie podzbioru	*OBJOPR	*EXECUTE
	Drukowanie raportu prototypowego	*OBJOPR	*EXECUTE
	Usunięcie podzbioru	*OBJOPR, *OBJEXIST	*EXECUTE
	Zmiana typu lub tekstu podzbioru	*OBJOPR	*EXECUTE
STRSDA	Zbiór źródłowy	*READ, *ADD, *UPD, *DLT	*EXECUTE
	Aktualizowanie i dodawanie nowego podzbioru	*CHANGE, *OBJMGT	*READ, *ADD
	Usunięcie podzbioru	*ALL	*EXECUTE
STRSEU [1]	Zbiór źródłowy	*USE	*EXECUTE
	Edytowanie lub zmiana podzbioru	*CHANGE, *OBJMGT	*EXECUTE
	Dodawanie podzbioru	*USE, *OBJMGT	*READ, *ADD
	Przeglądanie podzbioru	*USE	*EXECUTE
	Drukowanie podzbioru	*USE	*EXECUTE
	Usunięcie podzbioru	*USE, *OBJEXIST	*EXECUTE
	Zmiana typu lub tekstu podzbioru	*USE, *OBJMGT	*EXECUTE
WRKLIBPDM [1]			
WRKMBRPDM [1]	Zbiór źródłowy	*USE	*EXECUTE
WRKOBJPDM [1]	Zbiór (File)	*READ lub prawo własności	*EXECUTE

Komendy projektowania aplikacji

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
[1] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.			
[2] Grupa odpowiada bibliotece.			
[3] Projekt składa się z jednej lub więcej grup (bibliotek).			

Komendy magazynu uprawnień: wymagane uprawnienia

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTAUTHLR (Q)	Powiązany obiekt, jeśli istnieje	*ALL	*EXECUTE
DLTAUTHLR	Magazyn uprawnień	*ALL	*EXECUTE
DSPAUTHLR	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.

Komendy listy autoryzacji: wymagane uprawnienia

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki QSYS**
ADDAUTLE [1]	*AUTL	*AUTLMGT lub prawo własności	*EXECUTE
CHGAUTLE [1]	*AUTL	*AUTLMGT lub prawo własności	*EXECUTE
CRTAUTL			
DLTAUTL	*AUTL	Właściciel lub *ALLOBJ	*EXECUTE
DSPAUTL	*AUTL		*EXECUTE
	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
DSPAUTLDLO	*AUTL	*USE	*EXECUTE
DSPAUTLOBJ	*AUTL	*READ	*EXECUTE
	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
EDTAUTL [1]	*AUTL	*AUTLMGT lub prawo własności	*EXECUTE
RMVAUTLE [1]	*AUTL	*AUTLMGT lub prawo własności	*EXECUTE
RTVAUTLE [2]	*AUTL	*AUTLMGT lub prawo własności	*EXECUTE
WRKAUTL [3,4,5]	*AUTL		

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki QSYS**

[1] Użytkownik musi być właścicielem lub mieć uprawnienia do zarządzania listą autoryzacji oraz uprawnienia nadawane lub odbierane.

[2] Jeśli użytkownik nie ma uprawnień *OBJMGT lub *AUTLMGT, może odtworzyć uprawnienia *PUBLIC oraz własne. Aby odtworzyć własne uprawnienia, użytkownik musi mieć uprawnienie *READ do własnego profilu.

[3] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

[4] Użytkownik nie może być wykluczony (*EXCLUDE) z listy autoryzacji.

[5] Wymagane są niektóre uprawnienia do listy autoryzacji.

Komendy katalogu konsolidacji: wymagane uprawnienia

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDBNDDIRE	Katalog konsolidacji	*OBJOPR, *ADD	*USE
CRTBNDDIR	Katalog konsolidacji		*READ, *ADD
DLTBNDDIR	Katalog konsolidacji	*OBJEXIST	*EXECUTE
DSPBNDDIR	Katalog konsolidacji	*READ, *OBJOPR	*USE
RMVBNDDIRE	Katalog konsolidacji	*OBJOPR, *DLT	*READ, *OBJOPR
WRKBNDDIR [1]	Katalog konsolidacji	Dowolne uprawnienia	*USE
WRKBNDDIRE [1]	Katalog konsolidacji	*READ, *OBJOPR	*USE

[1] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operacje.

Komendy opisu żądania zmiany

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDCMDCRQA (Q)	Opis żądania zmiany	*CHANGE	*EXECUTE
ADDOBJCRQA (Q)	Opis żądania zmiany	*CHANGE	*EXECUTE
ADDPRDCRQA (Q)	Opis żądania zmiany	*CHANGE	*EXECUTE
ADDPTFCRQA (Q)	Opis żądania zmiany	*CHANGE	*EXECUTE
ADDRSCCRQA (Q)	Opis żądania zmiany	*CHANGE	*EXECUTE
CHGCMDCRQA (Q)	Opis żądania zmiany	*CHANGE	*EXECUTE
CHGOBJCRQA (Q)	Opis żądania zmiany	*CHANGE	*EXECUTE
CHGPRDCRQA (Q)	Opis żądania zmiany	*CHANGE	*EXECUTE
CHGPTFCRQA (Q)	Opis żądania zmiany	*CHANGE	*EXECUTE
CHGCRQD	Opis żądania zmiany	*CHANGE	*EXECUTE
CHGRSCCRQA (Q)	Opis żądania zmiany	*CHANGE	*EXECUTE
CRTCRQD	Opis żądania zmiany		*READ, *ADD
DLTCRQD	Opis żądania zmiany	*OBJEXIST	*EXECUTE
RMVCRQDA	Opis żądania zmiany	*CHANGE	*EXECUTE

Komendy opisu żądania zmiany

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
WRKCRQD [1]	Opis żądania zmiany		*EXECUTE

[1] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

Komendy wykresów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
DLTCHTFMT	Format wykresu	*OBJEXIST	*EXECUTE
DSPCHT	Format wykresu	*USE	*USE
	Zbiór bazy danych	*USE	*USE
DSPGDF	Zbiór bazy danych	*USE	*USE
STRBGU (Opcja 3) [2]	Format wykresu	*CHANGE, *OBJEXIST	*EXECUTE
WRKCHTFMT [1]	Format wykresu	Dowolne uprawnienia	*USE

[1] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

[2] Opcja 3 menu B (pojawiającego się po uruchomieniu komendy STRGBU) jest opcją Zmiana formatu wykresu.

Komendy klas

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGCLS	Klasa	*OBJMGT, *OBJOPR	*EXECUTE
CRTCLS	Klasa		*READ, *ADD
DLTCLS	Klasa	*OBJEXIST	*EXECUTE
DSPCLS	Klasa	*USE	*EXECUTE
WRKCLS [1]	Klasa	*OBJOPR	*USE

[1] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

Komendy klas usług

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGCOSD [3]	Opis klasy usług	*CHANGE, OBJMGT	*EXECUTE
CRTCOSD [3]	Opis klasy usług		
DLTCOSD	Opis klasy usług	*OBJEXIST	*EXECUTE
DSPCOSD	Opis klasy usług	*USE	*EXECUTE
WRKCOSD [1,2]	Opis klasy usług	*OBJOPR	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki

[1] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

[2] Wymagane są niektóre uprawnienia do obiektu.

[3] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

Komendy klastra

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ADDCLUNODE (Q)[1]	Program usługowy QCSTCTL	*USE	
ADDCRGDEVE (Q)[1]	Program usługowy QCSTCRG1	*USE	
	Grupa zasobów klastra	*CHANGE	*EXECUTE (QUSRSYS)
	Program obsługi wyjścia	*EXECUTE[2]	*EXECUTE[2]
	Profil użytkownika uruchamiający program obsługi wyjścia	*USE	
	Opis urządzenia	*USE, *OBJMGT	
ADDCRGNODE (Q)[1]	Program usługowy QCSTCRG1	*USE	
	Grupa zasobów klastra	*CHANGE	*EXECUTE (QUSRSYS)
	Program obsługi wyjścia	*EXECUTE[2]	*EXECUTE[2]
	Profil użytkownika uruchamiający program obsługi wyjścia	*USE	
	Kolejka komunikatów przełączania awaryjnego	*OBJOPR, *ADD	*EXECUTE
	Kolejka użytkownika dystrybucji informacji	*OBJOPR, *ADD	*EXECUTE
ADDDEVDMNE (Q)[1]	Program usługowy QCSTDD	*USE	
CHGCLUCFG (Q)[1]	Program usługowy QCSTCTL2	*USE	
CHGCLUNODE (Q)[1]	Program usługowy QCSTCTL	*USE	
CHGCLURCY	Grupa zasobów klastra	*USE	
		*JOBCTL	
		*SERVICE lub funkcja śledzenia serwisowego	
CHGCLUVER (Q)[1]	Program usługowy QCSTCTL2	*USE	

Komendy klastra

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CHGCRG (Q)[1]	Program usługowy QCSTCRG1	*USE	
	Grupa zasobów klastra	*CHANGE	*EXECUTE (QUSRSYS)
	Program obsługi wyjścia	*EXECUTE[2]	*EXECUTE[2]
	Profil użytkownika uruchamiający program obsługi wyjścia	*USE	
	Opis urządzenia	*USE, *OBJMGT	
	Kolejka komunikatów przełączania awaryjnego	*OBJOPR, *ADD	*EXECUTE
CHGCRGDEVE (Q)[1]	Program usługowy QCSTCRG1	*USE	
	Grupa zasobów klastra	*CHANGE	*EXECUTE (QUSRSYS)
	Program obsługi wyjścia	*EXECUTE[2]	*EXECUTE[2]
	Profil użytkownika uruchamiający program obsługi wyjścia	*USE	
	Opis urządzenia	*USE, *OBJMGT	
CHGCRGPRI (Q)[1]	Program usługowy QCSTCRG2	*USE	
	Grupa zasobów klastra	*CHANGE	*EXECUTE (QUSRSYS)
	Program obsługi wyjścia	*EXECUTE[2]	*EXECUTE[2]
	Profil użytkownika uruchamiający program obsługi wyjścia	*USE	
	Opis urządzenia	*USE, *OBJMGT	
	Komenda Zmiana statusu konfiguracji (Vary configuration - VFYCFG)	*USE	
CRTCLU (Q)[1]	Program usługowy QCSTCTL	*USE	
CRTCRG (Q) [1]	Program usługowy QCSTCRG1	*USE	
	Biblioteka grupy zasobów klastra		*OBJOPR, *ADD, *READ (QUSRSYS)
	Program obsługi wyjścia	*EXECUTE[2]	*EXECUTE[2]
	Profil użytkownika uruchamiający program obsługi wyjścia	*USE	
	Opis urządzenia	*USE, *OBJMGT	
	Kolejka użytkownika dystrybucji informacji	*OBJOPR, *ADD	*EXECUTE
	Kolejka komunikatów przełączania awaryjnego	*OBJOPR, *ADD	*EXECUTE
DLTCLU (Q)[1]	Program usługowy QCSTCTL	*USE	
DLTCRG[1]	Grupa zasobów klastra	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)
DLTCRGCLU (Q)[1]	Program usługowy QCSTCRG1	*USE	
	Grupa zasobów klastra	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)
	Program obsługi wyjścia	*EXECUTE[2]	*EXECUTE[2]
	Profil użytkownika uruchamiający program obsługi wyjścia	*USE	

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
DMPCLUTRC	Grupa zasobów klastra	*USE	
		*SERVICE lub funkcja śledzenia serwisowego	
DSPCLUINF			
DSPCRGINF	Grupa zasobów klastra	*USE	*EXECUTE (QUSRSYS)
ENDCLUNOD (Q)[1]	Program usługowy QCSTCTL	*USE	
ENDCHTSVR (Q)	Lista autoryzacji	*CHANGE	
ENDCRG (Q)[1]	Program usługowy QCSTCRG2	*USE	
	Grupa zasobów klastra	*CHANGE	*EXECUTE (QUSRSYS)
	Program obsługi wyjścia	*EXECUTE[2]	*EXECUTE[2]
	Profil użytkownika uruchamiający program obsługi wyjścia	*USE	
RMVCLUNODE (Q)[1]	Program usługowy QCSTCTL	*USE	
RMVCRGDEVE (Q)[1]	Program usługowy QCSTCRG1	*USE	
	Grupa zasobów klastra	*CHANGE	*EXECUTE
	Program obsługi wyjścia	*EXECUTE[2]	*EXECUTE[2]
	Profil użytkownika uruchamiający program obsługi wyjścia	*USE	
	Opis urządzenia	*USE, *OBJMGT	
RMVCRGNODE (Q) [1]	Program usługowy QCSTCRG1	*USE	
	Grupa zasobów klastra	*CHANGE, *OBJEXIST	*EXECUTE
	Program obsługi wyjścia	*EXECUTE[2]	*EXECUTE[2]
	Profil użytkownika uruchamiający program obsługi wyjścia	*USE	
	Opis urządzenia	*USE, *OBJMGT	
RMVDEVDMNE (Q)[1]	Program usługowy QCSTDD	*USE	
STRCHTSVR	Lista autoryzacji	*CHANGE	
STRCLUNOD (Q)[1]	Program usługowy QCSTCTL	*USE	
STRCRG (Q)[1]	Program usługowy QCSTCRG2	*USE	
	Grupa zasobów klastra	*CHANGE	*EXECUTE
	Program obsługi wyjścia	*EXECUTE[2]	*EXECUTE[2]
	Profil użytkownika uruchamiający program obsługi wyjścia	*USE	
	Opis urządzenia	*USE, *OBJMGT	

1 Do użycia tej komendy konieczne jest uprawnienie specjalne (*IOSYSCFG).

2 Dotyczy wywołania profilu użytkownika i profilu użytkownika uruchamiającego program obsługi wyjścia.

Komendy *CMD

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGCMD	Komenda	*OBJMGT	*EXECUTE
CHGCMDDFT	Komenda	*OBJMGT, *USE	*EXECUTE
CRTCMD	Zbiór źródłowy	*USE	*EXECUTE
	Komenda: REPLACE(*NO)		*READ, *ADD
	Komenda: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
DLTCMD	Komenda	*OBJEXIST	*EXECUTE
DSPCMD	Komenda	*USE	*EXECUTE
GENCMDDOC[3]	Komenda	*USE	*EXECUTE
	Panel grupowy (powiązany)	*USE	*EXECUTE
	Zbiór wyjściowy: REPLACE = (*YES)	*ALL	*CHANGE
SBMRMTCMD	Komenda	*OBJOPR	*EXECUTE
	Plik DDM	*USE	*EXECUTE
SLTCMD [1]	Komenda	Dowolne uprawnienia	*USE
WRKCMD [2]	Komenda	Dowolne uprawnienia	*USE

1 Wymagane jest prawo własności lub niektóre uprawnienia do obiektu.

2 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

3 Użytkownik musi posiadać uprawnienie do wykonywania (*X) do katalogów w ścieżce dla wygenerowanego zbioru oraz uprawnienie do zapisu i wykonywania do katalogu nadrzędnego wygenerowanego zbioru.

Komendy kontroli transakcji

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
COMMIT			
ENDCMTCTL	Kolejka komunikatów, jaką podano w słowie kluczowym NFYOBJ dla związanej z nim komendy STRCMTCTL.	*OBJOPR, *ADD	*EXECUTE
ROLLBACK			
STRCMTCTL	Kolejka komunikatów, gdy podano słowo kluczowe NFYOBJ	*OBJOPR, *ADD	*EXECUTE
	Obszar danych, który podano w słowie kluczowym NFYOBJ dla związanej z nim komendy STRCMTCTL.	*CHANGE	*EXECUTE
	Zbiory, jakie podano w słowie kluczowym NFYOBJ dla związanej z nim komendy STRCMTCTL.	*OBJOPR *READ	*EXECUTE
WRKCMTDFN [1]			

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
[1] Każdy użytkownik może uruchomić tę komendę dla definicji kontroli transakcji należących do zadania, które jest uruchamiane za pomocą profilu tego użytkownika. Użytkownik, który ma uprawnienia specjalne *JOBCTL, może uruchamiać tę komendę dla dowolnej definicji kontroli transakcji.			

Komendy informacji po stronie komunikacyjnej

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGCSI	Obiekt informacji po stronie komunikacyjnej	*USE, *OBJMGT	*EXECUTE
	Opis urządzenia [1]	*CHANGE	
CRTCSI	Obiekt informacji po stronie komunikacyjnej		*READ, *ADD
	Opis urządzenia [1]	*CHANGE	
DLTCSI	Obiekt informacji po stronie komunikacyjnej	*OBJEXIST	*EXECUTE
DSPCSI	Obiekt informacji po stronie komunikacyjnej	*READ	*EXECUTE
WRKCSI	Obiekty informacji po stronie komunikacyjnej	*USE	*EXECUTE
[1] Uprawnienia sprawdzane są podczas używania obiektu informacji po stronie komunikacyjnej.			

Komendy konfiguracji

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
PRTDEVADR	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis urządzenia	*USE	*EXECUTE
RSTCFG (Q) [5]	Każdy obiekt odtwarzany z zeskładowanej wersji	*OBJEXIST [1]	*EXECUTE
	Do biblioteki		*ADD, *EXECUTE [1]
	Profil użytkownika będący właścicielem tworzonych obiektów	*ADD [1]	
	Jednostka taśm	*USE	*EXECUTE
	Zbiór taśmowy (QSYSTAP)	*USE [1]	*EXECUTE
	Zbiór składowania, jeśli podano	*USE	*EXECUTE
	Zbiór wydruku (QPSRLDSP), jeśli określono output(*print)	*USE	*EXECUTE
	Zbiór wyjściowy, jeśli został podany	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Zbiór opisów pól QSYS/QASRRSTO, jeśli podano zbiór wyjściowy, który nie istnieje	*USE	*EXECUTE
RTVCFGSTS	Obiekt	*OBJOPR	*EXECUTE

Komendy konfiguracji

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
RTVCFGSRC	Obiekt	*USE	*EXECUTE
	Zbiór źródłowy	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
SAVCFG [2]	Zbiór składowania, jeśli jest pusty	*USE, *ADD	*EXECUTE
	Zbiór składowania, jeśli istnieją w nim rekordy	*USE, *ADD, *OBJMGT	*EXECUTE
SAVRSTCFG	W systemie źródłowym są to takie same uprawnienia, jak wymagane dla komendy SAVCFG.		
	W systemie docelowym są to takie same uprawnienia, jak wymagane dla komendy RSTCFG.		
VRYCFG [3,6]	Obiekt	*USE, *OBJMGT	*EXECUTE
WRKCFGSTS [4]	Obiekt	*OBJOPR	*EXECUTE

1 Jeśli użytkownik ma uprawnienia specjalne *SAVSYS, nie potrzebuje podanych tu uprawnień.

2 Użytkownik musi mieć uprawnienia specjalne *SAVSYS.

3 Jeśli użytkownik posiada uprawnienie specjalne *JOBCTL, uprawnienie do obiektu nie jest niezbędne.

4 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

5 Aby podać parametr ALWOBJDIF(*ALL), użytkownik musi mieć uprawnienia specjalne *ALLOBJ.

6 Jeśli status ma wartość *ALLOCATE lub *DEALLOCATE, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG do biblioteki nośników.

Komendy list konfiguracji

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDCFGLE [2]	Lista konfiguracji	*CHANGE, *OBJMGT	*EXECUTE
CHGCFGL [2]	Lista konfiguracji	*CHANGE, *OBJMGT	*EXECUTE
CHGCFGLE [2]	Lista konfiguracji	*CHANGE, *OBJMGT	*EXECUTE
CPYCFGL [2]	Lista konfiguracji	*USE, *OBJMGT	*ADD
CRTCFGL [2]	Lista konfiguracji		
DLTCFGL	Lista konfiguracji	*OBJEXIST	*EXECUTE
DSPCFGL [2]	Lista konfiguracji	*USE, *OBJMGT	*EXECUTE
RMVCFGLE [2]	Lista konfiguracji	*CHANGE, *OBJMGT	*EXECUTE
WRKCFGL [1, 2]	Lista konfiguracji	*OBJOPR	*EXECUTE

1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

2 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

Komendy listy połączeń

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
DLTCNNL	Lista połączeń	*OBJEXIST	*EXECUTE
DSPCNNL	Lista połączeń	*USE	*EXECUTE
WRKCNNL [1]	Lista połączeń	*OBJOPR	*EXECUTE

1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

Komendy opisu kontrolera

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGCTLAPPC [2]	Opis kontrolera	*CHANGE, *OBJMGT	*EXECUTE
	Opis linii (SWTLINLST)	*USE	*EXECUTE
	Lista połączeń (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLASC [2]	Opis kontrolera	*CHANGE, *OBJMGT	*EXECUTE
	Opis linii (SWTLINLST)	*USE	*EXECUTE
CHGCTLBSC [2]	Opis kontrolera	*CHANGE, *OBJMGT	*EXECUTE
	Opis linii (SWTLINLST)	*USE	*EXECUTE
CHGCTLFNC [2]	Opis kontrolera	*CHANGE, *OBJMGT	*EXECUTE
	Opis linii (SWTLINLST)	*USE	*EXECUTE
CHGCTLHOST [2]	Opis kontrolera	*CHANGE, *OBJMGT	*EXECUTE
	Opis linii (SWTLINLST)	*USE	*EXECUTE
	Lista połączeń (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLLWS [2]	Opis kontrolera	*CHANGE, *OBJMGT	*EXECUTE
	Program (INZPGM)	*USE	*EXECUTE
CHGCTLNET [2]	Opis kontrolera	*CHANGE, *OBJMGT	*EXECUTE
CHGCTLRTL [2]	Opis kontrolera	*CHANGE, *OBJMGT	*EXECUTE
	Opis linii (SWTLINLST)	*USE	*EXECUTE
CHGCTLRWS [2]	Opis kontrolera	*CHANGE, *OBJMGT	*EXECUTE
	Opis linii (SWTLINLST)	*USE	*EXECUTE
	Lista połączeń (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLTAP [2]	Opis kontrolera	*CHANGE, *OBJMGT	*EXECUTE
CHGCTLVWS [2]	Kontroler	*CHANGE, *OBJMGT	*EXECUTE
CRTCTLAPPC [2]	Opis linii (LINE lub SWTLINLST)	*USE	*EXECUTE
	Opis urządzenia (DEV)	*USE	*EXECUTE
	Lista połączeń (CNNLSTOUT)	*USE	*EXECUTE
	Opis kontrolera		
CRTCTLASC [2]	Opis linii (LINE lub SWTLINLST)	*USE	*EXECUTE
	Opis urządzenia (DEV)	*USE	*EXECUTE
	Opis kontrolera		

Komendy opisu kontrolera

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTCTLBSC [2]	Opis linii (LINE lub SWTLINLST)	*USE	*EXECUTE
	Opis urządzenia (DEV)	*USE	*EXECUTE
	Opis kontrolera		
CRTCTLFNC [2]	Opis linii (LINE lub SWTLINLST)	*USE	*EXECUTE
	Opis urządzenia (DEV)	*USE	*EXECUTE
	Opis kontrolera		
CRTCTLHOST [2]	Opis linii (LINE lub SWTLINLST)	*USE	*EXECUTE
	Opis urządzenia (DEV)	*USE	*EXECUTE
	Lista połączeń (CNNLSTOUT)	*USE	*EXECUTE
	Opis kontrolera		
CRTCTLLWS [2]	Opis urządzenia (DEV)	*USE	*EXECUTE
	Opis kontrolera		
	Program (INZPGM)	*USE	*EXECUTE
CRTCTLNET [2]	Opis linii (LINE)	*USE	*EXECUTE
	Opis urządzenia (DEV)	*USE	*EXECUTE
	Opis kontrolera		
CRTCTLRTL [2]	Opis linii (LINE lub SWTLINLST)	*USE	*EXECUTE
	Opis urządzenia (DEV)	*USE	*EXECUTE
	Opis kontrolera		
CRTCTLRWS [2]	Opis linii (LINE lub SWTLINLST)	*USE	*EXECUTE
	Opis urządzenia (DEV)	*USE	*EXECUTE
	Lista połączeń (CNNLSTOUT)	*USE	*EXECUTE
	Opis kontrolera		
CRTCTLTAP [2]	Opis urządzenia (DEV)	*USE	*EXECUTE
	Opis kontrolera		
CRTCTLVWS [2]	Opis urządzenia (DEV)	*USE	*EXECUTE
	Opis kontrolera		
DLTCTLD	Opis kontrolera	*OBJEXIST	*EXECUTE
DSPCTLD	Opis kontrolera	*USE	*EXECUTE
ENDCTLRCY	Opis kontrolera	*USE	*EXECUTE
PRTCMNSEC [3]			
RSMCTLRCY	Opis kontrolera	*USE	*EXECUTE
WRKCTLD [1]	Opis kontrolera	*OBJOPR	*EXECUTE

1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

2 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

3 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *ALLOBJ i *IOSYSCFG lub *AUDIT.

Komendy szyfrowania

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
	Kolejka komunikatów QHST	*OBJOPR, *ADD	*EXECUTE
CHGCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	Kolejka komunikatów QHST	*OBJOPR, *ADD	*EXECUTE
CHGMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	Kolejka komunikatów QHST	*OBJOPR, *ADD	*EXECUTE
CPHDTA (Q)			
ENCCPHK (Q)			
ENCFRMMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
ENCTOMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
GENCPHK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
GENCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
	QCRP/QPCRGENX *FILE	*OBJOPR, *READ	*EXECUTE
	Kolejka komunikatów QHST	*OBJOPR, *ADD	*EXECUTE
GENMAC (Q)			
GENPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
RMVCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *DLT	*EXECUTE
	Kolejka komunikatów QHST	*OBJOPR, *ADD	*EXECUTE
SETMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	Kolejka komunikatów QHST	*OBJOPR, *ADD	*EXECUTE
TRNPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
VFYMSTK (Q)	Kolejka komunikatów QHST	*OBJOPR, *ADD	*EXECUTE
VFYPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, READ	*EXECUTE

Komendy obszaru danych

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGDTAARA [1]	Obszar danych	*CHANGE	*EXECUTE
CRTDTAARA [1]	Obszar danych		*READ, *ADD
	Opis urządzenia APPC [4]	*CHANGE	
DLTDTAARA	Obszar danych	*OBJEXIST	*EXECUTE
DSPDTAARA	Obszar danych	*USE	*EXECUTE

Komendy obszaru danych

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
RTVDTAARA [2]	Obszar danych	*USE	*EXECUTE
WRKDTAARA [3]	Obszar danych	Dowolne uprawnienia	*USE

1 Jeśli komendy tworzenia i zmiany obszaru danych uruchamiane są za pomocą funkcji języka wysokiego poziomu, te uprawnienia nadal są wymagane, chociaż uprawnienia do komendy nie.

2 Uprawnienia sprawdzane są w trakcie uruchamiania, ale nie w trakcie kompilowania.

3 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

4 Uprawnienia sprawdzane są podczas używania obszaru danych.

Komendy kolejek danych

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTDTAQ	Kolejka danych		*READ, *ADD
	Docelowa kolejka danych dla programu QSNDDTAQ	*OBJOPR, *ADD	*EXECUTE
	Źródłowa kolejka danych dla programu QRCVDTAQ	*OBJOPR, *READ	*EXECUTE
	Opis urządzenia APPC [2]	*CHANGE	
DLTDTAQ	Kolejka danych	*OBJEXIST	*EXECUTE
WRKDTAQ [1]	Kolejka danych	*READ	*USE

1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

2 Uprawnienia sprawdzane są podczas używania obszaru danych.

Komendy opisów urządzeń

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CFGDEVMLB [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVAPPC [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
	Opis trybu (MODE)	*USE	*EXECUTE
CHGDEVASC [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVASP[4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVBSC [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVCRP[4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVDKT [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVDSP [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
	Drukarka (PRINTER)	*USE	*EXECUTE
CHGDEVFNC [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVHOST [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVINTR [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CHGDEVMLB [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVNET [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVOPT [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVPRT [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
	Lista weryfikacji (jeśli podano)	*READ	*EXECUTE
CHGDEVRTL [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVSNPT [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVSNUF [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVTAP [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CRTDEVAPPC [4]	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis urządzenia		
	Opis trybu (MODE)	*USE	*EXECUTE
CRTDEVASC [4]	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis urządzenia		
CRTDEVASP [4]	Opis urządzenia		*EXECUTE
CRTDEVBSC [4]	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis urządzenia		
CRTDEVCRP[4]	Opis urządzenia		*EXECUTE
CRTDEVDKT [4]	Opis urządzenia		*EXECUTE
CRTDEVDSP [4]	Opis drukarki (PRINTER)	*USE	*EXECUTE
	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis urządzenia		
CRTDEVFNC [4]	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis urządzenia		
CRTDEVHOST [4]	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis urządzenia		
CRTDEVINTR [4]	Opis urządzenia		
CRTDEVMLB [4]	Opis urządzenia		*EXECUTE
CRTDEVNET [4]	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis urządzenia		
CRTDEVOPT [4]	Opis urządzenia		*EXECUTE
CRTDEVPRT [4]	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis urządzenia		
	Lista weryfikacji (jeśli podano)	*READ	*EXECUTE
CRTDEVRTL [4]	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis urządzenia		
CRTDEVSNPT [4]	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis urządzenia		
CRTDEVSNUF [4]	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis urządzenia		

Komendy opisów urządzeń

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTDEVTAP [4]	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis urządzenia		
DLTDEVD [1]	Opis urządzenia	*OBJEXIST	*EXECUTE
DSPCNNSTS	Opis urządzenia	*OBJOPR	*EXECUTE
DSPDEVD	Opis urządzenia	*USE	*EXECUTE
ENDDEVRCY	Opis urządzenia	*USE	*EXECUTE
HLDCMNDEV [2]	Opis urządzenia	*OBJOPR	*EXECUTE
PRTCMNSEC [4, 5]			
RLSCMNDEV	Opis urządzenia	*OBJOPR	*EXECUTE
RSMDEVRCY	Opis urządzenia	*USE	*EXECUTE
WRKDEVD [3]	Opis urządzenia	*OBJOPR	*EXECUTE

1 Aby usunąć kolejkę wyjściową, wymagane jest uprawnienie *OBJEXIST do kolejki wyjściowej oraz uprawnienie do odczytu dla biblioteki QUSRSYS.

2 Użytkownik musi mieć uprawnienia specjalne sterowania zadaniem (*JOBCTL) oraz uprawnienie do korzystania z obiektu dla opisu zadania.

3 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

4 Aby uruchomić komendę, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

5 Aby uruchomić komendę, użytkownik musi mieć uprawnienia specjalne *ALLOBJ.

Komendy emulacji urządzeń

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDEMLCFGE	Zbiór konfiguracyjny emulacji	*CHANGE	*EXECUTE
CHGEMLCFGE	Zbiór konfiguracyjny emulacji	*CHANGE	*EXECUTE
EJTEMLOUT	Opis emulowanego urządzenia, jeśli określono	*OBJOPR	*EXECUTE
	Opis emulowanego urządzenia, jeśli określono położenie	*OBJOPR	*EXECUTE
ENDPRTEML	Opis emulowanego urządzenia, jeśli określono	*OBJOPR	*EXECUTE
	Opis emulowanego urządzenia, jeśli określono położenie	*OBJOPR	*EXECUTE
EMLPRTKEY	Opis emulowanego urządzenia, jeśli określono	*OBJOPR	*EXECUTE
	Opis emulowanego urządzenia, jeśli określono położenie	*OBJOPR	*EXECUTE
EML3270	Opis emulowanego urządzenia	*OBJOPR	*EXECUTE
	Opis emulowanego kontrolera	*OBJOPR	*EXECUTE
RMVEMLCFGE	Zbiór konfiguracyjny emulacji	*CHANGE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
STREML3270	Zbiór konfiguracyjny emulacji	*OBJOPR	*EXECUTE
	Urządzenie emulowane, opis emulowanego kontrolera, terminal i opis kontrolera terminalu	*OBJOPR	*EXECUTE
	Opis drukarki, program użytkownika obsługi wyjścia i tabele translacji, jeśli podano	*OBJOPR	*EXECUTE
STRPRTEML	Zbiór konfiguracyjny emulacji	*OBJOPR	*EXECUTE
	Opis urządzenia emulowanego i opis emulowanego kontrolera	*OBJOPR	*EXECUTE
	Opis drukarki, zbiór wydruku, kolejka komunikatów, opis zadania, kolejka zadań i tabele konwersji, jeśli określono	*OBJOPR	*EXECUTE
SNDEMLIGC	Źródłowy zbiór	*OBJOPR	*EXECUTE
TRMPRTEML	Opis emulowanego urządzenia	*OBJOPR	*EXECUTE

Komendy katalogu i tworzenia cienia katalogu

Te komendy nie wymagają żadnych uprawnień do obiektu:

ADDDIRE [2]	CHGDIRSHD [1]	ENDDIRSHD [4]	STRDIRSHD [4]
ADDDIRSHD [1]	CPYFRMDIR [1]	RMVDIRE [1]	WRKDIRE [3,5]
CHGSYSDIRA [2]	CPYTODIR [1]	RMVDIRSHD [1]	WRKDIRLOC [1,5]
CHGDIRE [3]	DSPDIRE	RNMDIRE [2]	WRKDIRSHD [1,5]

1 Użytkownik musi mieć uprawnienia specjalne *SECADM.

2 Użytkownik musi mieć uprawnienia specjalne *SECADM lub *ALLOBJ.

3 Użytkownik z uprawnieniami specjalnymi *SECADM może pracować ze wszystkimi pozycjami katalogu. Użytkownicy bez uprawnień specjalnych *SECADM mogą pracować tylko ze swoimi pozycjami.

4 Użytkownik musi mieć uprawnienia specjalne *JOBCTL.

5 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

Komendy dysków

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Te komendy nie wymagają żadnych uprawnień do obiektów:

ENDDSKRGZ (Q) [1]	STRDSKRGZ (Q) [1]	WRKDSKSTS

1 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *ALLOBJ.

Komendy tranzytu terminalu

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komendy tranzytu terminalu

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ENDPASTHR			
STRPASTHR	Urządzenie APPC w systemie źródłowym	*CHANGE	*EXECUTE
	Urządzenie APPC w systemie docelowym	*CHANGE	*EXECUTE
	Kontroler wirtualny w systemie docelowym [1]	*USE	*EXECUTE
	Urządzenie wirtualne w systemie docelowym [1],[2]	*CHANGE	*EXECUTE
	Program podany w wartości systemowej QRMTSIGN w systemie docelowym, jeśli jest [1]	*USE	*USE
TFRPASTHR			

1 Profil użytkownika, który wymaga tego uprawnienia, to profil uruchamiający zadanie wsadowe tranzytu. W przypadku tranzytu pomijającego ekran wpisania się profil użytkownika jest określany w parametrze użytkownika zdalnego (RMTUSER). W przypadku tranzytu używającego standardowej procedury wpisywania się (RMTUSER(* NONE)), użytkownikiem jest domyślny profil użytkownika określony w pozycji komunikacji podsystemu obsługującego żądanie tranzytu. Zazwyczaj jest to użytkownik QUSER.

2 Jeśli tranzyt używa standardowej procedury wpisywania się, to profil użytkownika określony na ekranie wpisania się na systemie docelowym musi mieć uprawnienie do tego obiektu.

Komendy dystrybucji

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDDSTQ (Q)			
ADDDSTRTE (Q)			
ADDDSTSYSN (Q)			
CFGDSTSRV (Q)			
CFGRPDS (Q)			
CHGDSTD [1]	Dokument [2]	*CHANGE	*EXECUTE
CHGDSTQ (Q)			
CHGDSTRTE (Q)			
DLTDST [1]			
DSPDSTLOG (Q)	Kronika	*USE	*EXECUTE
	Dziennik	*USE	*EXECUTE
DSPDSTSRV (Q)			
HLDDSTQ (Q)			
INZDSTQ (Q)			
QRYDST [1]	Żądany zbiór	*CHANGE	*EXECUTE
RCVDST [1]	Żądany zbiór	*CHANGE	*EXECUTE
	Folder	*CHANGE	*EXECUTE
RLSDSTQ (Q)			

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
RMVDSTQ (Q)			
RMVDSTRTE (Q)			
RMVDSTSYSN (Q)			
SNDDST [1]	Żądany zbiór lub dokument	*USE	*EXECUTE
SNDDSTQ (Q)			
WRKDSTQ (Q)			
WRKDPCQ (Q)			

1 Jeśli użytkownik żąda dystrybucji za innego użytkownika, musi mieć uprawnienia do pracy w imieniu tego użytkownika.

2 Kiedy dystrybucja jest wprowadzana.

Komendy list dystrybucyjnych

Te komendy nie wymagają żadnych uprawnień do obiektu:

ADDDSTLE [1]	CRTDSTL	DSPDSTL	RNMDSTL [1]
CHGDSTL[1]	DLTDSTL [1]	RMVDSTLE [1]	WRKDSTL [2]

1 Użytkownik musi mieć uprawnienia specjalne *SECADM lub być właścicielem listy dystrybucyjnej.

2 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

Komendy obiektów biblioteki dokumentów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ADDDLOAUT	Obiekt biblioteki dokumentów	*ALL lub właściciel	*EXECUTE
CHGDLOAUD [1]			
CHGDLOAUT	Obiekt biblioteki dokumentów	*ALL lub właściciel	*EXECUTE
CHGDLOOWN	Obiekt biblioteki dokumentów	Właściciel lub uprawnienia specjalne *ALLOBJ	*EXECUTE
	Poprzedni profil użytkownika	*DLT	*EXECUTE
	Nowy profil użytkownika	*ADD	*EXECUTE
CHGDLOPGP	Obiekt biblioteki dokumentów	Właściciel lub uprawnienia specjalne *ALLOBJ	*EXECUTE
	Poprzedni podstawowy profil grupowy	*DLT	*EXECUTE
	Nowy podstawowy profil grupowy	*ADD	*EXECUTE
CHGDOCD [2]	Opis dokumentu	*CHANGE	*EXECUTE
CHKDLO [2]	Obiekt biblioteki dokumentów	Jeśli wymagane przez słowo kluczowe AUT	*EXECUTE

Komendy DLO

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHKDOC	Dokument	*CHANGE	*EXECUTE
	Słownik sprawdzania pisowni	*CHANGE	*EXECUTE
CPYDOC	Z dokumentu	*USE	*EXECUTE
	Do dokumentu, jeśli zastępowany jest istniejący dokument	*CHANGE	*EXECUTE
	Do folderu, jeśli dokument docelowy jest nowy	*CHANGE	*EXECUTE
CRTDOC	W folderze	*CHANGE	*EXECUTE
CRTFLR	W folderze	*CHANGE	*EXECUTE
DLTDLO [3]	Obiekt biblioteki dokumentów	*ALL	*EXECUTE
DLTDOCL[20]	Lista dokumentów	*ALL [4]	*EXECUTE
DMPDLO [15]			
DSPAUTLDLO	Lista autoryzacji	*USE	*EXECUTE
	Obiekt biblioteki dokumentów	*USE	*EXECUTE
DSPDLOAUD[21]	Zbiór wyjściowy, jeśli został podany	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
DSPDLOAUT	Obiekt biblioteki dokumentów	*USE lub właściciel	*EXECUTE
DSPDLONAM[22]	Obiekt biblioteki dokumentów	*USE	*EXECUTE
DSPDOC	Dokument	*USE	*EXECUTE
DSPFLR	Folder	*USE	*EXECUTE
EDTDLOAUT	Obiekt biblioteki dokumentów	*ALL lub właściciel	*EXECUTE
EDTDOC	Dokument	*CHANGE	*EXECUTE
FILDOC [2]	Żądany zbiór	*USE	*EXECUTE
	Folder	*CHANGE	*EXECUTE
MOVDOC	Z folderu, jeśli dokument źródłowy jest w folderze	*CHANGE	*EXECUTE
	Z dokumentu	*ALL	*EXECUTE
	Do folderu	*CHANGE	*EXECUTE
MRGDOC [5]	Dokument	*USE	*EXECUTE
	Z folderu	*USE	*EXECUTE
	Do dokumentu, jeśli dokument jest zastępowany	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Do folderu, jeśli dokument docelowy jest nowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
PAGDOC	Dokument	*CHANGE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
PRTDOC	Folder	*USE	*EXECUTE
	Dokument	*USE	*EXECUTE
	Komendy DLTPF, DLTF i DLTOVR, jeśli podano instrukcję *INDEX*	*USE	*EXECUTE
	Komendy CRTPF, OVRPRTF, DLTSPLF i DLTOVR, jeśli podano instrukcję *RUN*	*USE	*EXECUTE
	Zeskładowany dokument, jeśli podano parametr SAVOUTPUT (*YES)	*USE	*EXECUTE
	Zeskładowany folder, jeśli podano parametr SAVOUTPUT (*YES)	*USE	*EXECUTE
QRYDOCLIB [2,6]	Żądany zbiór	*USE	*EXECUTE
	Lista dokumentów, jeśli istnieje	*CHANGE	*EXECUTE
RCLDLO	Obiekt biblioteki dokumentów		
	Dokumenty wewnętrzne lub wszystkie dokumenty i foldery [16]		
RGZDLO	Obiekt biblioteki dokumentów	*CHANGE lub właściciel	*EXECUTE
	DLO(*ALL), DLO(*ALL) FLR(*ANY) lub DLO(*ALL) FLR(*ANY) MAIL(*YES)[16]		
RMVDLOAUT	Obiekt biblioteki dokumentów	*ALL lub właściciel	*EXECUTE
RNMDLO	Obiekt biblioteki dokumentów	*ALL	*EXECUTE
	W folderze	*CHANGE	*EXECUTE
RPLDOC [2]	Żądany zbiór	*READ	*EXECUTE
	Dokument	*CHANGE	*EXECUTE
RSTDLO	Obiekt biblioteki dokumentów, jeśli jest zastępowany	*ALL[10]	*EXECUTE
	Folder nadrzędny, jeśli nowy obiekt DLO	*CHANGE[10]	*EXECUTE
	Profil użytkownika właściciela, jeśli nowy obiekt DLO	*ADD[10]	*EXECUTE
	Zbiór wyjściowy, jeśli został podany	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Zbiór składowania	*USE	*EXECUTE
	Zbiór nośnika optycznego (OPTFILE) [17]	*R	Nie dotyczy
	Przedrostek ścieżki pliku nośnika optycznego (OPTFILE) [17]	*X	Nie dotyczy
	Wolumin optyczny [19]	*USE	Nie dotyczy
	Jednostka taśm, jednostka dyskietek i jednostka optyczna	*USE	*EXECUTE
RSTS36FLR [11,12,14]	Folder S/36	*USE	*EXECUTE
	Do folderu	*CHANGE	*EXECUTE
	Zbiór urządzenia lub opis urządzenia	*USE	*EXECUTE
RTVDLONAM[22]	Obiekt biblioteki dokumentów	*USE	*EXECUTE

Komendy DLO

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
RTVDOC [2]	Dokument, jeśli jest sprawdzany	*CHANGE	*EXECUTE
	Dokument, jeśli nie jest sprawdzany	*USE	*EXECUTE
	Żądany zbiór	*CHANGE	*EXECUTE
SAVDLO [7,13]	Obiekt biblioteki dokumentów	*ALL[10]	*EXECUTE
	Jednostka taśm, jednostka dyskietek i jednostka optyczna	*USE	*EXECUTE
	Zbiór składowania, jeśli jest pusty	*USE, *ADD	*EXECUTE
	Zbiór składowania, jeśli istnieją w nim rekordy	*USE, *ADD, *OBJMGT	*EXECUTE
	Zbiór wyjściowy, jeśli został podany	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Zbiór nośnika optycznego (OPTFILE) [17]	*RW	Nie dotyczy
	Katalog nadrzędny pliku nośnika optycznego (OPTFILE) [17]	*WX	Nie dotyczy
	Przedrostek ścieżki pliku nośnika optycznego (OPTFILE) [17]	*X	Nie dotyczy
	Katalog główny (/) woluminu [17, 18]	*RWX	Nie dotyczy
	Wolumin optyczny [19]	*CHANGE	Nie dotyczy
SAVRSTDLO	W systemie źródłowym są to takie same uprawnienia, jak wymagane dla komendy SAVDLO.		
	W systemie docelowym są to takie same uprawnienia, jak wymagane dla komendy RSTDLO.		
WRKDOC	Folder	*USE	
WRKFLR	Folder	*USE	

1 Użytkownik musi mieć uprawnienia specjalne *AUDIT.

2 Jeśli użytkownik pracuje w imieniu innego użytkownika, sprawdzane są uprawnienia tego użytkownika do obiektu.

3 Aby usunąć folder i wszystkie obiekty znajdujące się w nim, użytkownik musi mieć uprawnienia *ALL do wszystkich obiektów w tym folderze.

4 Jeśli użytkownik ma uprawnienia specjalne *ALLOBJ lub *SECADM, nie potrzebuje uprawnień *ALL do listy biblioteki dokumentów.

5 Użytkownik musi mieć uprawnienia do obiektu używanego jako źródło scalania. Na przykład jeśli podano parametr MRGTYPE(*QRY), użytkownik musi mieć uprawniania do zapytania podanego w parametrze QRYDFN.

6 Tylko obiekty, które spełniają kryteria zapytania i do których użytkownik ma przynajmniej uprawnienia *USE, zwracane są do listy dokumentów lub zbioru wyjściowego.

7 Wymagane są uprawnienia *SAVSYS, *ALLOBJ lub zarejestrowanie się w katalogu dystrybucyjnym systemu.

8 Aby użyć kombinacji parametru RSTDLO DLO(*MAIL), wymagane są uprawnienia specjalne *SAVSYS lub *ALLOBJ.

9 Aby podać parametr ALWOBJDIF(*ALL), wymagane są uprawnienia *ALLOBJ.

10 Jeśli użytkownik ma uprawnienia specjalne *SAVSYS lub *ALLOBJ, nie potrzebuje podanych tu uprawnień.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
[11] Jeśli dokument ma być zastąpiony, wymagane są uprawnienia *ALL. Użytkownik musi mieć uprawnienie operacyjne i do danych dla folderu w przypadku odtwarzania nowych informacji do folderów albo musi posiadać uprawnienie *ALLOBJ.			
[12] Jeśli używane dla katalogu danych, wymagane są tylko uprawnienia do komendy.			
[13] Aby użyć podanych poniżej podanych kombinacji parametrów, wymagane są uprawnienia specjalne *SAVSYS lub *ALLOBJ: SAVDLO DLO(*ALL) FLR(*ANY) SAVDLO DLO(*MAIL) SAVDLO DLO(*CHG) SAVDLO DLO(*SEARCH) OWNER(nie *CURRENT)			
[14] Użytkownik musi być zarejestrowany w katalogu dystrybucyjnym systemu, jeśli folder źródłowy jest folderem dokumentów.			
[15] Aby wykonać zrzut wewnętrznych obiektów biblioteki dokumentów, wymagane są uprawnienia specjalne *ALLOBJ.			
[16] Użytkownik musi mieć uprawnienia specjalne *ALLOBJ lub *SECADM.			
[17] To sprawdzanie uprawnień przeprowadzane jest jedynie wtedy, kiedy nośnik optyczny jest w formacie UDF (Universal Disk Format).			
[18] To sprawdzanie uprawnień przeprowadzane jest jedynie wtedy, kiedy nośnik optyczny jest czyszczony.			
[19] Woluminy optyczne nie są rzeczywistymi obiektami systemowymi. Dowiązanie między woluminem optycznym a listą autoryzacji używaną do ochrony obiektu jest utrzymywane przez funkcję obsługi nośników optycznych.			
[20] Użytkownik musi mieć uprawnienie specjalne *ALLOBJ, gdy określono parametry OWNER (*ALL) lub OWNER (nazwa), a nazwą jest inny profil użytkownika jako program wywołujący.			
[21] Aby używać tej komendy, użytkownik musi mieć uprawnienie specjalne *ALLOBJ lub *AUDIT.			
[22] Użytkownik musi mieć uprawnienie specjalne do obiektów (*ALLOBJ), aby używać tej komendy w przypadku określenia parametru *DST dla klasy obiektu do znalezienia.			

Komendy zestawu znaków dwubajtowych (DBCS)

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CPYIGCTBL	Tabela sortowania DBCS (*IN)	*ALL	*EXECUTE
	Tabela sortowania DBCS (*OUT)	*USE	*EXECUTE
CRTIGCDCT	Słownik konwersji DBCS		*READ, *ADD
DLTIGCDCT	Słownik konwersji DBCS	*OBJEXIST	*EXECUTE
DLTIGCSRT	Tabela sortowania DBCS	*OBJEXIST	*EXECUTE
DLTIGCTBL	Tabela czcionek DBCS	*OBJEXIST	*EXECUTE
DSPIGCDCT	Słownik konwersji DBCS	*USE	*EXECUTE
EDTIGCDCT	Słownik konwersji DBCS	*USE, *UPD	*EXECUTE
	Słownik użytkownika	*ADD, *DLT	*EXECUTE
STRCGU	Tabela sortowania DBCS	*CHANGE	*EXECUTE
	Tabela czcionek DBCS	*CHANGE	*EXECUTE

Komendy zestawu znaków dwubajtowych (DBCS)

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
STRFMA	Tabela czcionek DBCS, jeśli podano opcję kopiowania do	*OBJOPR, *READ *ADD, *UPD	*EXECUTE
	Tabela czcionek DBCS, jeśli podano opcję kopiowania z	*OBJOPR, *READ	*EXECUTE
	Zbiór roboczy FMA (QGPL/QAFSVDF)	*CHANGE	*EXECUTE

Komendy opisu edycji

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTEDTD	Opis edycji		*EXECUTE, *ADD
DLTEDTD	Opis edycji	*OBJEXIST	*EXECUTE
DSPEDTD	Opis edycji	*OBJOPR	*EXECUTE
WRKEDTD [1]	Opis edycji	Dowolne uprawnienia	*USE

1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

Komendy zmiennych środowiskowych

Te komendy nie wymagają żadnych uprawnień do obiektu.			
ADDENVVAR[1]	CHGENVVAR [1]	RMVENVVAR[1]	WRKENVVAR[1]

1 Aby zaktualizować zmienne środowiskowe na poziomie systemu, użytkownik musi mieć uprawnienia specjalne *JOBCTL.

Komendy konfiguracji rozszerzonej bezprzewodowej sieci LAN

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDEWCBCDE	Zbiór źródłowy	*USE	*EXECUTE
ADDEWCM	Zbiór źródłowy	*USE	*EXECUTE
ADDEWCPTCE	Zbiór źródłowy	*USE	*EXECUTE
ADDEWLM	Zbiór źródłowy	*USE	*EXECUTE
CHGEWCBCDE	Zbiór źródłowy	*USE	*EXECUTE
CHGEWCM	Zbiór źródłowy	*USE	*EXECUTE
CHGEWCPTCE	Zbiór źródłowy	*USE	*EXECUTE
CHGEWLM	Zbiór źródłowy	*USE	*EXECUTE
DSPEWCBCDE	Zbiór źródłowy	*USE	*EXECUTE
DSPEWCM	Zbiór źródłowy	*USE	*EXECUTE
DSPEWCPTCE	Zbiór źródłowy	*USE	*EXECUTE
DSPEWLM	Zbiór źródłowy	*USE	*EXECUTE
RMVEWCBCDE	Zbiór źródłowy	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
RMVEWCPTCE	Zbiór źródłowy	*USE	*EXECUTE

Komendy zbiorów

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ADDICFDEVE	Plik ICF	*OBJOPR, *OBJMGT	*EXECUTE
ADDLFM	Zbiór logiczny	*OBJOPR, *OBJMGT lub *OBJALTER	*EXECUTE, *ADD
	Zbiór, do którego odniesienie znajduje się w parametrze DTAMBRS, gdy zbiór logiczny zawiera klucz	*OBJOPR, *OBJMGT lub *OBJALTER	*EXECUTE
	Zbiór, do którego odniesienie znajduje się w parametrze DTAMBRS, gdy zbiór logiczny nie zawiera klucza	*OBJOPR	*EXECUTE
ADDPFCST	Zbiór zależny, jeśli podano parametr TYPE(*REFCST)	*OBJMGT lub *OBJALTER	*EXECUTE
	Zbiór nadrzędny, jeśli podano parametr TYPE(*REFCST)	*OBJMGT lub *OBJREF	*EXECUTE
	Zbiór, jeśli podano parametry TYPE(*UNQCST) lub TYPE(*PRIKEY)	*OBJMGT	*EXECUTE
ADDPFM	Zbiór fizyczny	*OBJOPR, *OBJMGT lub *OBJALTER	*EXECUTE, *ADD
ADDPFTRG	Zbiór fizyczny dla programu wyzwalanego wstawianiem	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Zbiór fizyczny dla programu wyzwalanego usuwaniem	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Zbiór fizyczny dla programu wyzwalanego aktualizacją	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Program wyzwalany	*EXECUTE	*EXECUTE
CHGDDMF	Plik DDM	*OBJOPR, *OBJMGT	*EXECUTE
	Opis urządzenia [7]	*CHANGE	
CHGDKTF	Zbiór dyskietkowy	*OBJOPR, *OBJMGT	*EXECUTE
	Urządzenie, jeśli w komendzie podano nazwę urządzenia	*OBJOPR	*EXECUTE
CHGDSPF	Zbiór ekranowy	*OBJOPR, *OBJMGT	*EXECUTE
	Urządzenie, jeśli podano nazwę urządzenia	*OBJOPR	*EXECUTE

Komendy zbiorów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGDTA	Zbiór danych	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	Program	*USE	*EXECUTE
	Zbiór ekranowy	*USE	*EXECUTE
CHGICFDEVE	Plik ICF	*OBJOPR, *OBJMGT	*EXECUTE
CHGICFF	Plik ICF	*OBJOPR, *OBJMGT	*EXECUTE
CHGLF	Zbiór logiczny	*OBJMGT lub *OBJALTER	*EXECUTE
CHGLFM	Zbiór logiczny	*OBJMGT lub *OBJALTER	*EXECUTE
CHGPF	Zbiór fizyczny	*OBJMGT lub *OBJALTER	*EXECUTE
CHGPFCST	Zbiór zależny	*OBJMGT lub *OBJALTER	*EXECUTE
CHGPFM	Zbiór fizyczny	*OBJMGT lub *OBJALTER	*EXECUTE
CHGPFTRG	Zbiór fizyczny	*OBJMGT lub *OBJALTER	*EXECUTE
CHGPRTF	Zbiór wydruku	*OBJOPR, *OBJMGT	*EXECUTE
	Urządzenie, jeśli podano nazwę urządzenia	*OBJOPR	*EXECUTE
CHGSAVF	Zbiór składowania	*OBJOPR, *OBJMGT	*EXECUTE
CHGSRCPF	Źródłowy zbiór fizyczny	*OBJMGT lub *OBJALTER	*EXECUTE
CHGTAPF	Zbiór taśmowy	*OBJOPR, *OBJMGT	*EXECUTE
	Urządzenie, jeśli podano nazwę urządzenia	*OBJOPR	*EXECUTE
CLRPFM	Zbiór fizyczny	*OBJOPR, *OBJMGT lub *OBJALTER, *DLT	*EXECUTE
CLRSAVF	Zbiór składowania	*OBJOPR, *OBJMGT	*EXECUTE
CPYF	Źródłowy zbiór	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór (zbiór urządzenia)	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór (zbiór fizyczny)	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Oparty na zbiorze, jeśli zbiór początkowy jest zbiorem logicznym	*READ	*EXECUTE
CPYFRMDKT	Źródłowy zbiór	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór (zbiór urządzenia)	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór (zbiór fizyczny)	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CPYFRMIMPF	Źródłowy zbiór	*OBJOPR, *READ	*USE
	Docelowy zbiór (zbiór urządzenia)	*OBJOPR, *READ	*USE
	Docelowy zbiór (zbiór fizyczny)	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Oparty na zbiorze, jeśli zbiór początkowy jest zbiorem logicznym	*READ	*USE
CPYFRMQRYF [1]	Źródłowy zbiór	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór (zbiór urządzenia)	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór (zbiór fizyczny)	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
CPYFRMSTMF	Plik strumieniowy	*R	
	Katalogi w przedrostku nazwy ścieżki pliku strumieniowego	*X	
	Docelowy zbiór bazy danych, jeśli podano MBROPT(*ADD)	*X, *ADD	*X
	Docelowy zbiór bazy danych, jeśli podano MBROPT(*REPLACE)	*X, *ADD, *DLT, *OBJMGT	*X
	Docelowy zbiór bazy danych, jeśli utworzono nowy podzbiór	*X, *OBJMGT, *ADD	*X, *ADD
	Tabela konwersji *TBL używana do tłumaczenia danych	*OBJOPR	*X
	Docelowy zbiór składowania istnieje	*RX, *ADD, *OBJMGT	*X
	Docelowy zbiór składowania jest tworzony		*RX, *ADD
CPYFRMTAP	Źródłowy zbiór	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór (zbiór urządzenia)	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór (zbiór fizyczny)	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
CPYSRCF	Źródłowy zbiór	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór (zbiór urządzenia)	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór (zbiór fizyczny)	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
CPYTODKT	Docelowy zbiór i ze zbioru	*OBJOPR, *READ	*EXECUTE
	Urządzenie, jeśli w komendzie podano nazwę urządzenia	*OBJOPR, *READ	*EXECUTE
	Oparty na zbiorze fizycznym, jeśli zbiór początkowy jest zbiorem logicznym	*READ	*EXECUTE

Komendy zbiorów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CPYTOIMPF	Źródłowy zbiór	*OBJOPR, *READ	*USE
	Docelowy zbiór (zbiór urządzenia)	*OBJOPR, *READ	*USE
	Docelowy zbiór (zbiór fizyczny)	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Oparty na zbiorze, jeśli zbiór początkowy jest zbiorem logicznym	*READ	*USE
CPYTOSTMF	Zbiór bazy danych lub zbiór składowania	*RX	*X
	Plik strumieniowy, jeśli już istnieje	*W	
	Katalog nadrzędny pliku strumieniowego, jeśli plik strumieniowy nie istnieje	*WX,	
	Przedrostek nazwy ścieżki pliku strumieniowego	*X	
	Tabela konwersji *TBL używana do tłumaczenia danych	*OBJOPR	*X
CPYTOTAP	Docelowy zbiór i 'ze zbioru'	*OBJOPR, *READ	*EXECUTE
	Urządzenie, jeśli podano nazwę urządzenia	*OBJOPR, *READ	*EXECUTE
	Oparty na zbiorze fizycznym, jeśli zbiór początkowy jest zbiorem logicznym	*READ	*EXECUTE
CRTDDMF	Plik DDM: REPLACE(*NO)		*READ, *ADD
	Plik DDM: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Opis urządzenia [7]	*CHANGE	
CRTDKTF	Urządzenie, jeśli podano nazwę urządzenia	*OBJOPR	*EXECUTE
	Zbiór dyskietkowy: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Zbiór dyskietkowy: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD, *EXECUTE
CRTDSPF	Zbiór źródłowy	*USE	*EXECUTE
	Urządzenie, jeśli podano nazwę urządzenia	*OBJOPR	*EXECUTE
	Zbiory podane w słowach kluczowych REF i REFFLD	*OBJOPR	*EXECUTE
	Zbiór ekranowy: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Zbiór ekranowy: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD, *EXECUTE
CRTICFF	Zbiór źródłowy	*USE	*EXECUTE
	Zbiory podane w słowach kluczowych REF i REFFLD	*OBJOPR	*EXECUTE
	Plik ICF: REPLACE(*NO)		*READ, *ADD
	Plik ICF: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTLF	Zbiór źródłowy	*USE	*EXECUTE
	Zbiór podany w słowach kluczowych PFILE lub JFILE, gdy podano zbiór logiczny	*OBJOPR, *OBJMGT lub *OBJALTER	*EXECUTE
	Zbiór podany w słowach kluczowych PFILE lub JFILE, gdy nie podano zbioru logicznego	*OBJOPR	*EXECUTE
	Zbiory podane w słowach kluczowych FORMAT i REFACCPTH	*OBJOPR	*EXECUTE
	Tabele podane w słowie kluczowym ALTSEQ	*OBJOPR	*EXECUTE
	Zbiór logiczny		*EXECUTE, *ADD
	Zbiór, do którego odniesienie znajduje się w parametrze DTAMBRS, gdy zbiór logiczny zawiera klucz	*OBJOPR, *OBJMGT lub *OBJALTER	*EXECUTE
	Zbiór, do którego odniesienie znajduje się w parametrze DTAMBRS, gdy zbiór logiczny nie zawiera klucza	*OBJOPR	*EXECUTE
CRTPF	Zbiór źródłowy	*USE	*EXECUTE
	Zbiory podane w słowach kluczowych FORMAT i REFFLD oraz tabela podana w słowie kluczowym ALTSEQ	*OBJOPR	*EXECUTE
	Zbiór fizyczny		*EXECUTE, *ADD
CRTPRTF	Zbiór źródłowy	*USE	*EXECUTE
	Urządzenie, jeśli podano nazwę urządzenia	*OBJOPR	*EXECUTE
	Zbiory podane w słowach kluczowych REF i REFFLD	*OBJOPR	*EXECUTE
	Zbiór wydruku: Replace(*NO)		*READ, *ADD, *EXECUTE
	Zbiór wydruku: Replace(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD, *EXECUTE
CRTSAVF	Zbiór składowania		*READ, *ADD, *EXECUTE
CRTSRCPF	Źródłowy zbiór fizyczny		*READ, *ADD, *EXECUTE
CRTS36DSPF	Zbiór docelowy, gdy wartością parametru TOMBR nie jest *NONE	*ALL	*CHANGE
	Zbiór źródłowy QS36SRC	*USE	*EXECUTE
	Zbiór ekranowy: REPLACE(*NO)		*READ, *ADD
	Zbiór ekranowy: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Komenda Tworzenie zbioru ekranowego (Create Display File - CRTDSPF)	*OBJOPR	*EXECUTE

Komendy zbiorów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTTAPF	Zbiór taśmowy: REPLACE(*NO)		*READ, *ADD
	Zbiór taśmowy: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Urządzenie, jeśli podano nazwę urządzenia	*OBJOPR	*EXECUTE
DLTF	Zbiór (File)	*OBJOPR, *OBJEXIST	*EXECUTE
DSPCPCST	Zbiór bazy danych, który ma ograniczenie w toku	*OBJOPR, *READ	*EXECUTE
DSPDBR	Zbiór bazy danych	*OBJOPR	*EXECUTE
	Zbiór wyjściowy, jeśli został podany	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
DSPDDMF	Plik DDM	*OBJOPR	
DSPDTA	Zbiór danych	*USE	*EXECUTE
	Program	*USE	*EXECUTE
	Zbiór ekranowy	*USE	*EXECUTE
DSPFD [2]	Zbiór (File)	*OBJOPR	*EXECUTE
	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Zbiór jest zbiorem fizycznym i podano parametr TYPE(*ALL, *MBR lub *MBRLST)	Uprawnienia do danych inne niż *EXECUTE	*EXECUTE
DSPFFD	Zbiór (File)	*OBJOPR	*EXECUTE
	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
DSPPFM	Zbiór fizyczny	*USE	*EXECUTE
DSPSAVF	Zbiór składowania	*USE	*EXECUTE
EDTCPCST	Obszar danych, który podano w słowie kluczowym NFYOBJ dla związanej z nim komendy STRCMTCTL.	*CHANGE	*EXECUTE
	Zbiory, jakie podano w słowie kluczowym NFYOBJ dla związanej z nim komendy STRCMTCTL.	*OBJOPR, *ADD	*EXECUTE
GENCAT	Zbiór bazy danych	*OBJOPR i uprawnienia do danych inne niż *EXECUTE	*EXECUTE
INZPFM	Zbiór fizyczny, gdy podano parametr RECORD(*DFT)	*OBJOPR, *OBJMGT lub *OBJALTER, *ADD	*EXECUTE
	Zbiór fizyczny, gdy podano parametr RECORD(*DLT)	*OBJOPR, *OBJMGT lub *OBJALTER, *ADD, *DLT	*EXECUTE
MRGSRC	Zbiór docelowy	*CHANGE, *OBJMGT	*CHANGE
	Zbiór obsługi	*USE	*EXECUTE
	Zbiór główny	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
OPNDBF	Zbiór bazy danych	*OBJOPR i uprawnienia do danych inne niż *EXECUTE	*EXECUTE
OPNQRYF	Zbiór bazy danych	*OBJOPR i uprawnienia do danych inne niż *EXECUTE	*EXECUTE
PRTTRGPGM [11]			
RGZPFM	Zbiór zawierający podzbiór	*OBJOPR, *OBJMGT lub *OBJALTER, *READ, *ADD, *UPD, *DLT, *EXECUTE	*EXECUTE
RMVICFDEVE	Plik ICF	*OBJOPR, *OBJMGT	*EXECUTE
RMVM	Zbiór zawierający podzbiór	*OBJEXIST, *OBJOPR	*EXECUTE
RMVPFCST	Zbiór (File)	*OBJMGT lub *OBJALTER	*EXECUTE
RMVPFTRG	Zbiór fizyczny	*OBJALTER, *OBJMGT	*EXECUTE
RNMM	Zbiór zawierający podzbiór	*OBJOPR, *OBJMGT	*EXECUTE, *UPD
RSTS36F [4] (Q)	Docelowy zbiór	*ALL	Więcej informacji znajduje się w zasadach ogólnych.
	Źródłowy zbiór	*USE	*EXECUTE
	W oparciu o zbiór fizyczny, jeśli odtwarzany zbiór jest zbiorem logicznym (alternatywnie)	*CHANGE	*EXECUTE
	Opis urządzenia dla dyskietki lub taśmy	*USE	*EXECUTE
RTVMBRD	Zbiór (File)	*USE	*EXECUTE
SAVSAVFDTA	Opis urządzania taśmy, dyskietki i optycznego	*USE	*EXECUTE
	Zbiór składowania	*USE	*EXECUTE
	Zbiór składowania/odtwarzania nośnika optycznego [8] (jeśli wcześniej istniał)	*RW	Nie dotyczy
	Katalog nadrzędny OPTFILE[8]	*WX	Nie dotyczy
	Przedrostek ścieżki OPTFILE[8]	*X	Nie dotyczy
	Katalog główny (/) woluminu optycznego [8, 9]	*RWX	Nie dotyczy
	Wolumin optyczny [10]	*CHANGE	Nie dotyczy
SAVS36F	Źródłowy zbiór	*USE	*EXECUTE
	Zbiór docelowy, gdy jest zbiorem fizycznym	*ALL	Więcej informacji znajduje się w zasadach ogólnych.
	Zbiór urządzenia lub opis urządzenia	*USE	*EXECUTE
SAVS36LIBM	Zbiór docelowy, gdy jest zbiorem fizycznym	*ALL	Więcej informacji znajduje się w zasadach ogólnych.
	Źródłowy zbiór	*USE	*EXECUTE
	Zbiór urządzenia lub opis urządzenia	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
STRAPF [3]	Zbiór źródłowy	*OBJMGT, *CHANGE	*READ, *ADD
	Komendy CRTPF, CRTLF, ADDPFM, ADDLFM i RMVM	*USE	*EXECUTE
STRDFU [3]	Program (jeśli tworzone są opcje programu)		*READ, *ADD
	Program (jeśli opcje są zmieniane lub usuwane)	*OBJEXIST	*READ, *ADD
	Zbiór (jeśli opcje danych są zmieniane lub wyświetlane)	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	Zbiór (jeśli opcje danych są wyświetlane)	*READ	*EXECUTE
UPDDTA	Zbiór (File)	*CHANGE	*EXECUTE
WRKCMTDFN [1]			
WRKDDMF [3]	Plik DDM	*OBJOPR, *OBJMGT, *OBJEXIST	*READ, *ADD
WRKF [3,5]	Zbiory	*OBJOPR	*USE
WRKPFCST[3]			*EXECUTE

1 Komenda CPYFRMQRYF korzysta z parametru FROMOPNID, a nie FROMFILE. Przed uruchomieniem komendy CPYFRMQRYF użytkownik musi mieć wystarczające uprawnienia do wykonania komendy OPNQRYF. Jeśli dla komendy CPYFRMQRYF podano parametr CRTFILE(*YES), przy określaniu uprawnień dla nowego zbioru docelowego, jako zbiór źródłowy pierwszy pod uwagę brany jest zbiór podany w odpowiednim parametrze OPNQRYF FILE.

2 Wymagane jest prawo własności lub uprawnienia do działania na zbiorze.

3 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

4 Jeśli tworzony jest nowy zbiór, a w zbiorze istnieje magazyn uprawnień, użytkownik musi mieć uprawnienia specjalne *ALL do tego magazynu lub być jego właścicielem. Jeśli nie ma magazynu uprawnień, właścicielem zbioru jest użytkownik, który wpisał komendę RSTS36F i ma uprawnienia publiczne *ALL.

5 Wymagane są niektóre uprawnienia do obiektu.

6 Użytkownik musi mieć uprawnienia specjalne *ALLOBJ.

7 Uprawnienia sprawdzane są podczas używania pliku DDM.

8 To sprawdzanie uprawnień przeprowadzane jest jedynie wtedy, kiedy nośnik optyczny jest w formacie UDF (Universal Disk Format).

9 To sprawdzanie uprawnień przeprowadzane jest jedynie wtedy, kiedy nośnik optyczny jest czyszczony.

10 Woluminy optyczne nie są rzeczywistymi obiektami systemowymi. Dowiązanie między woluminem optycznym a listą autoryzacji używaną do ochrony obiektu jest utrzymywane przez funkcję obsługi nośników optycznych.

11 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *ALLOBJ lub *AUDIT.

Komendy filtrów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDALRACNE	Filtr	*USE, *ADD	*EXECUTE
ADDALRSLTE	Filtr	*USE, *ADD	*EXECUTE
ADDPRBACNE	Filtr	*USE, *ADD	*EXECUTE
ADDPRBSLTE	Filtr	*USE, *ADD	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CHGALRACNE	Filtr	*USE, *UPD	*EXECUTE
CHGALRSLTE	Filtr	*USE, *UPD	*EXECUTE
CHGFTR	Filtr	*OBJMGT	*EXECUTE
CHGPRBACNE	Filtr	*USE, *UPD	*EXECUTE
CHGPRBSLTE	Filtr	*USE, *UPD	*EXECUTE
CRTFTR	Filtr		*READ, *ADD
DLTFTR	Filtr	*OBJEXIST	*EXECUTE
RMVFTRACNE	Filtr	*USE, *DLT	*EXECUTE
RMVFTRSLTE	Filtr	*USE, *DLT	*EXECUTE
WRKFTR [1]	Filtr	Dowolne uprawnienia	*EXECUTE
WRKFTRACNE [1]	Filtr	*USE	*EXECUTE
WRKFTRSLTE [1]	Filtr	*USE	*EXECUTE
1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.			

Komendy finansowe

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
SBMFNCJOB (Q)	Opis zadania i kolejka komunikatów [1]	*OBJOPR	*EXECUTE
SNDFNCIMG (Q)	Opis zadania i kolejka komunikatów [1]	*OBJOPR	*EXECUTE
WRKDEVTBL (Q)	Opis urządzenia [1]	Przynajmniej jedno uprawnienie do danych	*EXECUTE
WRKPGMTBL (Q)			
WRKUSRTBL (Q)			
1 To uprawnienie musi mieć profil użytkownika QFNC.			

Operacje graficzne systemu OS/400

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CHGFCNUSG[5]			
DSPFCNUSG			
EDTWSOAUT	Obiekt stacji roboczej [1]	*OBJMGT [2,3,4]	*EXECUTE
GRTWSOAUT	Obiekt stacji roboczej [1]	*OBJMGT [2,3,4]	*EXECUTE
RVKWSOAUT	Obiekt stacji roboczej [1]	*OBJMGT [2,3,4]	*EXECUTE
SETCSTDTA	Profil użytkownika dla kopiowania z	*CHANGE	*EXECUTE
	Profil użytkownika dla kopiowania do	*CHANGE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
WRKFCNUSG			

[1] Obiekt stacji roboczej to obiekt wewnętrzny, który tworzony jest podczas instalowania opcji OS/400 Graphical Operations. Dostarczany jest z uprawnieniami publicznymi *USE.

[2] Użytkownik musi być właścicielem lub mieć uprawnienia *OBJMGT oraz uprawnienia nadawane lub odbierane.

[3] Aby nadać uprawnienia *OBJMGT lub *AUTLMGT, użytkownik musi być właścicielem lub mieć uprawnienia *ALLOBJ.

[4] Aby zabezpieczyć obiekt stacji roboczej za pomocą listy autoryzacji lub ją usunąć, należy:
być właścicielem obiektu stacji roboczej,
mieć uprawnienia *ALL do tego obiektu,
mieć uprawnienie specjalne *ALLOBJ.

[5] Do zmiany użycia funkcji niezbędne jest uprawnienie administratora ochrony (*SECADM).

Komendy zestawu symboli graficznych

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CRTGSS	Zbiór źródłowy	*USE	*EXECUTE
	Zestaw symboli graficznych		*READ, *ADD
DLTGSS	Zestaw symboli graficznych	*OBJEXIST	*EXECUTE
WRKGSS [1]	Zestaw symboli graficznych	*OBJOPR	*USE

[1] Wymagane jest prawo własności lub niektóre uprawnienia do obiektu.

Komendy serwera hosta

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Te komendy nie wymagają uprawnień do obiektu.	
ENDHOSTSVR (Q)	STRHOSTSVR (Q)

Komendy obrazów

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu
ADDIMGCLGE (Q)[1]				
CHGIMGCLG (Q)[1]				
CHGIMGCLGE (Q)[1]				

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu
CRTIMGCLG (Q)[1]				
DLTIMGCLG (Q)[1]				
LODIMGCLG (Q)[1]				
RMVIMGCLGE (Q)[1]				
VFYIMGCLG (Q)[1]				
WRKIMGCLGE (Q)[1]				
[1] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *ALLOBJ i *SECADM.				

Komendy zintegrowanego systemu plików

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
ADDLNK	Obiekt	*STMF	QOpenSys, ″główny″, UDFS	*OBJEXIST
	Dowiązanie nadrzędne do nowego dowiązania	*DIR	QOpenSys, ″główny″, UDFS	*WX
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
CHGATR	Obiekt, gdy ustawiany jest atrybut inny niż *USECOUNT, *ALWCKPWRT, *DISKSTGOPT,*MAINSTGOPT, *ALWSAV, *SCAN, *CRTOBJSCAN, *SETUID, *SETGID, *RSTRDRNMUNL	Dowolne	Wszystkie z wyjątkiem QSYS.LIB	*W
	Obiekt, gdy ustawiany jest atrybut *USECOUNT, *DISKSTGOPT, *MAINSTGOPT, *ALWSAV	Dowolne	Wszystkie z wyjątkiem QSYS.LIB	*OBJMGT
		*FILE	QSYS.LIB	*OBJOPR, *OBJMGT
		*MBR	QSYS.LIB	*X, *OBJMGT (uprawnienia dziedziczone z nadrzędnego atrybutu *FILE)
		pozostałe	QSYS.LIB	*OBJMGT
	Obiekt, gdy ustawiany jest atrybut *ALWCKPWRT	Dowolne	Wszystkie	*OBJMGT
	Katalog który zawiera obiekty, gdy podano parametr SUBTREE(*ALL)	Dowolny katalog	Wszystkie	*RX
	Obiekt, gdy ustawiane są następujące atrybuty: *CRTOBJSCAN lub *SCAN	*DIR i *STMF	QOpenSys, ″główny″, UDFS	Patrz uwaga [26]
	Obiekt, gdy ustawiane są następujące atrybuty: *SETUID, *SETGID, *RSTDRNMUNL	Dowolne	Wszystkie z wyjątkiem QSYS.LIB i QDLS	Prawo własności [15]
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
CHGAUD [4]				
CHGAUT	Obiekt	Wszystkie	QOpenSys, ″główny″, UDFS	Prawo własności [15]
			QSYS.LIB, QOPT[11]	Prawo własności lub *ALLOBJ
			QDLS	Prawo własności, *ALL lub *ALLOBJ
				*OBJMGT
	Wolumin optyczny	*DDIR	QOPT[8]	*CHANGE
CHGCURDIR	Obiekt	Dowolny katalog		*R
	Wolumin optyczny	*DDIR	QOPT[8]	*X
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
CHGOWN	Obiekt	Wszystkie	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		Wszystkie	QOpenSys, ″główny″, UDFS	Prawo własności i *OBJEXIST [15]
		Wszystkie	QDLS	Prawo własności lub *ALLOBJ
			QOPT[11]	Prawo własności lub *ALLOBJ
CHGOWN[24]	Profil użytkownika poprzedniego właściciela — wszystkie z wyjątkiem QOPT, QDLS	*USRPRF	Wszystkie	*DLT
	Profil użytkownika nowego właściciela — wszystkie z wyjątkiem QOPT	*USRPRF	Wszystkie	*ADD
	Wolumin optyczny	*DDIR	QOPT[8]	*CHANGE
CHGPGP	Obiekt	Wszystkie	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		Wszystkie	QOpenSys, ″główny″, UDFS	Prawo własności [5, 15]
		Wszystkie	QDLS	Prawo własności lub *ALLOBJ
			QOPT[11]	Prawo własności lub *ALLOBJ
CHGPGP	Profil użytkownika poprzedniej grupy podstawowej — wszystkie z wyjątkiem QOPT	*USRPRF	Wszystkie	*DLT
	Profil użytkownika nowej grupy podstawowej — wszystkie z wyjątkiem QOPT	*USRPRF	Wszystkie	*ADD
	Wolumin optyczny	*DDIR	QOPT[8]	*CHANGE
CHKIN	Obiekt, jeśli jest to użytkownik, który sprawdzał.	*STMF	QOpenSys, ″główny″, UDFS	*W
		*DOC	QDLS	*W
	Obiekt, jeśli nie jest to użytkownik, który sprawdzał.	*STMF	QOpenSys, ″główny″, UDFS	*ALL lub *ALLOBJ lub prawo własności
		*DOC	QDLS	*ALL lub *ALLOBJ lub prawo własności
	Ścieżka, jeśli nie jest to użytkownik, który sprawdzał.	*DIR	QOpenSys, ″główny″, UDFS	*X
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
CHKOUT	Obiekt	*STMF	QOpenSys, ″główny″, UDFS	*W
		*DOC	QDLS	*W
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
CPY[25]	Kopiowany obiekt, obiekt źródłowy	Dowolne	QOpenSys, ″główny″, UDFS	*R i *OBJMGT lub prawo własności
		*DOC	QDLS	*RWX i *ALL lub prawo własności
		*MBR	QSYS.LIB	Brak
		pozostałe	QSYS.LIB	*RX, *OBJMGT
		*DSTMF	QOPT[11]	*R
	Obiekt docelowy, gdy podano parametr REPLACE(*YES) (jeśli obiekt docelowy już istnieje)	Dowolne	Wszystkie [10]	*W, *OBJEXIST, *OBJMGT
		*DSTMF	QOPT[11]	*W
		*LIB	QSYS.LIB	*RW, *OBJMGT, *OBJEXIST
		*FILE (PF lub LF)	QSYS.LIB	*RW, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*RWX, *ALL
	Kopiowany katalog, który zawiera obiekty, gdy podano parametr SUBTREE(*ALL) w celu skopiowania zawartości	*DIR	QOpenSys, ″główny″, UDFS	*RX, *OBJMGT
CPY[25]	Ścieżka (docelowa), katalog nadrzędny obiektu docelowego	*FILE	QSYS.LIB	*RX, *OBJMGT
		*LIB	QSYS.LIB	*RX, *ADD
		*DIR	QOpenSys, ″główny″, UDFS	*WX
		*FLR	QDLS	*RWX
		*DDIR	QOPT[11]	*WX
	Źródłowy wolumin optyczny	*DDIR	QOPT[8]	*USE
	Docelowy wolumin optyczny	*DDIR	QOPT[8]	*CHANGE

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
CPY[25]	Katalog nadrzędny obiektu źródłowego	*DIR	QOpenSys, ″główny″, UDFS	*X
		*FLR	QDLS	*X
		Pozostałe	QSYS.LIB	*RX
		*DDIR	QOPT[11]	*X
	Przedrostek ścieżki (miejsce docelowe)	*LIB	QSYS.LIB	*WX
		*DIR	QOpenSys, ″główny″, UDFS	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
	Przedrostek ścieżki (obiekt źródłowy)	*DDIR	QOPT[11]	*X
CRTDIR[21, 22]	Katalog nadrzędny	*DIR	QOpenSys, ″główny″, UDFS	*WX
		*FLR	QDLS	*CHANGE
		*FILE	QSYS.LIB	*RX, *ADD
		Dowolne		*ADD
		*DDIR	QOPT[11]	*WX
CRTDIR	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
	Wolumin optyczny	*DDIR	QOPT[8]	*CHANGE
CVTDIR (Q)[16]				
DSPAUT	Obiekt	Wszystkie	QDLS	*ALL
		Wszystkie	Wszystkie pozostałe	*OBJMGT lub prawo własności
		ALL	QOPT[11]	Brak
	Wolumin optyczny	*DDIR	QOPT[8]	*USE
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
DSPCURDIR	Przedrostek ścieżki	*DIR	QOpenSys, ″główny″, UDFS	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*DIR		*R
		*DDIR	QOPT[11]	*RX

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
DSPCURDIR	Katalog bieżący	*DIR	QOpenSys, ″główny″, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DIR		*R
		*DDIR	QOPT[11]	*X
	Wolumin optyczny	*DDIR*	QOPT[8]	*USE
DSPLNK	Dowolne	Dowolne	″główny″, QOpenSys, UDFS QSYS.LIB, QDLS, QOPT[11]	Brak
	Zbiór, opcja 12 (Wyświetl dowiązania)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	″główny″, QOpenSys, UDFS	*R
DSPLNK	Obiekt dowiązania symbolicznego	*SYMLNK	″główny″, QOpenSys, UDFS	Brak
	Wolumin optyczny	*DDIR	QOPT[8]	*USE
	Katalog nadrzędny obiektu odniesienia - brak wzorca [13]	*DIR	″główny″, QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Katalog nadrzędny obiektu odniesienia - podano wzorzec [13]	*DIR	″główny″, QOpenSys, UDFS	*R
		*LIB, *FILE	QSYS.LIB	*R
		*FLR	QDLS	*R
		*DDIR	QOPT[11]	*R
		*DDIR		*R
	Katalog nadrzędny obiektu odniesienia - opcja 8 (Wyświetl atrybuty)	*DIR	″główny″, QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
DSPLNK	Katalog nadrzędny obiektu odniesienia - opcja 12 (Wyświetl dowiązania)	*DIR	″główny″, QOpenSys, UDFS	*RX
		*SYMLNK	″główny″, QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Przedrostek nadrzędnego obiektu odniesienia - brak wzorca [13]	*DIR	″główny″, QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Przedrostek nadrzędnego obiektu odniesienia - podano wzorzec [13]	*DIR	″główny″, QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Przedrostek nadrzędnego obiektu odniesienia - opcja 8 (Wyświetl atrybuty)	*DIR	″główny″, QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Przedrostek nadrzędnego obiektu odniesienia - opcja 12 (Wyświetl dowiązania)	*DIR	″główny″, QOpenSys, UDFS	*RX
		*SYMLNK	″główny″, QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
DSPLNK	Względna nazwa ścieżki [14] : bieżący katalog roboczy zawierający obiekt - brak wzorca [13]	*DIR	″główny″, QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Względna nazwa ścieżki [14] : bieżący katalog roboczy zawierający obiekt - podano wzorzec [13]	*DIR	″główny″, QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
DSPLNK	Względna nazwa ścieżki [14] : przedrostek bieżącego katalogu roboczego zawierającego obiekt - brak wzorca [13]	*DIR	″główny″, QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
DSPLNK	Względna nazwa ścieżki [14] : przedrostek bieżącego katalogu roboczego zawierającego obiekt - podano wzorzec [13]	*DIR	″główny″, QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
DSPMFSINF	Obiekt	Dowolne	Dowolne	Brak
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
ENDJRN	Obiekt	*DIR jeśli parametr Subtree (*ALL)	QOpenSys, ″główny″, UDFS	*R, *X, *OBJMGT
		*DIR jeśli parametr Subtree (*NONE), *SYMLNK, *STMF	QOpenSys, ″główny″, UDFS	*R, *OBJMGT
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT
	Katalog nadrzędny	*DIR	QOpenSys, ″główny″, UDFS	*X
		*LIB	QSYS.LIB	*X
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
	Kronika			*OBJMGT, *OBJOPR
MOV[19]	Obiekt przeniesiony w obrębie tego samego systemu plików	*DIR	QOpenSys, ″główny″	*OBJMGT, *W
		Nie *DIR	QOpenSys, ″główny″	*OBJMGT
		*DOC	QDLS	*ALL
		*FILE	QSYS.LIB	*OBJOPR, *OBJMGT
		*MBR	QSYS.LIB	Brak
		pozostałe	QSYS.LIB	Brak
		*STMF	QOPT[11]	*W
MOV	Ścieżka (źródłowa), katalog nadrzędny	*DIR	QOpenSys, ″główny″, UDFS	*WX
		*FLR	QDLS	*RWX
		*FILE	QSYS.LIB, ″główny″	*RX, *OBJEXIST
		pozostałe	QOpenSys, ″główny″	*RWX
	Ścieżka (docelowa), katalog nadrzędny	*DIR	QSYS.LIB	*WX
		*FLR	QDLS	*CHANGE (*RWX)
		*FILE	QSYS.LIB	*X, *ADD, *DLT, *OBJMGT
		*LIB	QSYS.LIB	*RWX
		*DDIR	QOPT[11]	*WX

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
MOV	Przedrostek ścieżki (docelowej)	*LIB	QSYS.LIB	*X, *ADD
		*FLR	QDLS	*X
		*DIR	pozostałe	*X
		*DDIR	QOPT[11]	*X
	Obiekt przeniesiony poprzez systemy plików do systemu QOpenSys, głównego lub QDLS (plik strumieniowy *STMF i tylko *DOC, *MBR).	*STMF	QOpenSys, ″główny″, UDFS	*R, *OBJEXIST, *OBJMGT
		*DOC	QDLS	*ALL
		*MBR	QSYS.LIB	Nie dotyczy
		*DSTMF	QOPT[11]	*RW
MOV	Przeniesiony do systemu QSYS, *MBR	*STMF	QOpenSys, ″główny″, UDFS	*R, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*ALL
		*DSTMF	QOPT[11]	*RW
MOV	Ścieżka (źródłowa), przeniesiony poprzez systemy plików, katalog nadrzędny	*DIR	QOpenSys, ″główny″, UDFS	*WX
		*FLR	QDLS	*X
		*FILE	QSYS. LIB	prawo własności, *RX, *OBJEXIST
		*DDIR	QOPT[11]	*WX
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
	Wolumin optyczny (źródłowy i docelowy)	*DDIR	QOPT[8]	*CHANGE
RLSIFSLCK [18]	*dowolny_stmf*	*STMF	″główny″, QOpenSys, UDFS	*R
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
RMVDIR[19,20]	Katalog	*DIR	QOpenSys, ″główny″, UDFS	*OBJEXIST
		*LIB	QSYS.LIB	*RX, *OBJEXIST
		*FILE	QSYS.LIB	*OBJOPR, *OBJEXIST
		*FLR	QDLS	*ALL
		*DDIR	QOPT[11]	*W

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
RMVDIR	Katalog nadrzędny	*DIR	QOpenSys, ″główny″, UDFS	*WX
		*FLR	QDLS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*DDIR	QOPT[11]	*WX
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
	Wolumin optyczny	*DDIR	QOPT[8]	*CHANGE
RMVLNK[19]	Obiekt	*DOC	QDLS	*ALL
		*MBR	QSYS.LIB	
		*FILE	QSYS.LIB	*OBJOPR, *OBJEXIST
		*JRNRCV	QSYS.LIB	*OBJEXIST, *R
		pozostałe	QSYS.LIB	*OBJEXIST
		*DSTMF	QOPT[11]	*W
		dowolne	QOpenSys, ″główny″, UDFS	*OBJEXIST
RMVLNK	Katalog nadrzędny	*FLR	QDLS	*X
		*FILE	QSYS.LIB	*X, *OBJEXIST
		*LIB	QSYS.LIB	*X
		*DIR	QOpenSys, ″główny″, UDFS	*WX
		*DDIR	QOPT[11]	*WX
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
	Wolumin optyczny	*DDIR	QOPT[8]	*CHANGE
RNM[19]	Obiekt	*DIR	QOpenSys, ″główny″, UDFS	*OBJMGT, *W
		Nie *DIR	QOpenSys, ″główny″, UDFS	*OBJMGT
		*DOC, *FLR	QDLS	*ALL
		*MBR	QSYS.LIB	Nie dotyczy
		*FILE	QSYS.LIB	*OBJMGT, *OBJOPR
		pozostałe	QSYS.LIB	*OBJMGT
		*DSTMF	QOPT[11]	*W
	Wolumin optyczny (źródłowy i docelowy)	*DDIR	QOPT[8]	*CHANGE

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
RNM	Katalog nadrzędny	*DIR	QOpenSys, ″główny″, UDFS	*WX
		*FLR	QDLS	*CHANGE (*RWX)
		*FILE	QSYS.LIB	*X, *OBJMGT
		*LIB	QSYS.LIB	*X, *UPD
		*DDIR	QOPT[11]	*WX
	Przedrostek ścieżki	*LIB	QSYS.LIB	*X, *UPD
		Dowolne	QOpenSys, ″główny″, UDFS, QDLS	*X
RST (Q) [23]	Obiekt, jeśli istnieje [2]	Dowolne	QOpenSys, ″główny″, UDFS	*W, *OBJEXIST
			QSYS.LIB	Zależności [10]
			QDLS	*ALL
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
RST (Q)	Katalog nadrzędny odtwarzanego obiektu [2]	*DIR	QOpenSys, ″główny″, UDFS	*WX
	Katalog nadrzędny odtwarzanego obiektu, jeśli obiekt nie istnieje [2]	*FLR	QDLS	*CHANGE
		*DIR		*OBJMGT, *OBJALTER, *READ, *ADD, *UPD
	Profil użytkownika będący właścicielem odtwarzanego obiektu [2]	*USRPRF	QSYS.LIB	*ADD
	Jednostka taśm, jednostka dyskietek, jednostka optyczna lub zbiór składowania	*DEVD, *FILE	QSYS.LIB	*RX
RST (Q)	Biblioteka dla opisu urządzenia lub zbioru składowania	*LIB	QSYS.LIB	*EXECUTE
	Zbiór wyjściowy, jeśli został podany	*STMF	QOpenSys, ″główny″, UDFS	*W
		*USRSPC	QSYS.LIB	*RWX
	Przedrostek ścieżki zbioru wyjściowego	*DIR	QOpenSys, ″główny″, UDFS	*X
		*LIB	QSYS.LIB	*RX

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
RST (Q)	Wolumin optyczny, jeśli odtwarzanie odbywa się z urządzenia optycznego	*DDIR	QOPT[8]	*USE
	Przedrostek ścieżki nośnika optycznego i katalogu nadrzędnego, jeśli odtwarzanie odbywa się z urządzenia optycznego	*DDIR	QOPT[11]	*X
	Zbiór nośnika optycznego, jeśli odtwarzanie odbywa się z urządzenia optycznego	*DSTMF	QOPT[11]	*R
RTVCURDIR	Przedrostek ścieżki	*DIR	QOpenSys, ″główny″, UDFS, QDLS, QOPT[11]	*RX
		*DDIR	QOPT[11]	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		Dowolne		*R
RTVCURDIR	Katalog bieżący	*DIR	QOpenSys, ″główny″, UDFS, QOPT [11]	*X
		*DDIR	QOPT[11]	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		Dowolne		*R
SAV	Obiekt [2]	Dowolne	QOpenSys, ″główny″, UDFS	*R, *OBJEXIST
			QSYS.LIB	Zależności [10]
			QDLS	*ALL
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
	Jednostka taśm, jednostka dyskietek lub jednostka optyczna	*DEVD	QSYS.LIB	*RX
SAV	Zbiór składowania, jeśli jest pusty	*FILE	QSYS.LIB	*USE, *ADD
	Zbiór składowania, jeśli nie jest pusty	*FILE	QSYS.LIB	*OBJMGT, *USE, *ADD
	Kolejka komunikatów składowania podczas użycia	*MSGQ	QSYS.LIB	*OBJOPR, *ADD
	Biblioteki opisu urządzenia, zbioru składowania, kolejki komunikatów składowania podczas użycia	*LIB	QSYS.LIB	*EXECUTE

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
SAV	Zbiór wyjściowy, jeśli został podany	*STMF	QOpenSys, ″główny″, UDFS	*W
		*USRSPC	QSYS.LIB	*RWX
	Przedrostek ścieżki zbioru wyjściowego	*DIR	QOpenSys, ″główny″, UDFS	*X
		*LIB	QSYS.LIB	*RX
SAV	Wolumin optyczny, jeśli składowanie odbywa się do urządzenia optycznego	*DDIR	QOPT[8]	*CHANGE
	Przedrostek ścieżki nośnika optycznego, jeśli składowanie odbywa się na urządzenie optyczne	*DDIR	QOPT[11]	*X
	Katalog nadrzędny nośnika optycznego, jeśli składowanie odbywa się na urządzenie optyczne	*DDIR	QOPT[11]	*WX
	Zbiór nośnika optycznego (jeśli istnieje)	*DSTMF	QOPT[11]	*RW
SAVRST	W systemie źródłowym są to takie same uprawnienia, jak wymagane dla komendy SAV.			
	W systemie docelowym są to takie same uprawnienia, jak wymagane dla komendy RST.			
STATFS	Obiekt	Dowolne	Dowolne	Brak
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
STRJRN	Obiekt	*DIR jeśli parametr Subtree (*ALL)	QOpenSys, ″główny″, UDFS	*R, *X, *OBJMGT
		*DIR jeśli parametr Subtree (*NONE), *SYMLNK, *STMF	QOpenSys, ″główny″, UDFS	*R, *OBJMGT
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT
	Katalog nadrzędny	*DIR	QOpenSys, ″główny″, UDFS	*X
		*LIB	QSYS.LIB	*X
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
	Kronika	*JRN		*OBJMGT, *OBJOPR
WRKAUT[6, 7]	Obiekt	*DOC lub *FLR	QDLS	*ALL
		Wszystkie	Nie QDLS	*OBJMGT lub prawo własności
		*DDIR i *DSTMF	QOPT[11]	*NONE
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
	Wolumin optyczny	*DDIR	QOPT[8]	*USE

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
WRKLNK	Dowolne	Dowolne	″główny″, QOpenSys, UDFS, QSYS.LIB, QDLS, QOPT[11]	Brak
	Zbiór, opcja 12 (Wyświetl dowiązania)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	″główny″, QOpenSys, UDFS	*R
	Obiekt dowiązania symbolicznego	*SYMLNK	″główny″, QOpenSys, UDFS	Brak
	Wolumin optyczny	*DDIR	QOPT[8]	*USE
WRKLNK	Katalog nadrzędny obiektu odniesienia - brak wzorca [13]	*DIR	″główny″, QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Katalog nadrzędny obiektu odniesienia - podano wzorzec	*DIR	″główny″, QOpenSys, UDFS	*R
		*LIB *FILE	QSYS.LIB	*R
		*FLR	QDLS	*R
		*DDIR	QOPT[11]	*R
		*DDIR		*R
WRKLNK	Katalog nadrzędny obiektu odniesienia - opcja 8 (Wyświetl atrybuty)	*DIR	″główny″, QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Katalog nadrzędny obiektu odniesienia - opcja 12 (Wyświetl dowiązania)	*DIR	″główny″, QOpenSys, UDFS	*RX
		*SYMLNK	″główny″, QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
WRKLNK	Przedrostek nadrzędnego obiektu odniesienia - brak wzorca [13]	*DIR	″główny″, QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Przedrostek nadrzędnego obiektu odniesienia - podano wzorzec [13]	*DIR	″główny″, QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Przedrostek nadrzędnego obiektu odniesienia - opcja 8 (Wyświetl atrybuty)	*DIR	″główny″, QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Przedrostek nadrzędnego obiektu odniesienia - opcja 12 (Wyświetl dowiązania)	*DIR	″główny″, QOpenSys, UDFS	*RX
		*SYMLNK	″główny″, QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
WRKLNK	Względna nazwa ścieżki [14] : bieżący katalog roboczy zawierający obiekt - brak wzorca [13]	*DIR	″główny″, QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Względna nazwa ścieżki [14] : bieżący katalog roboczy zawierający obiekt - podano wzorzec [13]	*DIR	″główny″, QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
WRKLNK	Względna nazwa ścieżki [14] : przedrostek bieżącego katalogu roboczego zawierającego obiekt - brak wzorca [13]	*DIR	″główny″, QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Względna nazwa ścieżki [14] przedrostek bieżącego katalogu roboczego zawierającego obiekt - podano wzorzec [13]	*DIR	″główny″, QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R

1 Uprawnienie adoptowane nie jest używane dla komend zintegrowanego systemu plików.

2 Jeśli użytkownik ma uprawnienie specjalne *SAVSYS, nie musi mieć uprawnień dla systemów plików QSYS.LIB, QDLS, QOpenSys i ″główny″.

3 Wymagane uprawnienia zależą do typu obiektu. Patrz opis funkcji API QLIRNMO w Centrum informacyjne. Jeśli obiekt jest podzbiorem bazy danych, należy zapoznać się z uprawnieniami do komendy Zmiana nazwy podzbioru (Rename Member - RNMM).

4 Aby zmienić wartość kontroli, użytkownik musi mieć uprawnienia specjalne *AUDIT.

5 Jeśli użytkownik wywołujący komendę nie ma uprawnień *ALLOBJ, to musi być członkiem nowej grupy podstawowej.

6 Ta komenda nie jest obsługiwana dla systemu plików QLANSrv.

7 Te komendy wymagają przedstawionych uprawnień oraz uprawnień wymaganych przez komendę DSPCURDIR.

8 Woluminy optyczne nie są rzeczywistymi obiektami systemowymi. Dowiązanie między woluminem optycznym a listą autoryzacji używaną do ochrony obiektu jest utrzymywane przez funkcję obsługi nośników optycznych.

Komendy zintegrowanego systemu plików

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu[1]
[9] Informacje dotyczące ograniczeń używania tej komendy znajdują się w rozdziale 7 podręcznika iSeries Optical Support. [10] Wymagane uprawnienia zmieniają się w zależności od użytej rodzimej komendy. W celu sprawdzenia wymaganych uprawnień, należy sprawdzić odpowiednie komendy SAVOBJ lub RSTOBJ. [11] Uprawnienia wymagane przez system QOPT do nośnika formatowanego w systemie UDF (Universal Disk Format). [12] *ADD wymagane jest tylko wtedy, gdy przenoszony obiekt jest obiektem typu *MRB. [13] Wzorzec: w niektórych komendach gwiazdka (*) lub znak zapytania (?) może być użyty w ostatnim komponencie nazwy ścieżki w celu wyszukania nazw pasujących do wzorca.				
[14] Względna nazwa ścieżki: jeśli nazwa ścieżki nie zaczyna się od ukośnika, zakłada się, że poprzednikiem pierwszego komponentu nazwy ścieżki jest bieżący katalog roboczy procesu. Na przykład, jeśli podano nazwę ścieżki 'a/b', a bieżącym katalogiem roboczym jest katalog '/home/john', wtedy obiekt, do którego ma być uzyskany dostęp, to '/home/john/a/b'. [15] Jeśli użytkownik ma uprawnienia specjalne *ALLOBJ, nie potrzebuje podanych tu uprawnień. [16] Do użycia tej komendy konieczne jest uprawnienie specjalne (*ALLOBJ). [17] W powyższej tabeli biblioteka QSYS.LIB odwołuje się do systemów plików QSYS.LIB niezależnej ASP oraz do systemu plików QSYS.LIB. [18] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG. [19] Jeśli dla katalogu podano atrybut ograniczający zmianę nazwy oraz usuwanie dowiązania (znany także jako bit S_ISVTX), ogranicza on także usuwanie dowiązań obiektów z tego katalogu, chyba że spełnione są następujące warunki: użytkownik ma uprawnienie *ALLOBJ, użytkownik jest właścicielem odłączanego obiektu lub jest właścicielem katalogu. [20] Jeśli podano wartość RMVLNK (*YES), użytkownik musi mieć także uprawnienia *OBJEXIST do wszystkich obiektów w podanym katalogu. [21] Jeśli dla parametru CRTOBJAUD podano wartość inną niż *SYSVAL, to dla systemów plików QSYS.LIB, 'głównego', QOpenSys i systemu plików użytkownika (UDFS) wymagane są uprawnienia specjalne *AUDIT. [22] Aby podać wartość dla parametru Opcja skanowania dla obiektów (Scanning option for objects - CRTOBJSCAN) inną niż *PARENT, użytkownik musi mieć uprawnienia specjalne do wszystkich obiektów (*ALLOBJ) i uprawnienie administratora ochrony (*SECADM). [23] Aby dla parametru ALWOBJDIF określić wartość inną niż *NONE, niezbędne jest uprawnienie specjalne *ALLOBJ. [24] Użytkownik musi mieć uprawnienia specjalne do wszystkich obiektów (*ALLOBJ) i administratora ochrony (*SECADM), aby zmienić właściciela pliku strumieniowego (*STMF) z dołączonym programem Java, po uruchomieniu którego są sprawdzane uprawnienia użytkownika i właściciela. [25] Użytkownik musi mieć uprawnienia specjalne do wszystkich obiektów (*ALLOBJ) i administratora ochrony (*SECADM), aby skopiować plik strumieniowy (*STMF) z dołączonym programem Java, w przypadku którego są sprawdzane uprawnienia użytkownika i właściciela. [26] Aby określić atrybuty *CRTOBJSCAN i *SCAN, użytkownik musi mieć uprawnienia do wszystkich obiektów (*ALLOBJ) i administratora ochrony (*SECADM).				

Komendy IDD

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ADDDTADFN	Słownik danych	*CHANGE	*EXECUTE
	Zbiór (File)	*OBJOPR, *OBJMGT	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CRTDTADCT	Słownik danych		*READ, *ADD
DLTDTADCT [3]	Słownik danych	OBJEXIST, *USE	
DSPDTADCT	Słownik danych	*USE	*EXECUTE
LNKDTADFN [1]	Słownik danych	*USE	*EXECUTE
	Zbiór (File)	*OBJOPR, *OBJMGT	*EXECUTE
STRIDD			
WRKDTADCT [2]	Słownik danych	*OBJOPR	*EXECUTE
WRKDBFIDD [2]	Słownik danych	*USE [4]	*EXECUTE
	Zbiór bazy danych	*OBJOPR	*EXECUTE
WRKDTADFN [1]	Słownik danych	*USE, *CHANGE	*EXECUTE

1 Aby usunąć dowiązanie zbioru, nie są wymagane uprawnienia do słownika danych.

2 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

3 Przed usunięciem słownika usuwane są dowiązania wszystkich zbiorów. Informacje na temat uprawnień wymaganych do usuwania dowiązań zbiorów zawiera sekcja dotycząca komendy LNKDTADFN.

4 Aby utworzyć nowy zbiór, wymagane są uprawnienia do słownika danych. Aby wprowadzać dane do istniejącego zbioru, nie są wymagane żadne uprawnienia.

Komendy IPX

Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
DLTIPXD	Opis IPX	*OBJEXIST	*EXECUTE
DSPIPXD	Opis IPX	*USE	*EXECUTE
WRKIPXD	Opis IPX	*OBJOPR	*EXECUTE

Komendy indeksu wyszukiwania informacji

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ADDSCHIDXE	Indeks wyszukiwania	*CHANGE	*USE
	Panel grupowy	*USE	*EXECUTE
CHGSCHIDX	Indeks wyszukiwania	*CHANGE	*USE
CRTSCHIDX	Indeks wyszukiwania		*READ, *ADD
DLTSCHIDX	Indeks wyszukiwania	*OBJEXIST	*EXECUTE
RMVSCHIDXE	Indeks wyszukiwania	*CHANGE	*USE
STRSCHIDX	Indeks wyszukiwania	*USE	*EXECUTE
WRKSCHIDX [1]	Indeks wyszukiwania	*ANY	*USE
WRKSCHIDXE	Indeks wyszukiwania	*USE	*USE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
[1] Ta komenda nie jest obsługiwana dla systemu plików QLANSrv.			

Komendy atrybutów IPL

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Te komendy nie wymagają uprawnień do obiektów:
CHGIPLA (Q) [1] DSPIPLA
[1] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *SECADM i *ALLOBJ.

Komendy języka Java

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ANZJVM	Komenda QSYS/STRSRVJOB	*USE	
	Komenda QSYS/STRDBG	*USE	

Komendy zadań

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
BCHJOB	Opis zadania [9,11]	*USE	*EXECUTE
	Biblioteki na liście bibliotek (systemowa, bieżąca i użytkownika)[7]	*USE	
	Profil użytkownika w opisie zadania [10]	*USE	
	Tabela kolejności sortowania [7]	*USE	*EXECUTE
	Kolejka komunikatów [10]	*USE, *ADD	*EXECUTE
	Kolejka zadań [10,11]	*USE	*EXECUTE
	Kolejka wyjściowa [7]	*READ	*EXECUTE
CHGACGCDE [1]			
CHGGRPA [4]	Kolejka komunikatów, jeśli następuje powiązanie kolejki komunikatów z grupą	*OBJOPR	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CHGJOB [1,2,3]	Nowa kolejka zadania, jeśli zmieniana jest kolejka zadania [10,11]	*USE	*EXECUTE
	Nowa kolejka wyjściowa, jeśli zmieniana jest kolejka wyjściowa [7]	*READ	*EXECUTE
	Bieżąca kolejka wyjściowa, jeśli zmieniana jest kolejka wyjściowa [7]	*READ	*EXECUTE
	Tabela kolejności sortowania [7]	*USE	*EXECUTE
CHGPJ	Profil użytkownika dla żądania uruchomienia programu określający parametr *PGMSTRRQS	*USE	*EXECUTE
	Profil użytkownika i opis zadania	*USE	*EXECUTE
CHGSYSJOB(Q) [13]			
CHGUSRTRC[14]	Bufor śledzenia użytkownika, jeśli używany jest parametr CLEAR (*YES).[15]	*OBJOPR	*EXECUTE
	Bufor śledzenia użytkownika, gdy używany jest parametr MAXSTG [15]	*CHANGE, *OBJMGT	*USE
	Bufor śledzenia użytkownika, gdy używany jest parametr TRCFULL. [15]	*OBJOPR	*EXECUTE
DLTUSRTRC	Bufor śledzenia użytkownika [15]	*OBJOPR, *OBJEXIST	*EXECUTE
DLYJOB [4]			
DMPUSRTRC	Bufor śledzenia użytkownika [15]	*OBJOPR	*EXECUTE
DSCJOB [1]			
DSPACTPJ			
DSPJOB [1]			
DSPJOBTBL			
DSPJOBLOG [1,5]	Zbiór wyjściowy i podzbiór istnieją	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Podzbiór nie istnieje	*OBJOPR, *OBJMGT, *ADD	*EXECUTE, *ADD
	Zbiór wyjściowy nie istnieje	*OBJOPR	*EXECUTE, *ADD
ENDGRPJOB			
ENDJOB [1]			
ENDJOBABN [1]			
ENDPJ [6]			
HLDJOB [1]			
RLSJOB [1]			
RRTJOB			
RTVJOBA			
SBMDBJOB	Zbiór bazy danych	*USE	*EXECUTE
	Kolejka zadań	*READ	*EXECUTE
SBMDKTJOB	Kolejka komunikatów	*USE, *ADD	*EXECUTE
	Kolejka zadań i opis urządzenia	*READ	*EXECUTE

Komendy zadań

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
SBMJOB [2, 12]	Opis zadania [9,11]	*USE	*EXECUTE
	Biblioteki na liście bibliotek (systemowa, bieżąca i użytkownika)[7]	*USE	
	Kolejka komunikatów [10]	*USE, *ADD	*EXECUTE
	Profil użytkownika [10,11]	*USE	
	Profil użytkownika w opisie zadania [10]	*USE (na poziomie 40)	
	Kolejka zadań [10,11]	*USE	*EXECUTE
	Kolejka wyjściowa [7]	*READ	*EXECUTE
	Tabela kolejności sortowania [7]	*USE	*EXECUTE
	Urządzenia ASP w początkowej grupie ASP	*USE	
SBMNETJOB	Zbiór bazy danych	*USE	*EXECUTE
STRPJ [6]	Opis podsystemu	*USE	
	Program		*EXECUTE
TFRBCHJOB	Kolejka zadań	*READ	*EXECUTE
TFRGRPJOB	Pierwszy program grupy	*USE	*EXECUTE
TFRJOB [8]	Kolejka zadań	*USE	*EXECUTE
	Opis podsystemu, do którego przydzielana jest kolejka zadań	*USE	
TFRSECJOB			
WRKACTJOB			
WRKJOB [1]			
WRKSBMJOB			
WRKSBSJOB			
WRKUSRJOB			

1 Każdy użytkownik może uruchamiać te komendy dla zadań uruchomionych w jego własnym profilu użytkownika. Użytkownik z uprawnieniami specjalnymi do sterowania zadaniem (*JOBCTL) może uruchamiać te komendy dla dowolnych zadań. Jeśli użytkownik ma uprawnienia specjalne *SPLCTL, nie potrzebuje żadnych uprawnień do kolejki zadań. Jednak musi mieć uprawnienia do biblioteki, która zawiera kolejkę zadań.

2 Użytkownik musi mieć uprawnienia (podane w profilu użytkownika) do podanego priorytetu harmonogramu oraz priorytetu wyjścia.

3 Aby zmienić pewne atrybuty zadania, nawet we własnym zadaniu użytkownika, wymagane są uprawnienia specjalne do sterowania zadaniem (*JOBCTL). Dotyczy to atrybutów RUNPTY, TIMESLICE, PURGE, DFTWAIT i TSEPOOL.

4 Ta komenda wpływa tylko na zadanie, dla którego została podana.

5 Aby wyświetlić protokół zadania dla zadania, które ma uprawnienie specjalne *ALLOBJ, użytkownik musi mieć to uprawnienie lub uprawnienie do wykonywania funkcji All Object Job Log (Protokół zadania dla wszystkich obiektów) systemu OS/400 poprzez funkcję Administrowanie aplikacjami programu iSeries Navigator. Komenda Zmiana użycia funkcji (Change Function Usage - CHGFCNUSG), o identyfikatorze QIBM_ACCESS_ALLOBJ_JOBLOG, także może być stosowana do zmiany listy użytkowników, którzy mogą wyświetlać protokół zadania dla zadania z uprawnieniami specjalnymi *ALLOBJ.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
[6] Aby użyć tej komendy, wymagane są uprawnienia specjalne *JOBCTL. [7] Uprawnienia do obiektu odniesienia sprawdzane są dla profilu użytkownika, który wprowadził zadanie. Uprawnienia adoptowane użytkownika wprowadzającego lub zmieniającego zadanie nie są brane pod uwagę. [8] Jeśli przesyłane zadanie jest zadaniem interaktywnym, stosowane są następujące ograniczenia: • kolejka zadań, w której znajduje się zadanie, musi być powiązana z aktywnym podsystemem, • Stacja robocza powiązana z zadaniem musi mieć w opisie podsystemu powiązanym z nowym podsystemem odpowiednią pozycję stacji roboczej. • Ze stacją roboczą powiązaną z zadaniem nie może być powiązane inne zadanie, które zostało zawieszone za pomocą klawisza Sys Req (System Request). Przed uruchomieniem komendy Transfer Zadania (Transfer Job) zawieszone zadanie musi być anulowane, • zadanie nie może być zadaniem grupowym. [9] Sprawdzanie uprawnień do obiektu odniesienia odbywa się zarówno dla użytkownika wprowadzającego zadanie, jak i dla profilu użytkownika, dla którego będzie uruchomione zadanie. [10] Uprawnienia do obiektu odniesienia sprawdzane są dla użytkownika, który wprowadził zadanie.			
[11] Używane są uprawnienia adoptowane użytkownika wywołującego komendę CHGJOB lub SBMJOB. [12] Użytkownik musi być uprawniony do korzystania z profilu użytkownika i opisu zadania; profil użytkownika także musi być uprawniony do korzystania z opisu zadania. [13] Aby zmienić pewne atrybuty zadania, nawet we własnym zadaniu użytkownika, wymagane są uprawnienia specjalne do sterowania zadaniem (*JOBCTL)i do wszystkich obiektów (*ALLOBJ). [14] Każdy użytkownik może uruchamiać te komendy dla zadań uruchomionych w jego własnym profilu użytkownika. Użytkownik z uprawnieniami specjalnymi sterowania zadaniem (*JOBCTL) może uruchamiać te komendy dla dowolnych zadań. [15] Bufor śledzenia użytkownika jest obktem przestrzeni użytkownika (*USRSPC) w bibliotece QUSRSYS o nazwie QPOZ*nnnnnn*, gdzie '*nnnnnn*' jest numerem zadania używającego funkcji śledzenia użytkownika.			

Komendy opisu zadań

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGJOBD	Opis zadania	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Profil użytkownika (USER)	*USE	*EXECUTE
CPYAUDJRNE[8]	Zbiór wyjściowy już istnieje	*OBJOPR *OBJMGT *ADD *DLT	*EXECUTE
	Zbiór wyjściowy nie istnieje		*EXECUTE *ADD
CRTJOBD (Q)	Opis zadania		*READ, *ADD
	Profil użytkownika (USER)	*USE	*EXECUTE
DLTJOBD	Opis zadania	*OBJEXIST	*EXECUTE
DSPJOBD	Opis zadania	*OBJOPR, *READ	*EXECUTE
PRTJOBDAUT [1]			

Komendy opisu zadań

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
WRKJOBD	Opis zadania	Dowolne	*USE

[1] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *ALLOBJ lub *AUDIT.

Komendy kolejek zadań

Komenda	Obiekt odniesienia	Parametry kolejki zadań [4]		Uprawnienie specjalne	Wymagane uprawnienie	
		AUTCHK	**OPRCTL**		**Do obiektu**	**Do biblioteki**
CLRJOBQ [1]	Kolejka zadań	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CRTJOBQ [1]	Kolejka zadań					*READ, *ADD
DLTJOBQ	Kolejka zadań				*OBJEXIST	*EXECUTE
HLDJOBQ [1]	Kolejka zadań	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
PRTQAUT [5]						
RLSJOBQ [1]	Kolejka zadań	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKJOBQ [1,3]	Kolejka zadań	*DTAAUT			*READ	*EXECUTE
		*OWNER			Właściciel [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE

[1] Jeśli użytkownik ma uprawnienia specjalne *SPLCTL, to nie potrzebuje żadnych uprawnień do kolejki zadań, ale musi mieć uprawnienia do biblioteki zawierającej kolejkę zadań.

[2] Użytkownik musi być właścicielem kolejki zadań.

[3] Jeśli użytkownik zgłasza żądanie pracy z wszystkimi kolejkami zadań, wyświetlana lista obejmuje wszystkie kolejki zadań znajdujące się w bibliotece, do których użytkownik ma uprawnienia *EXECUTE.

[4] Aby wyświetlić parametry kolejki zadań, należy użyć funkcji API QSPRJOBQ.

[5] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *ALLOBJ lub *AUDIT.

Komendy harmonogramu zadań

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDJOBSCDE	Harmonogram zadań	*CHANGE	*EXECUTE
	Opis zadania [1]	*USE	*EXECUTE
	Kolejka zadań [1,2]	*READ	*EXECUTE
	Profil użytkownika	*USE	*EXECUTE
	Kolejka komunikatów [1]	*USE, *ADD	*EXECUTE
CHGJOBSCDE [3]	Harmonogram zadań	*CHANGE	*EXECUTE
	Opis zadania [1]	*USE	*EXECUTE
	Kolejka zadań [1,2]	*READ	*EXECUTE
	Profil użytkownika	*USE	*EXECUTE
	Kolejka komunikatów [1]	*USE, *ADD	*EXECUTE
HLDJOBSCDE [3]	Harmonogram zadań	*CHANGE	*EXECUTE
RLSJOBSCDE [3]	Harmonogram zadań	*CHANGE	*EXECUTE
RMVJOBSCDE [3]	Harmonogram zadań	*CHANGE	*EXECUTE
WRKJOBSCDE [4]	Harmonogram zadań	*USE	*EXECUTE

1 Sprawdzanie uprawnień do obiektu odniesienia odbywa się zarówno dla profilu użytkownika dodającego pozycję, jak i dla profilu użytkownika, dla którego uruchomione jest zadanie.

2 Uprawnienia do kolejki zadań nie mogą być uprawnieniami adoptowanymi.

3 Użytkownik musi mieć uprawnienia specjalne *JOBCTL lub musi być użytkownikiem, który dodał pozycję.

4 Aby wyświetlić szczegóły pozycji (opcja 5 lub format wydruku *FULL), użytkownik musi mieć uprawnienia specjalne *JOBCTL lub być użytkownikiem, który dodał pozycję.

Komendy kroniki

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do obiektu lub katalogu**
ADDRMTJRN	Kronika źródłowa	*CHANGE, *OBJMGT	*EXECUTE
	Kronika docelowa		*EXEC, *ADD
APYJRNCHG (Q)	Kronika	*USE	*EXECUTE
	Dziennik	*USE	*EXECUTE
	Obiekty niezintegrowanego systemu plików, których kronikowane zmiany są stosowane.	*OBJMGT, *CHANGE, *OBJEXIST	*EXECUTE, *ADD
	Obiekty zintegrowanego systemu plików, których kronikowane zmiany są stosowane.	*RW, *OBJMGT	*RX (jeśli poddrzewo *ALL)

Komendy kronik

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do obiektu lub katalogu**
APYJRNCHGX	Kronika	*USE	
	Dziennik	*USE	
	Zbiór (File)	*OBJMGT, *CHANGE, *OBJEXIST'	*EXECUTE, *ADD
CHGJRN (Q)	Dziennik, jeśli podano	*OBJMGT, *USE	*EXECUTE
	Podłączony dziennik	*OBJMGT, *USE	*EXECUTE
	Kronika	*OBJOPR, *OBJMGT, *UPD	*EXECUTE
	Kronika, jeśli podano RCVSIZOPT(*MINFIXLEN).	*OBJOPR, *OBJMGT, *UPD, *OBJALTER	*EXECUTE
CHGJRNOBJ [9]		*OBJOPR, *OBJMGT	
	Obiekty niezintegrowanego systemu plików	*READ, *OBJMGT	
	Obiekty zintegrowanego systemu plików *R	*OBJMGT	
	Ścieżka do obiektu SUBTREE(*ALL) *RX	*OBJMGT	
	Ścieżka do obiektu SUBTREE(*NONE) *R	*OBJMGT	
	Katalog nadrzędny *X		
CHGRMTJRN	Kronika źródłowa	*CHANGE, *OBJMGT	*EXECUTE
	Kronika źródłowa	*USE, *OBJMGT	*EXECUTE
CMPJRNIMG	Kronika	*USE	*EXECUTE
	Dziennik	*USE	*EXECUTE
	Zbiór (File)	*USE	*EXECUTE
CRTJRN	Kronika		*READ, *ADD
	Dziennik	*OBJOPR, *OBJMGT, *READ	*EXECUTE
DLTJRN	Kronika	*OBJOPR, *OBJEXIST	*EXECUTE
DSPAUDJRNE[8]			
DSPJRN [6]	Kronika	*USE	*EXECUTE
	Kronika, jeśli określono parametr FILE(*ALLFILE), określony zbiór został usunięty z systemu lub podano parametr *IGNFILSLT dla dowolnych wybranych kodów kroniki lub kronika jest zdalna.	*OBJEXIST, *USE	*EXECUTE
	Dziennik	*USE	*EXECUTE
	Zbiór, jeśli podano	*USE	*EXECUTE
	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
DSPJRNMNU[1]			
ENDJRN	Patrz "Komendy zintegrowanego systemu plików" na stronie 347.		
ENDJRNAP	Kronika	*OBJOPR, *OBJMGT	*EXECUTE
	Zbiór (File)	*OBJOPR, *OBJMGT	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do obiektu lub katalogu**
ENDJRNOBJ	Kronika	*OBJOPR, *OBJMGT	*EXECUTE
	Obiekt	*OBJOPR, *READ, *OBJMGT	*EXECUTE
ENDJRNPF	Kronika	*OBJOPR, *OBJMGT	*EXECUTE
	Zbiór (File)	*OBJOPR, *OBJMGT, *READ	*EXECUTE
JRNAP [2]			
JRNPF [3]			
RCVJRNE	Kronika	*USE	*EXECUTE
	Kronika, jeśli określono parametr FILE(*ALLFILE), określony zbiór został usunięty z systemu lub podano parametr *IGNFILSLT dla dowolnych wybranych kodów kroniki lub kronika jest zdalna.	*OBJEXIST, *USE	*EXECUTE
	Dziennik	*USE	*EXECUTE
	Zbiór (File)	*USE	*EXECUTE
	Program obsługi wyjścia	*EXECUTE	*EXECUTE
RMVJRNCHG (Q)	Kronika	*USE	*EXECUTE
	Dziennik	*USE	*EXECUTE
	Obiekty niezintegrowanego systemu plików, których kronikowane zmiany są usuwane.	*OBJMGT, *CHANGE	*EXECUTE
RTVJRNE	Kronika	*USE	*EXECUTE
	Kronika, jeśli określono parametr FILE(*ALLFILE), określony zbiór został usunięty z systemu lub podano parametr *IGNFILSLT dla dowolnych wybranych kodów kroniki lub kronika jest zdalna.	*OBJEXIST, *USE	*EXECUTE
	Dziennik	*USE	*EXECUTE
	Zbiór (File)	*USE	*EXECUTE
RMVRMTJRN	Kronika źródłowa	*CHG, *OBJMGT	
SNDJRNE	Kronika	*OBJOPR, *ADD	*EXECUTE
	Obiekt niezintegrowanego systemu plików, jeśli został określony	*OBJOPR	*EXECUTE
	Obiekt zintegrowanego systemu plików, jeśli został określony	*R	*X
STRJRN	Patrz “Komendy zintegrowanego systemu plików” na stronie 347.		
STRJRNAP	Kronika	*OBJOPR, *OBJMGT	*EXECUTE
	Zbiór (File)	*OBJOPR, *OBJMGT	*EXECUTE
STRJRNPF	Kronika	*OBJOPR, *OBJMGT	*EXECUTE
	Zbiór (File)	*OBJOPR, *OBJMGT	*EXECUTE
STRJRNOBJ	Kronika	*OBJOPR, *OBJMGT	*EXECUTE
	Obiekt	*OBJOPR, *READ, *OBJMGT	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do obiektu lub katalogu**
WRKJRN [4] (Q)	Kronika	*USE	*READ[7]
	Dziennik, jeśli zażądano informacji dziennika	*USE	*EXECUTE
	Zbiór, jeśli zażądano odtwarzania do przodu lub odtwarzania wstecz	*OBJMGT, *CHANGE	*EXECUTE
	Obiekty, które usuwane są podczas odzyskiwania	*OBJEXIST	*EXECUTE
WRKJRNA [6]	Kronika	*OBJOPR i uprawnienia do danych inne niż *EXECUTE	*EXECUTE
	Dziennik [5]	*OBJOPR i uprawnienia do danych inne niż *EXECUTE	*EXECUTE

1 Patrz komenda WRKJRN (ta komenda pełni tę samą funkcję)

2 Patrz komenda STRJRNAP.

3 Patrz komenda STRJRNPF.

4 Podczas wykonywania operacji, do wywoływanych funkcji wymagane są dodatkowe uprawnienia. Na przykład, aby odtworzyć obiekt, użytkownik musi mieć uprawnienia wymagane do komendy RSTOBJ.

5 Jeśli wybrano opcję usunięcia dzienników, wymagane są uprawnienia *OBJOPR i *OBJEXIST.

6 Aby podać parametr JRN(*INTSYSJRN), użytkownik musi mieć uprawnienia specjalne *ALLOBJ.

7 Do wyświetlania menu WRKJRN wymagane jest uprawnienie *READ. Do użycia opcji menu wymagane jest uprawnienie *EXECUTE do biblioteki.

8 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *AUDIT.

9 Aby podać parametr PTLTNS(*ALWUSE), użytkownik musi mieć uprawnienia specjalne *ALLOBJ.

Komendy dzienników

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTJRNRCV	Dziennik		*READ, *ADD
DLTJRNRCV	Dziennik	*OBJOPR, *OBJEXIST i uprawnienia do danych inne niż *EXECUTE	*EXECUTE
	Kronika	*OBJOPR	*EXECUTE
DSPJRNRCVA	Dziennik	*OBJOPR i uprawnienia do danych inne niż *EXECUTE	*EXECUTE
	Kronika, jeśli jest podłączona	*OBJOPR	*EXECUTE
WRKJRNRCV [1], [2], [3]	Dziennik	Dowolne uprawnienia	*USE

1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

2 Jeśli wybrano opcję usunięcia dzienników, wymagane są uprawnienia *OBJOPR i *OBJEXIST.

3 Aby użytkownik mógł przeglądać opisy w dzienniku, musi mieć uprawnienia *OBJOPR i do danych inne niż *EXECUTE.

Komendy języka

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTBNDC	Zbiór źródłowy	*USE	*EXECUTE
	Zewnętrznie opisane zbiory urządzeń oraz zbiory bazy danych odnoszące się do programu źródłowego	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Katalog podany w parametrach OUTPUT, PPSRCSTMF lub MAKEDEP	*USE	*EXECUTE
	Zbiór podany w parametrach OUTPUT, PPSRCSTMF lub MAKEDEP	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
CRTBNDCBL	Zbiór źródłowy	*USE	*EXECUTE
	Zewnętrznie opisane zbiory urządzeń oraz zbiory bazy danych odnoszące się do programu źródłowego	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Katalog konsolidacji	*USE	*EXECUTE
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
CRTBNDCL	Zbiór źródłowy	*USE	*EXECUTE
	Zewnętrznie opisane zbiory urządzeń oraz zbiory bazy danych odnoszące się do programu źródłowego	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTBNDCPP	Zbiór źródłowy	*USE	*EXECUTE
	Zewnętrznie opisane zbiory urządzeń oraz zbiory bazy danych odnoszące się do programu źródłowego	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Katalog podany w parametrach OUTPUT, PPSRCSTMF, TEMPLATE lub MAKEDEP	*USE	*EXECUTE
	Zbiór podany w parametrach OUTPUT, PPSRCSTMF, TEMPLATE lub MAKEDEP	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Nagłówki generowane przez parametr TEMPLATE	*USE	*EXECUTE
CRTBNDRPG	Zbiór źródłowy	*USE	*EXECUTE
	Zewnętrznie opisane zbiory urządzeń oraz zbiory bazy danych odnoszące się do programu źródłowego	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Katalog konsolidacji	*USE	*EXECUTE
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
CRTCBLMOD	Zbiór źródłowy	*USE	*EXECUTE
	Zewnętrznie opisane zbiory urządzeń oraz zbiory bazy danych odnoszące się do programu źródłowego	*OBJOPR	*EXECUTE
	Moduł: REPLACE(*NO)		*READ, *ADD
	Moduł: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
CRTCLD	Zbiór źródłowy	*USE	*EXECUTE
	Obiekt ustawień narodowych - REPLACE(*NO)		*READ, *ADD
	Obiekt ustawień narodowych - REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTCLMOD	Zbiór źródłowy	*USE	*EXECUTE
	Zewnętrznie opisane zbiory urządzeń oraz zbiory bazy danych odnoszące się do programu źródłowego	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
CRTCLPGM	Zbiór źródłowy	*USE	*EXECUTE
	Zewnętrznie opisane zbiory urządzeń oraz zbiory bazy danych odnoszące się do programu źródłowego	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
CRTCBLPGM (program licencjonowany COBOL/400* lub środowisko S/38)	Zbiór źródłowy	*USE	*EXECUTE
	Zewnętrznie opisane zbiory urządzeń oraz zbiory bazy danych odnoszące się do programu źródłowego	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
CRTCMOD	Zbiór źródłowy	*USE	*EXECUTE
	Zewnętrznie opisane zbiory urządzeń oraz zbiory bazy danych odnoszące się do programu źródłowego	*OBJOPR	*EXECUTE
	Moduł: REPLACE(*NO)		*READ, *ADD
	Moduł: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Zbiór podany w parametrach OUTPUT, PPSRCSTMF lub MAKEDEP	*USE	*EXECUTE
	Zbiór podany w parametrach OUTPUT, PPSRCSTMF lub MAKEDEP	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTCPPMOD	Zbiór źródłowy	*USE	*EXECUTE
	Zewnętrznie opisane zbiory urządzeń oraz zbiory bazy danych odnoszące się do programu źródłowego	*OBJOPR	*EXECUTE
	Moduł: REPLACE(*NO)		*READ, *ADD
	Moduł: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Katalog podany w parametrach OUTPUT, PPSRCSTMF, TEMPLATE lub MAKEDEP	*USE	*EXECUTE
	Zbiór podany w parametrach OUTPUT, PPSRCSTMF, TEMPLATE lub MAKEDEP	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Nagłówki generowane przez parametr TEMPLATE	*USE	*EXECUTE
CRTRPGMOD	Zbiór źródłowy	*USE	*EXECUTE
	Zewnętrznie opisane zbiory urządzeń oraz zbiory bazy danych odnoszące się do programu źródłowego	*OBJOPR	*EXECUTE
	Moduł: REPLACE(*NO)		*READ, *ADD
	Moduł: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
CRTRPGPGM (program licencjonowany RPG/400* i środowisko S/38)	Zbiór źródłowy	*USE	*EXECUTE
	Zewnętrznie opisane zbiory urządzeń oraz zbiory bazy danych odnoszące się do programu źródłowego	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
CRTRPTPGM (program licencjonowany RPG/400 i środowisko S/38)	Zbiór źródłowy	*USE	*EXECUTE
	Program - REPLACE(*NO)		*READ, *ADD
	Program - REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Zbiór źródłowy dla generowanego programu RPG	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Zewnętrznie opisane zbiory urządzeń oraz zbiory bazy danych odnoszące się do programu źródłowego	*OBJOPR	*EXECUTE
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTS36CBL (środowisko S/36)	Zbiór źródłowy	*USE	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
CRTS36RPG	Zbiór źródłowy	*USE	*READ, *ADD
	Program: REPLACE(*NO)		*READ, *ADD
	Program - REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
CRTS36RPGR	Zbiór źródłowy	*USE	*READ, *ADD
	Zbiór ekranowy: REPLACE(*NO)		*READ, *ADD
	Zbiór ekranowy: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
CRTS36RPT	Zbiór źródłowy	*USE	*EXECUTE
	Zbiór źródłowy dla generowanego programu RPG	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
CRTSQLC OS/400' (program licencjonowany DB2 Query Manager and SQL Development for OS/400) [1]	Zbiór źródłowy	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór źródłowy	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specyfikacja opisu danych	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
CRTSQLCI (program licencjonowany DB2 Query Manager and SQL Development for OS/400) [1]	Zbiór źródłowy	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór źródłowy	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specyfikacja opisu danych	*OBJOPR	*EXECUTE
	Obiekt: REPLACE(*NO)		*READ, *ADD
	Obiekt: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTSQLCBL (program licencjonowany DB2 Query Manager and SQL Development for OS/400) [1]	Zbiór źródłowy	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór źródłowy	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specyfikacja opisu danych	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
CRTSQLCBLI (program licencjonowany DB2 Query Manager and SQL Development for OS/400) [1]	Zbiór źródłowy	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór źródłowy	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specyfikacja opisu danych	*OBJOPR	*EXECUTE
	Obiekt: REPLACE(*NO)		*READ, *ADD
	Obiekt: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
CRTSQLCPPI (program licencjonowany DB2 Query Manager and SQL Development for OS/400) [1]	Zbiór źródłowy	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór źródłowy	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specyfikacja opisu danych	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
CRTSQLFTN (program licencjonowany DB2 Query Manager and SQL Development for OS/400) [1]	Zbiór źródłowy	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór źródłowy	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specyfikacja opisu danych	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTSQLPLI (program licencjonowany DB2 Query Manager and SQL Development for OS/400) [1]	Zbiór źródłowy	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór źródłowy	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specyfikacja opisu danych	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
CRTSQLRPG (program licencjonowany DB2 Query Manager and SQL Development for OS/400) [1]	Zbiór źródłowy	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór źródłowy	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specyfikacja opisu danych	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
CRTSQLRPGI (program licencjonowany DB2 Query Manager and SQL Development for OS/400) [1]	Zbiór źródłowy	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór źródłowy	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specyfikacja opisu danych	*OBJOPR	*EXECUTE
	Obiekt: REPLACE(*NO)		*READ, *ADD
	Obiekt: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
CVTRPGSRC	Zbiór źródłowy	*USE	*EXECUTE
	Zbiór wyjściowy	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Plik protokołu	*OBJOPR, *OBJMGT, *ADD	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CVTSQLCPP [1]	Zbiór źródłowy	*OBJOPR, *READ	*EXECUTE
	Docelowy zbiór źródłowy	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specyfikacja opisu danych	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Tabela podana w parametrze SRTSEQ	*USE	*EXECUTE
ENDCBLDBG (program licencjonowany COBOL/400 lub środowisko S/38)	Program	*CHANGE	*EXECUTE
ENTCBLDBG (środowisko S/38)	Program	*CHANGE	*EXECUTE
DLTCLD	Obiekt ustawień narodowych	*OBJEXIST, *OBJMGT	*EXECUTE
RTVCLDSRC	Obiekt ustawień narodowych	*USE	*EXECUTE
	Docelowy zbiór	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
RUNSQLSTM (program licencjonowany SQL/400) [1]	Zbiór źródłowy	*OBJOPR, *READ	*EXECUTE
STRCBLDBG	Program	*CHANGE	*EXECUTE
STRREXPRC	Zbiór źródłowy	*USE	*EXECUTE
	Program obsługi wyjścia	*USE	*EXECUTE
STRSQL (program licencjonowany DB2 Query Manager and SQL Development for OS/400) [1]	Tabela kolejności sortowania	*USE	*EXECUTE
	Opis drukarki	*USE	*EXECUTE
	Kolejka wyjściowa drukarki	*USE	*EXECUTE
	Zbiór drukarkowy	*USE	*EXECUTE

1 Więcej informacji na temat wymagań dotyczących ochrony dla instrukcji SQL znajduje się w temacie **Authorization, privileges and object ownership** (Autoryzacja, przywileje i prawo własności do obiektów) w podręczniku **DB2 for iSeries SQL Reference** (znajdującym się w Centrum informacyjnym iSeries).

Komendy bibliotek

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki, na której wykonywane są operacje**
ADDLIBLE	Biblioteka.		*USE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki, na której wykonywane są operacje**
CHGCURLIB	Nowa biblioteka bieżąca		*USE
CHGLIB [8]	Biblioteka.		*OBJMGT
CHGLIBL	Każda biblioteka umieszczana na liście bibliotek		*USE
CHGSYSLIBL (Q)	Biblioteki na nowej liście		*USE
CLRLIB [3]	Każdy obiekt usuwany z biblioteki	*OBJEXIST	*USE
	Typy obiektów *DTADCT[14], *JRN[14],*JRNRCV[14], *MSGQ[14], *SBSD[14]	Patrz uprawnienia wymagane przez komendę DLT*xxx* dla typu obiektu	
	Urządzenie ASP (jeśli jest podane)	*USE	
CPYLIB [4]	Z biblioteki		*USE
	Do biblioteki, jeśli istnieje		*USE, *ADD
	Komendy CHKOBJ, CRTDUPOBJ	*USE	
	Komenda CRTLIB, jeśli tworzona jest biblioteka docelowa	*USE	
	Kopiowany obiekt	Uprawnienie wymagane podczas używania komendy CRTDUPOBJ do kopiowania typu obiektu.	
CRTLIB [9]	Urządzenie ASP (jeśli jest podane)	*USE	
DLTLIB [3]	Każdy obiekt usuwany z biblioteki	*OBJEXIST	*USE, *OBJEXIST
	Typy obiektów *DTADCT[14], *JRN[14],*JRNRCV[14], *MSGQ, *SBSD[14]	Patrz uprawnienia wymagane przez komendę DLT*xxx* dla typu obiektu	
	Urządzenie ASP (jeśli jest podane)	*USE	
DSPLIB	Biblioteka.		*READ
	Obiekty w bibliotece [5]	Uprawnienia inne niż *EXCLUDE	
	Urządzenie ASP (jeśli jest podane)	*EXECUTE	
DSPLIBD	Biblioteka.		Uprawnienia inne niż *EXCLUDE
EDTLIBL	Biblioteka, która ma być dodana do listy		*USE
RCLLIB	Biblioteka.		*USE, *OBJEXIST

Komendy bibliotek

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki, na której wykonywane są operacje
RSTLIB [7] (Q)	Definicja nośnika	*USE	*EXECUTE
	Biblioteka, jeśli istnieje		*READ, *ADD
	Kolejki komunikatów odtwarzane do biblioteki, w której już istnieją	*OBJOPR, *OBJEXIST [7]	*EXECUTE. *READ, *ADD
	Programy adoptujące uprawnienie	Właściciel lub uprawnienia *ALLOBJ i *SECADM	*EXECUTE
	Składowana biblioteka, jeśli podano parametr VOL(*SAVVOL)		*USE [6]
	Każdy obiekt odtwarzany w bibliotece	*OBJEXIST [3]	*EXECUTE, *READ, *ADD
	Profil użytkownika będący właścicielem tworzonych obiektów	*ADD [6]	
	Jednostka taśm, jednostka dyskietek, jednostka optyczna	*USE	*EXECUTE
	Zbiór wyjściowy, jeśli został podany	Patrz zasady ogólne	Patrz zasady ogólne
	Zbiór opisów pól QSYS/QASAVOBJ dla zbioru wyjściowego, jeśli określono nieistniejący zbiór wyjściowy	*USE	*EXECUTE
RSTLIB [7] (Q)	Zbiór taśmowy (QSYSTAP) lub zbiór dyskietkowy (QSYSDKT)	*USE [6]	*EXECUTE
	Zbiór wydruku QSYS/QPSRLDSP, jeśli określono OUTPUT(*PRINT)	*USE	*EXECUTE
	Zbiór składowania	*USE	*EXECUTE
	Zbiór nośnika optycznego (OPTFILE) [12]	*R	Nie dotyczy
	Przedrostek ścieżki pliku nośnika optycznego (OPTFILE) [12]	*X	Nie dotyczy
	Wolumin optyczny [11]	*USE	
	Opis urządzenia ASP [15]	*USE	
RSTS36LIBM	Źródłowy zbiór	*USE	*EXECUTE
	Docelowy zbiór	*CHANGE	*EXECUTE
	Do biblioteki	*CHANGE	*EXECUTE
	Zbiór urządzenia lub opis urządzenia	*USE	*EXECUTE
RTVLIBD	Biblioteka.		Uprawnienia inne niż *EXCLUDE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki, na której wykonywane są operacje
SAVLIB	Każdy obiekt w bibliotece	*OBJEXIST [6]	*READ, *EXECUTE
	Definicja nośnika	*USE	*EXECUTE
	Zbiór składowania, jeśli jest pusty	*USE, *ADD	*EXECUTE
	Zbiór składowania, jeśli istnieją w nim rekordy	*USE, *ADD, *OBJMGT	*EXECUTE
	Kol. komunik. akt. składowania (Save active message queue)	*OBJOPR, *ADD	*EXECUTE
	Jednostka taśm, jednostka dyskietek, jednostka optyczna	*USE	*EXECUTE
	Zbiór wyjściowy, jeśli został podany	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Zbiór opisów pól QSYS/QASAVOBJ, jeśli zbiór wyjściowy został podany ale nie istnieje	*USE [6]	*EXECUTE
	Zbiór wydruku QSYS/QPSAVOBJ	*USE [6]	*EXECUTE
SAVLIB	Zbiór nośnika optycznego [12]	*RW	Nie dotyczy
	Katalog nadrzędny pliku nośnika optycznego (OPTFILE) [12]	*WX	Nie dotyczy
	Przedrostek ścieżki pliku nośnika optycznego (OPTFILE) [12]	*X	Nie dotyczy
	Katalog główny (/) woluminu optycznego [12, 13]	*RWX	Nie dotyczy
	Wolumin optyczny [11]	*CHANGE	
	Opis urządzenia ASP [15]	*USE	
SAVRSTLIB	Opis urządzenia ASP [15]	*USE	
SAVS36LIBM	Składowanie do zbioru fizycznego	*OBJOPR, *OBJMGT	*EXECUTE
	Komenda QSYSDKT dla dyskietki lub QSYSTAP dla taśmy, wszystkie komendy wymagają uprawnień do urządzenia	*OBJOPR	*EXECUTE
	Składowanie do zbioru fizycznego, jeśli podano parametr MBROPT(*ADD)	*ADD	*READ, *ADD
	Składowanie do zbioru fizycznego, jeśli podano parametr MBROPT(*REPLACE)	*ADD, *DLT	*EXECUTE
	Z biblioteki		*USE
WRKLIB [10]	Biblioteka.		*USE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki, na której wykonywane są operacje
[1]	W tej kolumnie wskazano uprawnienia wymagane do biblioteki, na której są wykonywane działania. Na przykład, aby do listy bibliotek dodać bibliotekę CUSTLIB korzystając z komendy ADDLIBLE, wymagane są uprawnienia Use do biblioteki CUSTLIB.		
[2]	W tej kolumnie wskazano uprawnienia wymagane do biblioteki QSYS, ponieważ wszystkie biblioteki znajdują się w bibliotece QSYS.		
[3]	Jeśli użytkownik nie ma uprawnienia do istnienia (existence) obiektu dla części obiektów w bibliotece, to te obiekty nie są usuwane, biblioteka nie jest pusta i nie jest usuwana. Usuwane są tylko obiekty, do których użytkownik ma odpowiednie uprawnienia .		
[4]	Do tej komendy mają zastosowanie wszystkie ograniczenia, które stosowane są dla komendy CRTDUPOBJ.		
[5]	Jeśli użytkownik nie ma uprawnień do obiektu w bibliotece, pojawia się tekst *NOT AUTHORIZED (NIEUPRAWNIONY).		
[6]	Jeśli użytkownik ma uprawnienia specjalne *SAVSYS, nie potrzebuje podanych tu uprawnień.		
[7]	Aby podać parametr ALWOBJDIF(*ALL), użytkownik musi mieć uprawnienia specjalne *ALLOBJ.		
[8]	Aby zmienić wartość CRTOBJAUD dla biblioteki, użytkownik musi mieć uprawnienia specjalne *AUDIT. Jeśli zmieniana jest tylko wartość CRTOBJAUD, uprawnienia *OBJMGT **nie** są wymagane. Uprawnienia *OBJMGT **są** wymagane, gdy zmieniana jest wartość CRTOBJAUD oraz inne wartości.		
[9]	Aby dla wartości CRTOBJAUD podać wartość inną niż *SYSVAL, użytkownik musi mieć uprawnienia specjalne *AUDIT.		
[10]	Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.		
[11]	Woluminy optyczne nie są rzeczywistymi obiektami systemowymi. Dowiązanie między woluminem optycznym a listą autoryzacji używaną do ochrony obiektu jest utrzymywane przez funkcję obsługi nośników optycznych.		
[12]	To sprawdzanie uprawnień przeprowadzane jest jedynie wtedy, kiedy nośnik optyczny ma format UDF (Universal Disk Format).		
[13]	To sprawdzanie uprawnień przeprowadzane jest jedynie wtedy, kiedy nośnik optyczny jest czyszczony.		
[14]	Ten obiekt jest dozwolony dla niezależnej ASP.		
[15]	Uprawnienie wymagane tylko, jeśli operacja składowania lub odtwarzania wymaga przełącznika przestrzeni nazw biblioteki.		

Komendy klucza licencyjnego

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ADDLICKEY (Q)	Zbiór wyjściowy	*USE	*EXECUTE
DSPLICKEY (Q)	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
RMVLICKEY (Q)	Zbiór wyjściowy	*CHANGE	*EXECUTE

Komendy programów licencjonowanych

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGLICINF (Q)	Komenda WRKLICINF	*USE	*EXECUTE
DLTLICPGM [1,2] (Q)			
DSPTM			
INZSYS (Q)			
RSTLICPGM [1,2] (Q)			
SAVLICPGM [1,2] (Q)			
WRKLICINF (Q)			

[1] Niektóre programy licencjonowane mogą być usunięte, składowane lub odtwarzane tylko przez użytkownika, który jest zarejestrowany w katalogu dystrybucyjnym systemu.

[2] Jeśli usuwany, odtwarzany lub składowany jest program licencjonowany zawierający foldery, wszystkie ograniczenia dotyczące komendy DLTDLO mają zastosowanie także do tej komendy.

[3] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

Komendy opisu linii

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGLINASC [2]	Opis linii	*CHANGE, *OBJMGT	*EXECUTE
	Opis kontrolera (SWTCTLLST)	*USE	*EXECUTE
CHGLINBSC [2]	Opis linii	*CHANGE, *OBJMGT	*EXECUTE
	Opis kontrolera (SWTCTLLST)	*USE	*EXECUTE
CHGLINDDI [2]	Opis linii	*CHANGE, *OBJMGT	*EXECUTE
CHGLINETH [2]	Opis linii	*CHANGE, *OBJMGT	*EXECUTE
CHGLINFAX [2]	Opis linii	*CHANGE, *OBJMGT	*EXECUTE
CHGLINFR [2]	Opis linii	*CHANGE, *OBJMGT	*EXECUTE
CHGLINPPP[2]	Opis linii	*CHANGE, *OBJMGT	*EXECUTE
CHGLINSDLC [2]	Opis linii	*CHANGE, *OBJMGT	*EXECUTE
CHGLINTDLC [2]	Opis linii	*CHANGE, *OBJMGT	*EXECUTE
CHGLINTRN [2]	Opis linii	*CHANGE, *OBJMGT	*EXECUTE
CHGLINX25 [2]	Opis linii	*CHANGE, *OBJMGT	*EXECUTE
	Opis kontrolera (SWTCTLLST)	*USE	*EXECUTE
	Lista połączeń (CNNLSTIN lub CNNLSTOUT)	*USE	*EXECUTE
	Opis interfejsu sieciowego (SWTNWILST)	*USE	*EXECUTE
CHGLINWLS [2]	Opis linii	*CHANGE, *OBJMGT	*EXECUTE
	Program (INZPGM)	*USE	*EXECUTE

Komendy opisu linii

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTLINASC [2]	Opis kontrolera (CTL i SWTCTLLST)	*USE	*EXECUTE
	Opis linii		*READ, *ADD
CRTLINBSC [2]	Opis kontrolera (SWTCTLLST i CTL)	*USE	*EXECUTE
	Opis linii		*READ, *ADD
CRTLINDDI [2]	Opis linii		*READ, *ADD
	Opis interfejsu sieciowego (NWI)	*USE	*EXECUTE
	Opis kontrolera (NETCTL)	*USE	*EXECUTE
CRTLINETH [2]	Opis kontrolera (NETCTL)	*USE	*EXECUTE
	Opis linii		*READ, *ADD
	Opis interfejsu sieciowego (NWI)	*USE	*EXECUTE
	Opis serwera sieciowego (NWS)	*USE	*EXECUTE
CRTLINFAX [2]	Opis linii		*READ, *ADD
	Opis kontrolera	*USE	*EXECUTE
CRTLINFR [2]	Opis linii		*READ, *ADD
	Opis interfejsu sieciowego (NWI)	*USE	*EXECUTE
	Opis kontrolera (NETCTL)	*USE	*EXECUTE
CRTLINPPP[2]	Opis kontrolera (NETCTL)	*USE	*EXECUTE
	Opis linii		*READ, *ADD
CRTLINSDLC [2]	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis linii		*READ, *ADD
CRTLINTDLC [2]	Opis kontrolera (WSC i CTL)	*USE	*EXECUTE
	Opis linii		*READ, *ADD
CRTLINTRN [2]	Opis kontrolera (NETCTL)	*USE	*EXECUTE
	Opis linii		*READ, *ADD
	Opis interfejsu sieciowego (NWI)	*USE	*EXECUTE
	Opis serwera sieciowego (NWS)	*USE	*EXECUTE
CRTLINX25 [2]	Opis kontrolera (SWTCTLLST)	*USE	*EXECUTE
	Opis kontrolera trwałego obwodu wirtualnego (PVC) (LGLCHLE)	*USE	*EXECUTE
	Opis linii		*READ, *ADD
	Lista połączeń (CNNLSTIN lub CNNLSTOUT)	*USE	*EXECUTE
	Opis interfejsu sieciowego (NWI lub SWTNWILST)	*USE	*EXECUTE
CRTLINWLS [2]	Opis linii		*READ, *ADD
	Opis kontrolera (NETCTL)	*USE	*EXECUTE
	Program (INZPGM)	*USE	*EXECUTE
DLTLIND	Opis linii	*OBJEXIST	*EXECUTE
DSPLIND	Opis linii	*USE	*EXECUTE
ENDLINRCY	Opis linii	*OBJOPR	*EXECUTE
PRTCMNSEC [2, 3]			

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
RSMLINRCY	Opis linii	*OBJOPR	*EXECUTE
WRKLIND [1]	Opis linii	*OBJOPR	*EXECUTE

1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

2 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

3 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *ALLOBJ.

Komendy sieci lokalnej (LAN)

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Te komendy nie wymagają żadnych uprawnień do obiektu:			
ADDLANADPI	DSPLANADPP	RMVLANADPT (Q)	WRKLANADPT
CHGLANADPI	DSPLANSTS	RMVLANADPI	

Komendy ustawień narodowych

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTLOCALE	Zbiór źródłowy	*USE	*USE, *ADD
DLTLOCALE	Ustawienia narodowe	*OBJEXIST	*USE

Komendy struktury serwera poczty

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Ta komenda nie wymaga żadnych uprawnień do obiektów:	
ENDMSF (Q)	STRMSF (Q)

Komendy nośników

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDTAPCTG	Opis biblioteki taśm	*USE	*EXECUTE
CFGDEVMLB[1]	Opis biblioteki taśm	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVMLB (Q)	Opis biblioteki taśm	*USE	*EXECUTE
CHGJOBMLBA[4]	Opis biblioteki taśm	*CHANGE	*EXECUTE
CHGTAPCTG	Opis biblioteki taśm	*USE	*EXECUTE
CHKDKT	Opis jednostki dyskietek	*USE	*EXECUTE

Komendy nośników

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CHKTAP	Opis napędu taśm	*USE	*EXECUTE
CLRDKT	Opis jednostki dyskietek	*USE	*EXECUTE
CRTTAPCGY	Opis biblioteki taśm		
DLTDKTLBL	Opis jednostki dyskietek	*USE	*EXECUTE
DLTMEDDFN	Definicja nośnika	*OBJEXIST	*EXECUTE
DLTTAPCGY	Opis biblioteki taśm		
DMPTAP (Q)	Opis napędu taśm	*USE	*EXECUTE
DSPDKT	Opis jednostki dyskietek	*USE	*EXECUTE
DSPTAP	Opis napędu taśm	*USE	*EXECUTE
DSPTAPCGY	Opis biblioteki taśm		
DSPTAPCTG	Opis biblioteki taśm	*USE	*EXECUTE
DSPTAPSTS	Opis biblioteki taśm	*USE	*EXECUTE
DUPDKT	Opis jednostki dyskietek	*USE	*EXECUTE
DUPTAP	Opis napędu taśm	*USE	*EXECUTE
INZDKT	Opis jednostki dyskietek	*USE	*EXECUTE
INZTAP	Opis napędu taśm	*USE	*EXECUTE
RMVTAPCTG	Opis biblioteki taśm	*USE	*EXECUTE
RNMDKT	Opis jednostki dyskietek	*USE	*EXECUTE
SETTAPCGY	Opis biblioteki taśm	*USE	*EXECUTE
WRKMLBRSCQ [3]	Opis biblioteki taśm	*USE	*EXECUTE
WRKMLBSTS [2] (Q)	Opis biblioteki taśm	*USE	*EXECUTE
WRKTAPCTG	Opis biblioteki taśm	*USE	*EXECUTE

1 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

2 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

3 Aby zmienić atrybuty biblioteki nośnika, użytkownik musi mieć uprawnienia *CHANGE do opisu biblioteki taśm. Aby zmienić priorytet lub pracować z zadaniem innego użytkownika, użytkownik musi mieć uprawnienia specjalne *JOBCTL.

4 Aby zmienić priorytet lub pracować z zadaniem innego użytkownika, użytkownik musi mieć uprawnienia specjalne *JOBCTL.

Komendy paneli grupowych i menu

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CHGMNU	Menu	*CHANGE	*USE
CRTMNU	Zbiór źródłowy	*USE	*EXECUTE
	Menu: REPLACE(*NO)		*READ, *ADD
	Menu: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTPNLGRP	Panel grupowy: Replace(*NO)		*READ, *ADD
	Pakiet Panel: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Zbiór źródłowy	*USE	*EXECUTE
	Włączenie zbioru	*USE	*EXECUTE
CRTS36MNU	Menu: REPLACE(*NO)		*READ, *ADD
	Menu: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Zbiór źródłowy	*USE	*EXECUTE
	Zbiory komunikatów nazwane w źródle	*OBJOPR, *OBJEXIST	*EXECUTE
	Zbiór docelowy, gdy wartością parametru TOMBR nie jest *NONE	*OBJOPR, *OBJMGT, *OBJEXIST, *ADD	*READ, *ADD
	Zbiór ekranowy menu, jeśli podano REPLACE(*YES)	*OBJOPR, *OBJEXIST	*EXECUTE
	Zbiór tekstów komunikatów komendy	*OBJOPR, *OBJEXIST	*EXECUTE
	Komenda Tworzenie zbioru komunikatów (Create Message File - CRTMSGF)	*OBJOPR	*EXECUTE
	Komenda Dodanie opisu komunikatu (Add Message Description - ADDMSGD)	*OBJOPR	*EXECUTE
	Komenda Tworzenie zbioru ekranowego (Create Display File - CRTDSPF)	*OBJOPR	*EXECUTE
DLTMNU	Menu	*OBJOPR, *OBJEXIST	*EXECUTE
DLTPNLGRP	Panel grupowy	*OBJEXIST	*EXECUTE
DSPMNUA	Menu	*USE	*USE
GO	Menu	*USE	*USE
	Zbiór ekranowy i zbiory komunikatów z podanym parametrem *DSPF	*USE	*EXECUTE
	Biblioteki bieżąca i produktu	*USE	
	Program z podanym parametrem *PGM	*USE	*EXECUTE
WRKMNU [1]	Menu	Dowolne	*USE
WRKPNLGRP [1]	Panel grupowy	Dowolne	*EXECUTE

1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

Komendy komunikatów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
DSPMSG	Kolejka komunikatów	*USE	*USE
	Kolejka komunikatów, w której jest umieszczana odpowiedź na komunikat z zapytaniem	*USE, *ADD	*USE
	Usuwanie komunikatów z kolejki komunikatów	*USE, *DLT	*USE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
RCVMSG	Kolejka komunikatów	*USE	*EXECUTE
	Usuwanie komunikatów z kolejki	*USE, *DLT	*EXECUTE
RMVMSG	Kolejka komunikatów	*OBJOPR, *DLT	*EXECUTE
RTVMSG	Zbiór komunikatów	*USE	*EXECUTE
SNDBRKMSG	Kolejka komunikatów, w której jest umieszczana odpowiedź na komunikaty z zapytaniem	*OBJOPR, *ADD	*EXECUTE
SNDMSG	Kolejka komunikatów	*OBOPR, *ADD	*EXECUTE
	Kolejka komunikatów, w której jest umieszczana odpowiedź na komunikat z zapytaniem	*OBJOPR, *ADD	*EXECUTE
SNDPGMMSG	Kolejka komunikatów	*OBJOPR, *ADD	*EXECUTE
	Zbiór komunikatów, podczas wysyłania komunikatu predefiniowanego	*USE	*EXECUTE
	Kolejka komunikatów, w której jest umieszczana odpowiedź na komunikat z zapytaniem	*OBJOPR, *ADD	*EXECUTE
SNDRPY	Kolejka komunikatów	*USE, *ADD	*EXECUTE
	Usuwanie komunikatów z kolejki	*USE, *ADD, *DLT	*EXECUTE
SNDUSRMSG	Kolejka komunikatów	*OBJOPR, *ADD	*EXECUTE
	Zbiór komunikatów, podczas wysyłania komunikatu predefiniowanego	*USE	*EXECUTE
WRKMSG	Kolejka komunikatów	*USE	*USE
	Kolejka komunikatów, w której jest umieszczana odpowiedź na komunikat z zapytaniem	*USE, *ADD	*USE
	Usuwanie komunikatów z kolejki komunikatów	*USE, *DLT	*USE

Komendy opisu komunikatów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDMSGD	Zbiór komunikatów	*USE, *ADD	*EXECUTE
CHGMSGD	Zbiór komunikatów	*USE, *UPD	*EXECUTE
DSPMSGD	Zbiór komunikatów	*USE	*EXECUTE
RMVMSGD	Zbiór komunikatów	*OBJOPR, *DLT	*EXECUTE
WRKMSGD [1]	Zbiór komunikatów	*USE	*EXECUTE

1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

Komendy zbiorów komunikatów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGMSGF	Zbiór komunikatów	*USE, *DLT	*EXECUTE
CRTMSGF	Zbiór komunikatów		*READ, *ADD

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
DLTMSGF	Zbiór komunikatów	*OBJEXIST	*EXECUTE
DSPMSGF	Zbiór komunikatów	*USE	*EXECUTE
MRGMSGF	Źródłowy zbiór komunikatów	*USE	*EXECUTE
	Do zbioru komunikatów	*USE, *ADD, *DLT	*EXECUTE
	Zastąpienie zbioru komunikatów	*USE, *ADD	*EXECUTE
WRKMSGF [1.]	Zbiór komunikatów	Dowolne uprawnienia	*USE
[1] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.			

Komendy kolejki komunikatów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGMSGQ	Kolejka komunikatów	*USE, *DLT	*EXECUTE
CLRMSGQ	Kolejka komunikatów	*OBJOPR, *DLT	*EXECUTE
CRTMSGQ	Kolejka komunikatów		*READ, *ADD
DLTMSGQ	Kolejka komunikatów	*OBJEXIST, *USE, *DLT	*EXECUTE
DSPLOG			*EXECUTE
WRKMSGQ [1]	Kolejka komunikatów	Dowolne uprawnienia	*USE
[1] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.			

Komendy migracji

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
RCVMGRDTA	Zbiór (File)	*ALL	*READ, *ADD
	Urządzenie	*CHANGE	*EXECUTE
SNDMGRDTA	Zbiór (File)	*ALL	*READ, *ADD
	Urządzenie	*CHANGE	*EXECUTE
Przedstawione poniżej komendy nie wymagają uprawnień do obiektu. Te komendy mają uprawnienia publiczne *EXCLUDE. Aby korzystać z tych komend, użytkownik musi mieć uprawnienia specjalne *ALLOBJ.			
ANZS34OCL	CVTS36JOB	MGRS36DSPF	MIGRATE
ANZS36OCL	CVTS36QRY	MGRS36ITM	QMUS36
CHGS34LIBM	CVTS38JOB	MGRS36LIB	RESMGRNAM
CHKS36SRCA	GENS36RPT	MGRS36MNU	RSTS38AUT
CVTBASSTR	GENS38RPT	MGRS36MSGF	STRS36MGR
CVTBASUNF	MGRS36	MGRS36QRY [1]	STRS38MGR
CVTBGUDTA	MGRS36APF [1]	MGRS36RPG	
CVTS36CFG	MGRS36CBL	MGRS36SEC	
CVTS36FCT	MGRS36DFU [1]	MGRS38OBJ	
[1] Użytkownik musi mieć uprawnienia specjalne *ALLOBJ i zainstalowaną opcję 4 OS/400.			

Komendy opisu trybu

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CHGMODD [2]	Opis trybu	*CHANGE, *OBJMGT	*EXECUTE
CRTMODD [2]	Opis trybu		*READ, *ADD
CHGSSNMAX	Opis urządzenia	*OBJOPR	*EXECUTE
DLTMODD	Opis trybu	*OBJEXIST	*EXECUTE
DSPMODD	Opis trybu	*USE	*EXECUTE
DSPMODSTS	Urządzenie	*OBJOPR	*EXECUTE
	Opis trybu	*OBJOPR	*EXECUTE
ENDMOD	Opis urządzenia	*OBJOPR	*EXECUTE
STRMOD	Opis urządzenia	*OBJOPR	*EXECUTE
WRKMODD [1]	Opis trybu	*OBJOPR	*EXECUTE

1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

2 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

Komendy modułu

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CHGMOD	Moduł	*OBJMGT, *USE	*USE
	Moduł, jeśli podano OPTIMIZE	*OBJMGT, *USE	*USE, *ADD, *DLT
	Moduł, jeśli podano FRCCRT(*YES)	*OBJMGT, *USE	*USE, *ADD, *DLT
	Moduł, jeśli podano ENBPRFCOL	*OBJMGT, *USE	*USE, *ADD, *DELETE
DLTMOD	Moduł	*OBJEXIST	*EXECUTE
DSPMOD	Moduł	*USE	*EXECUTE
RTVBNDSRC [1]	Moduł	*USE	*EXECUTE
	*SRVPGM i moduły podane z *SRVPGM	*USE	*EXECUTE
	Zbiór źródłowy bazy danych, jeśli zbiór i podzbiór istnieją oraz podano MBROPT(*REPLACE).	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Zbiór źródłowy bazy danych, jeśli zbiór i podzbiór istnieją oraz podano MBROPT(*ADD).	*OBJOPR, *ADD	*EXECUTE
	Zbiór źródłowy bazy danych, jeśli zbiór istnieje a podzbiór musi być utworzony.	*OBJOPR, *OBJMGT, *ADD	*EXECUTE, *READ, *ADD
	Zbiór źródłowy bazy danych, jeśli zbiór i podzbiór muszą być utworzone.		*EXECUTE, *READ, *ADD
	Komenda CRTSCRPF, jeśli zbiór nie istnieje		*EXECUTE
	Komenda ADDPFM, jeśli podzbiór nie istnieje		*EXECUTE
	Komenda RGZPFM w celu zreorganizowania podzbioru zbioru źródłowego	*OBJMGT	*EXECUTE
WRKMOD [2]	Moduł	Dowolne uprawnienia	*USE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**

[1] Uprawnienia *USE potrzebne są do:
- komendy CRTSRCPF, jeśli zbiór nie istnieje,
- komendy ADDPFM, jeśli podzbiór nie istnieje,
- komendy RGZPFM, aby zreorganizować podzbiór zbioru źródłowego; do reorganizowania podzbioru zbioru źródłowego wymagane są uprawnienia *CHANGE i *OBJALTER lub uprawnienia *OBJMGT; funkcja komendy RTVBNDSRC kończy reorganizowanie podzbioru zbioru źródłowego następującymi po sobie liczbami zero.

[2] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

Komendy opisu NetBIOS

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGNTBD [2]	Opis NetBIOS	*CHANGE, *OBJMGT	*EXECUTE
CRTNTBD [2]	Opis NetBIOS		*EXECUTE
DLTNTBD	Opis NetBIOS	*OBJEXIST	*EXECUTE
DSPNTBD	Opis NetBIOS	*USE	*EXECUTE
WKRNTBD[1]	Opis NetBIOS	*OBJOPR	*EXECUTE

[1] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

[2] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

Komendy sieciowe

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDNETJOBE (Q)	Profil użytkownika w pozycji zadania sieciowego	*USE	
APING	Opis urządzenia	*CHANGE	
AREXEC	Opis urządzenia	*CHANGE	
CHGNETA (Q) [4]			
CHGNETJOBE (Q)	Profil użytkownika w pozycji zadania sieciowego	*USE	
DLTNETF [2]	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
DSPNETA			

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
RCVNETF [2]	Podzbiór docelowy nie istnieje, podano MBROPT(*ADD)	*OBJMGT, *USE	*EXECUTE, *ADD
	Podzbiór docelowy nie istnieje, podano MBROPT(*REPLACE)	*OBJMGT, *CHANGE	*EXECUTE, *ADD
	Podzbiór docelowy istnieje, podano MBROPT(*ADD)	*USE	*EXECUTE
	Podzbiór docelowy istnieje, podano MBROPT(*REPLACE)	*OBJMGT, *CHANGE	*EXECUTE
RMVNETJOBE (Q)	Profil użytkownika w pozycji zadania sieciowego	*USE	
RTVNETA			
RUNRMTCMD	Opis urządzenia	*CHANGE	
SNDNETF	Zbiór fizyczny lub zbiór składowania	*USE	*EXECUTE
SNDNETMSG do użytkownika lokalnego	Kolejka komunikatów	*OBJOPR, *ADD	*EXECUTE
VFYAPPCCNN	Opis urządzenia	*CHANGE	
WRKNETF [2,3]			
WRKNETJOBE [3]	QUSRSYS/QANFNJE	*USE	*EXECUTE

1 Użytkownik musi mieć uprawnienia specjalne *ALLOBJ.

2 Użytkownik może uruchamiać te komendy na własnych zbiorach sieciowych użytkownika lub na zbiorach sieciowych, których właścicielem jest profil grupowy użytkownika. Aby przetwarzać zbiory sieciowe innego użytkownika, wymagane są uprawnienia specjalne *ALLOBJ.

3 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

4 Aby zmienić niektóre atrybuty sieciowe, niezbędne jest uprawnienie specjalne *IOSYSCFG lub *ALLOBJ i *IOSYSCFG.

Komendy sieciowego systemu plików

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu
ADDMFS [1,3]	katalog_do_podłączenia	*DIR	″główny″	*W
CHGNFSEXP [1,2]	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
DSPMFSINF	niektóre_katalogi	*DIR	″główny″	*RX
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
ENDNFSSVR [1,4]	brak			
EXPORTFS [1,2]	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
MOUNT [1,3]	katalog_do_podłączenia	*DIR	″główny″	*W

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu
RLSIFSLCK [1]	obiekt	*STMF	″główny″, QOpenSys, UDFS	*R
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
RMVMFS [1]				
STATFS	niektóre_katalogi	*DIR	″główny″	*RX
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
STRNFSSVR [1]	brak			
UNMOUNT [1]				

[1] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

[2] Jeśli zostanie podana opcja -F, a zbiór /etc/exports nie istnieje, użytkownik musi mieć uprawnienia do zapisywania i wykonywania (*WX) do katalogu /etc. Jeśli zostanie podana opcja -F i zbiór /etc/exports istnieje, użytkownik musi mieć uprawnienia do odczytywania i zapisywania (*RW) do zbioru /etc/exports oraz uprawnienia *X do katalogu /etc.

[3] Podłączany katalog (katalog_do_podłączenia) jest dowolnym katalogiem zintegrowanego systemu plików, który może być podłączany.

[4] Aby zakończyć jakiekolwiek zadania demona uruchomione przez innego użytkownika, użytkownik musi mieć uprawnienia specjalne *JOBCTL.

Komendy opisu interfejsu sieciowego

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CHGNWIFR [2]	Opis interfejsu sieciowego	*CHANGE, *OBJMGT	*EXECUTE
CRTNWIFR [2]	Opis interfejsu sieciowego		*READ, *ADD
	Opis linii (DLCI)	*USE	*EXECUTE
DLTNWID	Opis interfejsu sieciowego	*OBJEXIST	*EXECUTE
DSPNWID	Opis interfejsu sieciowego	*USE	*EXECUTE
WRKNWID [1]	Opis interfejsu sieciowego	*OBJOPR	*EXECUTE

[1] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

[2] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

Komendy serwera sieciowego

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu
ADDNWSSTGL [2]	Ścieżka (/QFPNWSSTG)	*DIR	″główny″	*X
	Katalog nadrzędny (nazwa przestrzeni pamięci)	*DIR	″główny″	*WX
	Zbiory tworzące przestrzeń pamięci	*FILE	″główny″	*RW
	Opis serwera sieciowego	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
CHGNWSUSRA [4]	Profil użytkownika	*USRPRF		*OBJMGT, *USE
CRTNWSSTG [2]	Ścieżka (katalog główny i /QFPNWSSTG)	*DIR	″główny″	*WX
DLTNWSSTG [2]	Ścieżka (/QFPNWSSTG)	*DIR	″główny″	*WX
	Katalog nadrzędny (nazwa przestrzeni pamięci)	*DIR	″główny″	*RWX, *OBJEXIST
	Zbiory tworzące przestrzeń pamięci	*FILE	″główny″	*OBJEXIST
DSPNWSSTG	Ścieżka do przestrzeni pamięci	*DIR	″główny″	*X
	Zbiory tworzące przestrzeń pamięci	*FILE	″główny″	*R
RMVNWSSTGL [2]	Ścieżka (/QFPNWSSTG)	*DIR	″główny″	*X
	Katalog nadrzędny (nazwa przestrzeni pamięci)	*DIR	″główny″	*WX
	Zbiory tworzące przestrzeń pamięci	*FILE	″główny″	*RW
	Opis serwera sieciowego	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
WRKNWSSTG	Ścieżka do przestrzeni pamięci	*DIR	″główny″	*X
	Zbiory tworzące przestrzeń pamięci	*FILE	″główny″	*R

Te komendy nie wymagają żadnych uprawnień do obiektu:

ADDRMTSVR	DSPNWSALS	SNDNWSMSG
CHGNWSA [4](Q)	DSPNWSSSN	WRKNWSALS
CHGNWSALS	DSPNWSSTC	WRKNWSENR
CRTNWSALS	DSPNWSUSR	WRKNWSSSN
DLTNWSALS	DSPNWSUSRA	WRKNWSSTS
DSPNWSA	SBMNWSCMD (Q) [3]	

1 Uprawnienia adoptowane nie są wykorzystywane dla komend serwera sieciowego.

2 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

3 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *JOBCTL.

4 Aby dla parametrów NDSTREELST i NTW3SVRLST określić wartość inną niż *NONE, niezbędne jest uprawnienie specjalne *SECADM.

Komendy opisu serwera sieciowego

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki QSYS**
CHGNWSD [2]	Opis serwera sieciowego	*CHANGE, *OBJMGT	*EXECUTE
	Opis NetBIOS (NTB)	*USE	*EXECUTE
CRTNWSD [2]	Opis NetBIOS (NTB)	*USE	*EXECUTE
	Opis linii (PORTS)	*USE	*EXECUTE
DLTNWSD	Opis serwera sieciowego	*OBJEXIST	*EXECUTE
DSPNWSD	Opis serwera sieciowego	*USE	*EXECUTE
WRKNWSD[1]	Opis serwera sieciowego	*OBJOPR	*EXECUTE

1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

2 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

Komendy listy węzłów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDNODLE	Lista węzłów	*OBJOPR, *ADD	*EXECUTE
CRTNODL	Lista węzłów		*READ, *ADD
DLTNODL	Lista węzłów	*OBJEXIST	*EXECUTE
RMVNODLE	Lista węzłów	*OBJOPR, *READ, *DLT	*EXECUTE
WRKNODL [1]	Lista węzłów	*USE	*USE
WRKNODLE	Lista węzłów	*USE	*EXECUTE

1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

Komendy usług biurowych

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Te komendy nie wymagają uprawnień do obiektu.		
ADDACC (Q)	GRTACCAUT [2,3,6] (Q)	RVKUSRPMN [1,2]
DSPACC	GRTUSRPMN [1,2]	WRKDOCLIB [4]
DSPACCAUT	RMVACC [1] (Q)	WRKDOCPRTQ [5]
DSPUSRPMN	RVKACCAUT [1]	

[1]	Aby nadać lub odebrać uprawnienia dla kodu dostępu lub uprawnienia do dokumentów innym użytkownikom, użytkownik musi mieć uprawnienia specjalne *ALLOBJ.
[2]	Dostęp jest ograniczony do dokumentów, folderów i poczty, które nie są osobiste.
[3]	Przed nadaniem uprawnień kod dostępu musin być zdefiniowany w systemie (za pomocą komendy Dodanie kodu dostępu (Add Access Code - ADDACC)). Użytkownik, któremu nadawane są te uprawnienia, musi być zarejestrowany w katalogu dystrybucyjnym.
[4]	Użytkownik musi mieć uprawnienia specjalne *SECADM.
[5]	Dla określonych funkcji wywoływanych przez wybrane operacje wymagane są dodatkowe uprawnienia. Uprawnienia dodatkowe są wymagane także do komend wywoływanych podczas wykonywania określonych funkcji.
[6]	Aby przyznawać uprawnienia dla kodu dostępu innym użytkownikom, niezbędne jest uprawnienie specjalne do wszystkich obiektów (*ALLOBJ) lub administratora ochrony (*SECADM).

Komendy kursów elektronicznych

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

		Wymagane uprawnienie	
Komenda	**Obiekt odniesienia**	**Do obiektu**	**Do biblioteki**
CVTEDU			
STREDU			

Komendy Asysty Operacyjnej

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

		Wymagane uprawnienie	
Komenda	**Obiekt odniesienia**	**Do obiektu**	**Do biblioteki**
CHGBCKUP [1]	QUSRSYS/QEZBACKUPL *USRIDX	*CHANGE	*EXECUTE
CHGCLNUP[2]			
CHGPWRSCD [3]		*USE	*EXECUTE
CHGPWRSCDE [3]		*USE	*EXECUTE
DSPBCKSTS	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
DSPBCKUP	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
DSPBCKUPL	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*USE	*EXECUTE
DSPPWRSCD			
EDTBCKUPL [1]	QUSRSYS/QEZBACKUPL *USRIDX	*CHANGE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*CHANGE	*EXECUTE
ENDCLNUP [4]	ENDJOB *CMD	*USE	*EXECUTE
PRTDSKINF (Q)	QUSRSYS/QAEZDISK *FILE, member QCURRENT	*USE	*EXECUTE
	Urządzenie ASP (jeśli jest podane)	*USE	

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
RTVBCKUP	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
RTVCLNUP			
RTVDSKINF (Q) [5]	Urządzenie ASP (jeśli jest podane)	*USE	
RTVPWRSCDE	Komenda DSPPWRSCD	*USE	
RUNBCKUP [1]	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*USE	*EXECUTE
	Komendy: SAVLIB, SAVCHGOBJ, SAVDLO, SAVSECDTA, SAVCFG, SAVCAL, SAV	*USE	*EXECUTE
STRCLNUP[4]	Profil użytkownika QPGMR	*USE	
	Kolejka zadań	*USE	*EXECUTE

1 Użytkownik musi mieć uprawnienia specjalne *ALLOBJ lub *SAVSYS.

2 Użytkownik musi mieć uprawnienia specjalne *ALLOBJ, *SECADM i *JOBCTL.

3 Użytkownik musi mieć uprawnienia specjalne *ALLOBJ i *SECADM.

4 Użytkownik musi mieć uprawnienia specjalne *JOBCTL.

5 Użytkownik musi mieć uprawnienia specjalne *ALLOBJ.

Komendy urządzeń optycznych

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Tabela 150.

Komenda	Obiekt odniesienia	Wymagane uprawnienie		
		Obiekt	**Biblioteka.**	**Wolumin optyczny [1]**
ADDOPTCTG (Q)	Urządzenie optyczne	*USE	*EXECUTE	
ADDOPTSVR (Q)	Serwer CSI	*USE	*EXECUTE	
CHGDEVOPT [4]	Urządzenie optyczne	*CHANGE, *OBJMGT	*EXECUTE	
CHGOPTA (Q)				
CHGOPTVOL	Katalog główny (/) woluminu podczas zmiany opisu tekstowego [5]	*W	Nie dotyczy	Nie dotyczy
	Urządzenie optyczne	*USE	*EXECUTE	*CHANGE[3]
	Serwer CSI	*USE	*EXECUTE	Nie dotyczy

Tabela 150. (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienie		
		Obiekt	**Biblioteka.**	**Wolumin optyczny [1]**
CPYOPT	Urządzenie optyczne	*USE	*EXECUTE	*USE - wolumin źródłowy
				*ALL - wolumin docelowy
	Każdy poprzedzający katalog w ścieżce zbioru źródłowego	*X	Nie dotyczy	Nie dotyczy
	Każdy poprzedzający katalog w ścieżce zbioru docelowego	*X	Nie dotyczy	Nie dotyczy
	Zbiór źródłowy (*DSTMF)[5]	*R	Nie dotyczy	Nie dotyczy
	Katalog nadrzędny zbioru docelowego	*WX	Nie dotyczy	Nie dotyczy
	Katalog nadrzędny katalogu nadrzędnego, jeśli tworzony jest katalog	*WX	Nie dotyczy	Nie dotyczy
CPYOPT	Zbiór docelowy, jeśli zastąpiony z powodu SLTFILE(*ALL)	*W	Nie dotyczy	Nie dotyczy
	Zbiór docelowy, jeśli zastąpiony z powodu SLTFILE(*CHANGED)	*RW	Nie dotyczy	Nie dotyczy
	Każdy katalog w ścieżce, który poprzedza katalog źródłowy	*X	Nie dotyczy	Nie dotyczy
	Każdy katalog w ścieżce, który poprzedza katalog docelowy	*X	Nie dotyczy	Nie dotyczy
CPYOPT	Kopiowany katalog [5]	*R	Nie dotyczy	Nie dotyczy
	Kopiowany katalog, jeśli zawiera pozycje	*RX	Nie dotyczy	Nie dotyczy
	Katalog nadrzędny katalogu docelowego	*WX	Nie dotyczy	Nie dotyczy
	Katalog docelowy, jeśli jest zastępowany, bo SLTFILE(*ALL)	*W	Nie dotyczy	Nie dotyczy
	Katalog docelowy, jeśli jest zastępowany, bo SLTFILE(*CHANGED)	*RW	Nie dotyczy	Nie dotyczy
	Katalog docelowy, jeśli mają być utworzone pozycje	*WX	Nie dotyczy	Nie dotyczy

Tabela 150. (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienie		
		Obiekt	**Biblioteka.**	**Wolumin optyczny [1]**
CPYOPT	Zbiory źródłowe	*R	Nie dotyczy	Nie dotyczy
	Zbiór docelowy, jeśli zastąpiony z powodu SLTFILE(*ALL)	*W	Nie dotyczy	Nie dotyczy
	Zbiór docelowy, jeśli zastąpiony z powodu SLTFILE(*CHANGED)	*RW	Nie dotyczy	Nie dotyczy
CRTDEVOPT [4]	Urządzenie optyczne		*EXECUTE	
CVTOPTBKU	Urządzenie optyczne	*USE	*EXECUTE	*ALL
DSPOPT	Przedrostek ścieżki, gdy DATA (*SAVRST)[5]	*X	Nie dotyczy	Nie dotyczy
	Przedrostek zbioru, gdy (*SAVRST)[2]	*R	Nie dotyczy	Nie dotyczy
	Urządzenie optyczne	*EXECUTE	*USE	
	Serwer CSI	*USE	*EXECUTE	
DSPOPTLCK				
DSPOPTSVR	Serwer CSI	*USE	*EXECUTE	
DUPOPT	Urządzenie optyczne	*USE	*EXECUTE	*USE - wolumin źródłowy
				*ALL - wolumin docelowy
INZOPT	Katalog główny (/) woluminu	*RWX	Nie dotyczy	Nie dotyczy
	Urządzenie optyczne	*USE	*EXECUTE	*ALL
RCLOPT (Q)	Urządzenie optyczne	*USE	*EXECUTE	
RMVOPTCTG (Q)	Urządzenie optyczne	*USE	*EXECUTE	
RMVOPTSVR (Q)	Serwer CSI	*USE	*EXECUTE	
WRKHLDOPTF[2]	Urządzenie optyczne	*USE	*EXECUTE	*USE
	Serwer CSI	*USE	*EXECUTE	
WRKOPTDIR[2]	Urządzenie optyczne	*USE	*EXECUTE	*USE
	Serwer CSI	*USE	*EXECUTE	
WRKOPTF[2]	Urządzenie optyczne	*USE	*EXECUTE	*USE
	Serwer CSI	*USE	*EXECUTE	
WRKOPTVOL[2]	Urządzenie optyczne	*USE	*EXECUTE	

Tabela 150. (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienie		
		Obiekt	Biblioteka.	Wolumin optyczny [1]

[1] Woluminy optyczne nie są rzeczywistymi obiektami systemowymi. Dowiązanie między woluminem optycznym a listą autoryzacji używaną do ochrony obiektu jest utrzymywane przez funkcję obsługi nośników optycznych.

[2] Z poziomu programów użytkowych nośnika optycznego można wywołać siedem opcji, które same w sobie nie są komendami. Te opcje oraz wymagane przez nie uprawnienia do woluminu optycznego przedstawiono poniżej.

Usunięcie zbioru: *CHANGE

Zmiana nazwy zbioru: *CHANGE

Usunięcie katalogu: *CHANGE

Tworzenie katalogu: *CHANGE

Zmiana nazwy woluminu: *ALL

Zwolnienie zawieszonego zbioru optycznego: *CHANGE

Składowanie zawieszonych zbiorów optycznych: *USE - wolumin źródłowy, *Change - wolumin docelowy

[3] Aby zmienić listę autoryzacji używaną do zabezpieczania woluminu, użytkownik musi mieć uprawnienia do zarządzania listą autoryzacji do listy, która aktualnie zabezpiecza wolumin optyczny.

[4] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

[5] To sprawdzanie uprawnień przeprowadzane jest jedynie wtedy, kiedy nośnik optyczny jest w formacie UDF (Universal Disk Format).

Komendy kolejki wyjściowej

Komenda	Obiekt odniesienia	Parametry kolejki wyjściowej		Uprawnienie specjalne	Wymagane uprawnienie	
		AUTCHK	OPRCTL		Do obiektu	Do biblioteki
CHGOUTQ [1]	Kolejka danych				*READ	*EXECUTE
	Kolejka wyjściowa	*DTAAUT			*OBJMGT, *READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CLROUTQ [1]	Kolejka wyjściowa	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CRTOUTQ	Kolejka danych				*READ	*EXECUTE
	Kolejka wyjściowa					*READ, *ADD
DLTOUTQ	Kolejka wyjściowa				*OBJEXIST	*EXECUTE
HLDOUTQ [1]	Kolejka wyjściowa	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
PRTQAUT [4]						

Komenda	Obiekt odniesienia	Parametry kolejki wyjściowej		Uprawnienie specjalne	Wymagane uprawnienie	
		AUTCHK	OPRCTL		Do obiektu	Do biblioteki
RLSOUTQ [1]	Kolejka wyjściowa	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKOUTQ [1,3]	Kolejka wyjściowa				*READ	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKOUTQD [1,3]	Kolejka wyjściowa				*READ	*EXECUTE
			*YES	*JOBCTL		*EXECUTE

1 Jeśli użytkownik ma uprawnienia specjalne *SPLCTL, nie potrzebuje żadnych uprawnień do kolejki wyjściowej. Jednak musi mieć uprawnienie *EXECUTE do biblioteki, w której znajduje się kolejka wyjściowa.

2 Użytkownik musi być właścicielem kolejki wyjściowej.

3 Jeśli użytkownik zgłasza żądanie pracy z wszystkimi kolejkami wyjściowymi, wyświetlana lista obejmuje wszystkie kolejki wyjściowe znajdujące się w bibliotece, do których użytkownik ma uprawnienia *EXECUTE.

4 Do użycia tej komendy konieczne jest uprawnienie specjalne (*ALLOBJ).

Komendy pakietów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CRTSQLPKG	Program	*OBJOPR, *READ	*EXECUTE
	Pakiet SQL: REPLACE(*NO)		*OBJOPR, *READ, *ADD, *EXECUTE
	Pakiet SQL: REPLACE(*YES)	*OBJOPR, *OBJMGT, *OBJEXIST, *READ	*OBJOPR, *READ, *ADD, *EXECUTE
DLTSQLPKG	Pakiet	*OBJEXIST	*EXECUTE
PRTSQLINF	Pakiet	*OBJOPR, *READ	*EXECUTE
	Program	*OBJOPR, *READ	*EXECUTE
	Program usługowy	*OBJOPR, *READ	*EXECUTE
STRSQL			

Komendy wydajności

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ADDPEXDFN (Q) [5]	Biblioteka PGM		*EXECUTE

Komendy wydajności

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDPEXFTR (Q)[5]	Biblioteka PGMTRG		*EXECUTE
	Biblioteka PGMFTR		*EXECUTE
	Ścieżka JVAFTR	*X dla katalogu	
	Ścieżka PATHFTR	*X dla katalogu	
ANZACCGRP (Q) [4]	QPFR/QPTPAGA0 *PGM	*USE	*EXECUTE
	Biblioteka modelu		*EXECUTE, *ADD
	Opis zadania	*USE	*EXECUTE
	QPFR/QCYRBCPP *PGM	*USE	*EXECUTE
	QPFR/QCYMBREX *PGM	*USE	*EXECUTE
ANZBESTMDL (Q)[4]	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Biblioteki aplikacji, które zawierają analizowane zbiory bazy danych		*EXECUTE
	Opis zadania	*USE	*EXECUTE
ANZDBF (Q)[4]	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Opis zadania	*USE	*EXECUTE
ANZDBFKEY (Q)	QPFR/QPTANZKC *PGM	*USE	*EXECUTE
	Biblioteki aplikacji, które zawierają analizowane programy		*EXECUTE
	Opis zadania	*USE	*EXECUTE
ANZPGM (Q)	QPFR/QPTANZPC *PGM	*USE	*EXECUTE
	Dane dotyczące wydajności [2]		*ADD, *READ
ANZPFRDTA (Q)[4]	QPFR/QACVPP *PGM	*USE	*EXECUTE
	Dane dotyczące wydajności [2]		*ADD, *READ
ANZPFRDT2 (Q)[4]	QPFR/QAVCPP *PGM	*USE	*EXECUTE
	QAPTAPGP *FILE	*CHANGE	*EXECUTE
	Komenda DLTFCNARA (Q)	*USE	*EXECUTE
	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
CFGPFRCOL (Q)	Biblioteka kolekcji		*EXECUTE
CHGFCNARA (Q)	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE	*CHANGE	*EXECUTE
CHGGPHFMT (Q)	QPFR/QPGCRTFM *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE	*CHANGE	*EXECUTE
	QAPGGPHF *FILE	*USE	*EXECUTE
CHGGPHPKG (Q)	QPFR/QPGCRTPK *PGM	*USE	*EXECUTE
	QAPMDMPT *FILE	*CHANGE	*EXECUTE
CHGJOBTYP (Q)	QPFR/QPTCHGJT *PGM	*USE	*EXECUTE
CHGPEXDFN (Q)[5]	Biblioteka PGM		*EXECUTE
CHKPFRCOL (Q)			

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CPYFCNARA (Q)[4]	QPFR/QPTAGRPR *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE w ″Z″ biblioteki	*USE	*EXECUTE
	″Do″ biblioteki (jeśli QAPGGPHF *FILE nie istnieje)		*EXECUTE, *ADD
	QAPGGPHF *FILE w ″Do″ biblioteki (podczas dodawania nowego formatu wykresu lub zastępowania istniejącego)	*CHANGE	*EXECUTE
CPYGPHFMT (Q)[4]	QPFR/QPGCPYGP *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE w ″Z″ biblioteki	*USE	*EXECUTE
	″Do″ biblioteki (jeśli QAPGPKGF *FILE nie istnieje)		*EXECUTE, *ADD
	QAPGPKGF *FILE w ″Do″ biblioteki (podczas dodawania nowego pakietu wykresu lub zastępowaniy istniejącego)	*CHANGE	*EXECUTE
	QAPGGPHF *FILE w ″Do″ biblioteki (podczas dodawania nowego pakietu wykresu lub zastępowania istniejącego)	*USE	*EXECUTE
CPYGPHPKG (Q)	QPFR/QPGCPYGP *PGM	*USE	*EXECUTE
	Z biblioteki		*EXECUTE
	Do biblioteki		*EXECUTE, *ADD
	Opis zadania	*USE	*EXECUTE
CPYPFRDTA (Q)	QPFR/QITCPYCP *PGM	*USE	*EXECUTE
	Dane dotyczące wydajności (wszystkie zbiory QAPM*)	*USE	*EXECUTE
	Biblioteka modelu		*EXECUTE, *ADD
	Opis zadania	*USE	*EXECUTE
	QPFR/QCYCBMCP *PGM	*USE	*EXECUTE
	QPFR/QCYCBMDL *PGM	*USE	*EXECUTE
	QPFR/QCYOPDBS *PGM	*USE	*EXECUTE
	QPFR/QCYCLIDS *PGM	*USE	*EXECUTE
CRTBESTMDL (Q)	QPFR/QCYCAPT *PGM	*USE	*EXECUTE
	Biblioteka, w której tworzony jest obszar funkcjonalny		*EXECUTE, *ADD
	QAPTAPGP *FILE w bibliotece docelowej (jeśli dodawany jest nowy obszar funkcjonalny)	*CHANGE	*EXECUTE
CRTFCNARA (Q)	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
	Biblioteka, w której tworzony jest format wykresu		*EXECUTE, *ADD
	QAPGGPHF *FILE w bibliotece docelowej (jeśli dodawany jest nowy format wykresu)	*CHANGE	*EXECUTE
CRTGPHFMT (Q)	QPFR/QPGCRTFM *PGM	*USE	*EXECUTE
	Biblioteka, w której tworzony jest pakiet wykresu		*EXECUTE, *ADD
	QAPGGPHF *FILE	*CHANGE	*EXECUTE
	QAPGPKGF *FILE w bibliotece docelowej (jeśli dodawany jest nowy pakiet wykresu)	*USE	*EXECUTE

Komendy wydajności

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTGPHPKG (Q)	QPFR/QPGCRTPK *PGM	*USE	*EXECUTE
	Biblioteka, w której tworzone są dane historyczne		*ADD, *READ
	Opis zadania	*USE	*EXECUTE
CRTHSTDTA (Q)	QPFR/QPGCRTHS *PGM	*USE	*EXECUTE
	Do biblioteki		*ADD, *READ
CRTPEXDTA (Q)[5]	Biblioteka *MGTCOL		*EXECUTE
	Biblioteka danych [1]		*READ, *ADD[2]
CRTPFRDTA (Q)	Z biblioteki		*EXECUTE
	Do biblioteki		*ADD, *READ
	Z biblioteki		*USE
CVTPFRDTA (Q)	Opis zadania	*USE	*EXECUTE
CVTPFRTHD (Q)	Dane dotyczące wydajności [2]		*ADD, *READ
	Biblioteka modelu		*EXECUTE, *ADD
	QPFR/QCYDBMDL *PGM	*USE	*EXECUTE
	QPFR/QCYCVTBD *CMD	*USE	*EXECUTE
DLTBESTMDL (Q)[4]	QPFR/QCYCBTOD *PGM	*USE	*EXECUTE
	QAPTAPGP *FILE w bibliotece obszaru funkcjonalnego	*CHANGE	*EXECUTE
DLTFCNARA (Q)[4]	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE w bibliotece formatu wykresu	*CHANGE	*EXECUTE
DLTGPHFMT (Q)[4]	QPFR/QPGDLTGP *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE w bibliotece pakietu wykresu	*CHANGE	*EXECUTE
DLTGPHPKG (Q)[4]	QPFR/QPGDLTGP *PGM	*USE	*EXECUTE
	QAPGHSTD *FILE w bibliotece danych historycznych	*CHANGE	*EXECUTE
	QAPGHSTI *FILE w bibliotece danych historycznych	*CHANGE	*EXECUTE
	QAPGSUMD *FILE w bibliotece danych historycznych	*CHANGE	*EXECUTE
DLTHSTDTA (Q)[4]	QPFR/QPGDLTHS *PGM	*USE	*EXECUTE
DLTPEXDTA (Q)[5]	Biblioteka danych [1]		*EXECUTE, *DELETE [2]
DLTPFRDTA (Q)[4]	QPFR/QPTDLTCP *PGM	*USE	*EXECUTE
DMPTRC (Q)[5]	Biblioteka, w której przechowywane są dane śledzenia		*EXECUTE, *ADD
	Zbiór wyjściowy (QAPTPAGD)	*CHANGE	*EXECUTE, *ADD

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
DSPACCGRP (Q)[4]	QPFR/QPTPAGD0 *PGM	*USE	*EXECUTE
	Format lub biblioteka pakietu		*EXECUTE
	Biblioteka danych historycznych		*EXECUTE
	Biblioteka zbioru wyjściowego		*EXECUTE, *ADD
	Kolejka wyjściowa	*USE	*EXECUTE
	Opis zadania	*USE	*EXECUTE
DSPHSTGPH (Q)[4]	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Biblioteka danych historycznych		*EXECUTE
DSPPFRDTA (Q) [4]	QPFR/QAVCPP *PGM	*USE	*EXECUTE
	Format lub biblioteka pakietu		*EXECUTE
	Dane dotyczące wydajności [2]		*EXECUTE
	Biblioteka zbioru wyjściowego		*EXECUTE, *ADD
	Kolejka wyjściowa	*USE	*EXECUTE
	Opis zadania	*USE	*EXECUTE
DSPPFRGPH (Q)[4]	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Biblioteka zbioru wyjściowego		*EXECUTE
	Opis zadania	*USE	*EXECUTE
ENDJOBTRC (Q)[4]	QPFR/QPTTRCJ0 *PGM	*USE	*EXECUTE
ENDPEX (Q)[5]	Biblioteka danych [1]		*READ, *ADD [2]
ENDPFRCOL (Q)			
PRTACTRPT (Q)[4]	QPFR/QITPRTAC *PGM	*USE	*EXECUTE
	Dane dotyczące wydajności [2]	*USE	*ADD, *READ
	Opis zadania	*USE	*EXECUTE
PRTCPTRPT (Q)[4]	QPFR/QPTCPTRP *PGM	*USE	*EXECUTE
	Dane dotyczące wydajności [2]		*ADD, *READ
	Opis zadania	*USE	*EXECUTE
PRTJOBRPT (Q)[4]	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	Dane dotyczące wydajności [2]		*ADD, *READ
	Opis zadania	*USE	*EXECUTE
PRTJOBTRC (Q)[4]	QPFR/QPTTRCRP *PGM	*USE	*EXECUTE
	Biblioteka pliku śledzenia zadania (QAPTTRCJ)		*EXECUTE
	Opis zadania	*USE	*EXECUTE
PRTLCKRPT (Q)[4]	QPFR/QPTLCKQ *PGM	*USE	*EXECUTE
PRTPEXRPT[5]	Biblioteka danych [1]		*EXECUTE[2]
	Zbiór wyjściowy	*USE	*EXECUTE, *ADD
	QPFR/QVPEPRTC *PGM	*USE	*EXECUTE
	QPFR/QVPESVGN *SRVPGM	*USE	*EXECUTE
	QPFR/QYPESVGN *SRVPGM	*USE	*EXECUTE

Komendy wydajności

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
PRTPOLRPT (Q)[4]	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	Dane dotyczące wydajności [2]		*ADD, *READ
	Opis zadania	*USE	*EXECUTE
PRTRSCRPT (Q)[4]	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	Dane dotyczące wydajności [2]		*ADD, *READ
	Opis zadania	*USE	*EXECUTE
PRTSYSRPT (Q)[4]	QPFR/QPTTNSRP *PGM	*USE	*EXECUTE
	QAPMDMPT *FILE		*EXECUTE
	Opis zadania	*USE	*EXECUTE
PRTTNSRPT (Q)[4]	QPFR/QPTTNSRP *PGM	*USE	*EXECUTE
	Biblioteka pliku śledzenia (QTRJOBT)		*EXECUTE
	Opis zadania	*USE	*EXECUTE
PRTTRCRPT (Q)[4]	QPFR/QPTTRCCP *PGM	*USE	*EXECUTE
RMVPEXDFN (Q)[5]			
RMVPEXFTR (Q)[5]			
STRBEST (Q)[4]	QPFR/QCYBMAIN *PGM	*USE	*EXECUTE
STRDBMON[3, 4]	Zbiór wyjściowy	*OBJOPR, *ADD	*EXECUTE
STRJOBTRC (Q)	QPFR/QPTTRCJ1 *PGM	*USE	*EXECUTE
STRPEX (Q)[5]			
STRPFRCOL (Q)			
STRPFRG (Q)[4]	QPFR/QPGSTART *PGM	*USE	*EXECUTE
STRPFRT (Q)[4]	QPFR/QMNMAIN0 *PGM	*USE	*EXECUTE
	QAPTAPGP *FILE w bibliotece obszarów funkcjonalnego	*CHANGE	*EXECUTE
	Komenda CHGFCNARA (Q)	*USE	*EXECUTE
	Komenda CPYFCNARA (Q)	*USE	*EXECUTE
	Komenda CRTFCNARA (Q)	*USE	*EXECUTE
	Komenda DLTFCNARA (Q)	*USE	*EXECUTE
	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QPFR/QPTAGRPR *PGM	*USE	*EXECUTE
WRKFCNARA (Q)[4]	QPFR/QPTAGRPC *PGM	*USE	*EXECUTE
	Zbiór wyjściowy (QAITMON)	*CHANGE, *ALTER	*EXECUTE, *ADD
WRKPEXDFN (Q)[5]			
WRKPEXFTR (Q)[5]			
WRKSYSACT (Q)[3, 4]	QPFR/QITMONCP *PGM	*USE	*EXECUTE
Te komendy nie wymagają żadnych uprawnień do obiektu: • ENDDBMON[3] • ENDPFRTRC (Q) • STRPFRTRC (Q)			

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**

[1] Jeśli podano bibliotekę domyślną (QPEXDATA), uprawnienia do tej biblioteki nie są sprawdzane.

[2] Wymagane są uprawnienia do biblioteki zawierającej zestaw zbiorów bazy danych. Uprawnienia do pojedynczych zestawów zbiorów bazy danych nie są sprawdzane.

[3] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *JOBCTL.

[4] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *SERVICE.

[5] Aby użyć tej komendy, użytkownik musi mieć uprawnienie specjalne *SERVICE lub uprawnienie do używania funkcji śledzenia serwisowego Operating System/400 w Administrowaniu aplikacjami w programie iSeries Navigator. Komenda Zmiana użycia funkcji (Change Function Usage - QSYCHFUI), o identyfikatorze QIBM_SERVICE_TRACE, może być stosowana do zmiany listy użytkowników uprawnionych do wykonania operacji śledzenia.

Komendy grupy deskryptorów wydruków

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGPDGPRF	Profil użytkownika	*OBJMGT	
CRTPDG	Grupa deskryptorów wydruków		*READ, *ADD
DLTPDG	Grupa deskryptorów wydruków	*OBJEXIST	*EXECUTE
DSPPDGPRF	Profil użytkownika	*OBJMGT	
RTVPDGPRF	Profil użytkownika	*READ	

Komendy konfiguracji Print Services Facility

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGPSFCFG [1, 2]			
CRTGPSFCFG [1, 2]			*READ, *ADD
DLTPSFCFG [1, 2]	Konfiguracja PSF	*OBJEXIST	*EXECUTE
DSPPSFCFG [1]	Konfiguracja PSF	*USE	*EXECUTE
WRKPSFCFG [1]	Konfiguracja PSF	*READ	*EXECUTE

[1] Do korzystania z tej komendy wymagana jest opcja PSF/400.

[2] Aby używać tej komendy, niezbędne jest uprawnienie specjalne *IOSYSCFG.

Komendy problemów

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDPRBACNE (Q)	Filtr	*USE, *ADD	*EXECUTE

Komendy problemów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDPRBSLTE (Q)	Filtr	*USE, *ADD	*EXECUTE
ANZPRB (Q)	Komenda SNDSRVRQS	*USE	*EXECUTE
CHGPRB (Q)			*EXECUTE
CHGPRBACNE (Q)	Filtr	*USE, *UPD	*EXECUTE
CHGPRBSLTE (Q)	Filtr	*USE, *UPD	*EXECUTE
DLTPRB (Q) [3]	Komenda: DLTAPARDTA	*USE	*EXECUTE
DSPPRB	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
PTRINTDTA (Q)			
QRYPRBSTS (Q)			
VFYCMN (Q)	Opis linii [1]	*USE	*EXECUTE
	Opis kontrolera [1]	*USE	*EXECUTE
	ID sieci [1]	*USE	*EXECUTE
VFYOPT (Q)	Opis urządzenia	*USE	*EXECUTE
VFYTAP[4] (Q)	Opis urządzenia	*USE, *OBJMGT	*EXECUTE
VFYPRT (Q)	Opis urządzenia	*USE	*EXECUTE
WRKPRB (Q) [2]	Linia, kontroler, NWID (ID sieci) i urządzenie - na podstawie analizy problemu	*USE	*EXECUTE

1 Do sprawdzanego obiektu komunikacyjnego wymagane są uprawnienia *USE.

2 Aby wydrukować problem, użytkownik musi mieć uprawnienia *USE do komendy SNDSRVRQS.

3 Jeśli związane z problemem dane APAR także mają być usunięte, użytkownik musi mieć uprawnienia do komendy DLTAPARDTA. Aby określić wymagane dodatkowe uprawnienia, należy sprawdzić pozycję DLTAPARDTA w tabeli Komendy usług - Wymagane uprawnienia.

4 Gdy opis urządzenia jest przydzielany przez urządzenie biblioteki nośników, użytkownik musi mieć uprawnienie specjalne *IOSYSCFG.

Komendy programów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
Uprawnienia do obiektów wymagane dla komend CRT*xxx*PGM znajdują się w tabeli Język w temacie “Komendy języka” na stronie 375.			
ADDBKP [1]	Punkt zatrzymania programu obsługi	*USE	*EXECUTE
ADDPGM [1,2]	Program	*CHANGE	*EXECUTE
ADDTRC [1]	Śledzenie programu obsługi	*USE	*EXECUTE
CALL	Program	*OBJOPR, *EXECUTE	*EXECUTE
	Program usługowy [4]	*EXECUTE	*EXECUTE
CHGDBG	Debugowanie	*USE, *ADD, *DLT	*EXECUTE
CHGHLLPTR [1]			

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGPGM	Program	*OBJMGT, *USE	*USE
	Program, jeśli podano opcję ponownego tworzenia, zmieniono poziom optymalizacji lub zmieniono kolekcję danych o wydajności	*OBJMGT, *USE	*USE, *ADD, *DLT
	Program, jeśli zmieniany jest parametr USRPRF lub USEADPAUT	Właściciel [7]	*USE, *ADD, *DLT
CHGPGMVAR [1]			
CHGPTR [1]			
CHGSRVPGM	Program usługowy	*OBJMGT, *USE	*USE
	Program usługowy, jeśli podano opcję ponownego tworzenia, zmieniono poziom optymalizacji lub zmieniono kolekcję danych o wydajności	*OBJMGT, *USE	*USE, *ADD, *DLT
	Program usługowy, jeśli zmieniany jest parametr USRPRF lub USEADPAUT	Właściciel [7], *USE, *OBJMGT	*USE, *ADD, *DLT
CLRTRCDTA [1]			
CRTPGM	Program, Replace(*NO)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Program, Replace(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Program usługowy podany w parametrze BNDSRVPGM.	*USE	*EXECUTE
	Moduł	*USE	*EXECUTE
	Katalog konsolidacji	*USE	*EXECUTE
CRTSRVPGM	Program usługowy, Replace(*NO)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Program usługowy, Replace(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Moduł	*USE	*EXECUTE
	Program usługowy podany w parametrze BNDSRVPGM.	*USE	*EXECUTE
	Zbiór źródłowy eksportu	*OBJOPR *READ	*EXECUTE
	Katalog konsolidacji	*USE	*EXECUTE
CVTCLSRC	Źródłowy zbiór	*USE	*EXECUTE
	Docelowy zbiór	*OBJOPR, *OBJMGT, *USE, *ADD, *DLT	*READ, *ADD
DLTDFUPGM	Program	*OBJEXIST	*EXECUTE
	Zbiór ekranowy	*OBJEXIST	*EXECUTE
DLTPGM	Program	*OBJEXIST	*EXECUTE
DLTSRVPGM	Program usługowy	*OBJEXIST	*EXECUTE
DMPCLPGM	Program CL	*USE	Brak [3]
DSPBKP [1]			

Komendy programów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
DSPDBG [1]			
DSPDBGWCH			
DSPMODSRC[2, 4]	Zbiór źródłowy	*USE	*USE
	Dowolne zbiory włączane	*USE	*USE
	Program	*CHANGE	*EXECUTE
DSPPGM	Program	*READ	*EXECUTE
	Program, jeśli podano DETAIL(*MODULE)	*USE	*EXECUTE
DSPPGMREF	Program	*OBJOPR	*EXECUTE
	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
DSPPGMVAR [1]			
DSPSRVPGM	Program usługowy	*READ	*EXECUTE
	Program usługowy, jeśli podano DETAIL(*MODULE)	*USE	*EXECUTE
DSPTRC [1]			
DSPTRCDTA [1]			
ENDCBLDBG (program licencjonowany COBOL/400 lub środowisko S/38)	Program	*CHANGE	*EXECUTE
ENDDBG [1]	Program debugowania źródła	*USE	*USE
ENDRQS [1]			*EXECUTE
ENTCBLDBG (środowisko S/38)	Program	*CHANGE	*EXECUTE
EXTPGMINF	Zbiór źródłowy i zbiory bazy danych	*OBJOPR	*EXECUTE
	Informacje o programie		*READ, *ADD
PRTCMDUSG	Program	*USE	*EXECUTE
RMVBKP [1]			
RMVPGM [1]			
RMVTRC [1]			
RSMBKP [1]			
RTVCLSRC	Program	*OBJMGT, *USE	*EXECUTE
	Zbiór źródłowy bazy danych	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
SETATNPGM	program obsługi klawisza ATTN	*EXECUTE	*EXECUTE
SETPGMINF	zbiory baz danych,	*OBJOPR	*EXECUTE
	Zbiór źródłowy	*USE	*EXECUTE
	Program główny	*CHANGE	*READ, *ADD
	Podprogram	*USE	*EXECUTE
STRCBLDBG	Program	*CHANGE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
STRDBG	Program [2]	*CHANGE	*EXECUTE
	Zbiór źródłowy [4]	*USE	*EXECUTE
	Dowolne zbiory włączane [4]	*USE	*EXECUTE
	Program debugowania źródła	*USE	*EXECUTE
	Program niemonitorowanych komunikatów	*USE	*EXECUTE
TFRCTL [4]	Program	*USE lub uprawnienia do danych inne niż *EXECUTE	*EXECUTE
	Niektóre funkcje języka podczas korzystania z języków wysokiego poziomu	*READ	*EXECUTE
UPDPGM	Program	*OBJMGT, *OBJEXIST, *USE	*USE, *ADD
	Program usługowy podany w parametrze BNDSRVPGM.	*USE	*EXECUTE
	Moduł	*USE	*EXECUTE
	Katalog konsolidacji	*USE	*EXECUTE
UPDSRVPGM	Program usługowy	*OBJMGT, *OBJEXIST, *USE	*USE, *ADD
	Program usługowy podany w parametrze BNDSRVPGM.	*USE	*EXECUTE
	Moduł	*USE	*EXECUTE
	Katalog konsolidacji	*USE	*EXECUTE
	Zbiór źródłowy eksportu	*OBJOPR *READ	*EXECUTE
WRKPGM [6]	Program	Dowolne uprawnienia	*USE
WRKSRVPGM [6]	Program usługowy	Dowolne uprawnienia	*USE

1 Kiedy program jest w trybie debugowania, nie są wymagane dalsze uprawnienia do komend debugowania.

2 Jeśli użytkownik ma uprawnienia specjalne *SERVICE, do programu wymagane są jedynie uprawnienia *USE.

3 Komenda DMPCLPGM jest zgłaszana z programu CL, który jest już uruchomiony. Ponieważ uprawnienia do biblioteki zawierającej program sprawdzane są w momencie wywoływania programu, nie są sprawdzane podczas uruchamiania komendy DMPCLPGM.

4 Dotyczy tylko programów ILE.

5 Więcej informacji na temat wymagań dotyczących ochrony dla instrukcji SQL znajduje się w temacie Authorization, privileges and object ownership (Autoryzacja, przywileje i prawo własności do obiektów) w podręczniku SQL Reference (znajdującym się w Centrum informacyjnym iSeries).

6 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

7 Użytkownik musi mieć prawo własności do programu lub uprawnienia specjalne *ALLOBJ i *SECADM.

Komendy zapytań

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ANZQRY	Definicja zapytania	*USE	*EXECUTE

Komendy zapytań

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGQRYA[4]			
CRTQMFORM	Formularz menedżera zapytań: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Formularz menedżera zapytań: REPLACE(*YES)	*ALL	*READ, *ADD, *EXECUTE
	Zbiór źródłowy	*USE	*EXECUTE
CRTQMQRY	Zapytanie menedżera zapytań: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Zapytanie menedżera zapytań: REPLACE(*YES)	*ALL	*READ, *ADD, *EXECUTE
	Zbiór źródłowy	*USE	*EXECUTE
	Komenda OVRDBF	*USE	*EXECUTE
DLTQMFORM	Formularz menedżera zapytań	OBJEXIST	*EXECUTE
DLTQMQRY	Zapytanie menedżera zapytań	*OBJEXIST	*EXECUTE
DLTQRY	Definicja zapytania	*OBJEXIST	*EXECUTE
RTVQMFORM	Formularz menedżera zapytań	*OBJEXIST	*EXECUTE
	Docelowy zbiór źródłowy	*ALL	*READ, *ADD, *EXECUTE
	Komendy ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, OVRDBF, RMVM	*USE	*EXECUTE
RTVQMQRY	Zapytanie menedżera zapytań	*USE	*EXECUTE
	Docelowy zbiór źródłowy	*ALL	*READ, *ADD
	Komendy ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, OVRDBF, RMVM	*USE	*EXECUTE
RUNQRY	Definicja zapytania	*USE	*USE
	Zbiory wejściowe	*USE	*EXECUTE
	Zbiory wyjściowe	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
STRQMQRY [1]	Zapytanie menedżera zapytań	*USE	*EXECUTE
	Formularz menedżera zapytań, jeśli podano	*USE	*EXECUTE
	Definicja zapytania, jeśli podano	*USE	*EXECUTE
	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Komendy ADDPFM, CHGOBJD, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, GRTOBJAUT OVRDBF, OVRPRTF RMVM (jeśli podano parametr OUTPUT(*OUTFILE))	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
STRQMPRC [1]	Zbiór źródłowy zawierający procedurę menedżera zapytań	*USE	*EXECUTE
	Zbiór źródłowy zawierający zbiór źródłowy komendy, jeśli podano	*USE	*EXECUTE
	Komenda OVRPRTF, jeśli instrukcje powodują drukowanie lub powstanie obiektu zapytania.	*USE	*EXECUTE
STRQRY			*EXECUTE
WRKQMFORM [3]	Formularz menedżera zapytań	Dowolne uprawnienia	*USE
WRKQMQRY [3]	Zapytanie menedżera zapytań	Dowolne uprawnienia	*USE
WRKQRY [3]			

1 Aby uruchomić komendę STRQM, użytkownik musi mieć uprawnienia wymagane przez instrukcje w zapytaniu. Na przykład, aby do tabeli wstawić wiersz wymagane są uprawnienia *OBJOPR, *ADD, i *EXECUTE do tej tabeli.

2 Wymagane jest prawo własności lub niektóre uprawnienia do obiektu.

3 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez pojedyncze operacje.

4 Aby korzystać z pojedynczych komend, użytkownik musi mieć uprawnienia specjalne *JOBCTL.

Komendy interpretera powłoki QSH

Te komendy nie wymagają żadnych uprawnień do obiektów:
STRQSH [1] [2] QSH[1] [2]

1 QSH jest aliasem dla komendy CL STRQSH.

2 Użytkownik musi mieć uprawnienie *X do wszystkich skryptów i do wszystkich katalogów w ścieżce do skryptu.

Komendy pytań i odpowiedzi

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ANSQST (Q)	Zbiór bazy danych QAQA*xx*BQPY [1]	*READ	*READ
ASKQST	Zbiór bazy danych QAQA*xx*BBPY [1] or QAQA*xx*BQPY [1]	*READ	*READ
CHGQSTDB (Q)	Zbiór bazy danych QAQA*xx*BQPY [1]	*READ	*READ
CRTQSTDB [2] (Q)	zbiory baz danych,		*READ, *ADD, *EXECUTE
CRTQSTLOD (Q)	Zbiór bazy danych QAQA*xx*BQPY [1]	*READ	*READ
DLTQST (Q)	Zbiór bazy danych QAQA*xx*BQPY [1]	*READ	*READ
DLTQSTDB (Q)	Zbiór bazy danych QAQA*xx*BQPY [1]	*READ	*READ

Komendy pytań i odpowiedzi

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
EDTQST (Q)	Zbiór bazy danych QAQA*xx*BQPY [1]	*READ	*READ
LODQSTDB [2] (Q)	Zbiór bazy danych QAQA*xx*BQPY [1,3]	*READ	*READ, *ADD, *EXECUTE
STRQST [4]	Zbiór bazy danych QAQA*xx*BBPY [1] or QAQA*xx*BQPY [1]	*READ	*READ
WRKQST	Zbiór bazy danych QAQA*xx*BBPY [1] lub QAQA*xx*BQPY [1]	*READ	*USE
WRKCNTINF			*EXECUTE

1 Część “xx” nazwy zbioru to indeks bazy danych pytań i odpowiedzi, na której działa komenda. Indeks składa się z dwucyfrowej liczby z zakresu od 00 do 99. Aby uzyskać indeks dla danej bazy danych pytań i odpowiedzi, należy użyć komendy WRKCNTINF.

2 Profil użytkownika, który uruchomił komendę staje się właścicielem nowo utworzonych zbiorów, chyba że parametr OWNER profilu użytkownika ma wartość *GRPPRF. Uprawnienie publiczne dla nowych zbiorów, oprócz QAQA*xx*BBPY, otrzymuje wartość *EXCLUDE. Uprawnienie publiczne dla QAQA*xx*BBPY otrzymuje wartość *READ.

3 Uprawnienia do zbioru wymagane są jedynie podczas ładowania poprzedniej bazy danych pytań i odpowiedzi.

4 Komenda wyświetla menu pytań i odpowiedzi. Aby korzystać z pojedynczych opcji, użytkownik musi mieć odpowiednie dla nich uprawnienia.

Komendy programu czytającego

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
STRDBRDR	Kolejka komunikatów	*OBJOPR, *ADD	*EXECUTE
	Zbiór bazy danych	*OBJOPR, *USE	*EXECUTE
	Kolejka zadań	*READ	*EXECUTE
STRDKTRDR	Kolejka komunikatów	*OBJOPR, *ADD	*EXECUTE
	Kolejka zadań	*READ	*EXECUTE
	Opis urządzenia	*OBJOPR, *READ	*EXECUTE
Te komendy nie wymagają żadnych uprawnień do obiektów:			
ENDRDR [1]	HLDRDR [1]	RLSRDR [1]	

1 Użytkownik musi uruchomić program czytający lub musi mieć uprawnienia specjalne do wszystkich obiektów (*ALLOBJ) lub do sterowania zadaniem (*JOBCTL).

Komendy narzędzia do rejestracji

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDEXITPGM (Q)			

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
RMVEXITPGM (Q)			
WRKREGINF			

Komendy relacyjnej bazy danych

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ADDRDBDIRE	Zbiór wyjściowy, jeśli został podany	*EXECUTE	*EXECUTE
CHGRDBDIRE	Zbiór wyjściowy, jeśli został podany	*EXECUTE	*EXECUTE
	Opis urządzenia miejsca zdalnego[7]	*CHANGE	
DSPRDBDIRE	Zbiór wyjściowy, jeśli został podany	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
Te komendy nie wymagają żadnych uprawnień do obiektów:			
RMVRDBDIRE WRKRDBDIRE			
[1] Uprawnienia zweryfikowane podczas używania pozycji katalogu RDB.			

Komendy zasobów

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
DSPHDWRSC			
DSPSFWRSC	Zbiór wyjściowy, jeśli został podany	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
EDTDEVRSC			
WRKHDWRSC [1]			
[1] Jeśli używana jest opcja tworzenia obiektu konfiguracyjnego, użytkownik musi mieć uprawnienia do używania odpowiedniej komendy CRT.			

Komendy RJE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ADDFCTE	Tabela sterująca formularzy	*DELETE, *USE, *ADD	*READ, *EXECUTE
	Zbiór urządzenia [1,2]	*USE	*READ, *EXECUTE
	Zbiór fizyczny [1,2] (RJE generuje podzbiory)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Zbiór fizyczny [1,2] (podano podzbiór)	*USE, *ADD	*READ, *EXECUTE
	Program [1,2]	*USE	*READ, *EXECUTE
	Kolejka komunikatów [1,2]	*USE, *ADD	*READ, *EXECUTE
	Profil użytkownika QUSER	*USE	*READ, *EXECUTE
ADDRJECMNE	Opis sesji	*USE, *ADD, *DLT	*READ, *EXECUTE
	Zbiór BSC/CMN [1,2]	*USE	*READ, *EXECUTE
	Opis urządzenia [2]	*USE	*READ, *EXECUTE
	Profil użytkownika QUSER	*USE	*READ, *EXECUTE
ADDRJERDRE	Opis sesji	*READ, *ADD, *DLT	*READ, *EXECUTE
	Kolejka zadań[2]	*READ	*READ, *EXECUTE
	Kolejka komunikatów[2]	*READ, *ADD	*READ, *EXECUTE
ADDRJEWTRE	Opis sesji	*READ, *ADD, *DLT	*READ, *EXECUTE
	Zbiór urządzenia [1,2]	*USE	*READ, *EXECUTE
	Zbiór fizyczny [1,2] (RJE generuje podzbiory)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Zbiór fizyczny [1,2] (podano podzbiór)	*OBJOPR, *ADD	*READ, *EXECUTE
	Program [1,2]	*USE	*READ, *EXECUTE
	Kolejka komunikatów [1,2]	*USE, *ADD	*READ, *EXECUTE
	Profil użytkownika QUSER	*USE	*READ, *EXECUTE
CHGFCT	Tabela sterująca formularzy	*OBJOPR, *OBJMGT	*READ, *EXECUTE
CHGFCTE	Tabela sterująca formularzy	*USE	*READ, *EXECUTE
	Zbiór urządzenia [1,2]	*USE	*READ, *EXECUTE
	Zbiór fizyczny [1,2] (RJE generuje podzbiory)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Zbiór fizyczny [1,2] (podano podzbiór)	*USE, *ADD	*READ, *EXECUTE
	Program [1,2]	*USE	*READ, *EXECUTE
	Kolejka komunikatów [1,2]	*USE, *ADD	*READ, *EXECUTE
	Profil użytkownika QUSER	*USE	*READ, *EXECUTE
CHGRJECMNE	Opis sesji	*USE	*READ, *EXECUTE
	Zbiór BSC/CMN [1,2]	*USE	*READ, *EXECUTE
	Opis urządzenia [2]	*USE	*READ, *EXECUTE
	Profil użytkownika QUSER	*USE	*READ, *EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGRJERDRE	Opis sesji	*USE, *ADD, *DLT	*READ, *EXECUTE
	Kolejka zadań[2]	*USE	*READ, *EXECUTE
	Kolejka komunikatów[2]	*USE, *ADD	*READ, *EXECUTE
CHGRJEWTRE	Opis sesji	*USE	*READ, *EXECUTE
	Zbiór urządzenia [1,2]	*USE	*READ, *EXECUTE
	Zbiór fizyczny [1,2] (RJE generuje podzbiory)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Zbiór fizyczny [1,2] (podano podzbiór)	*OBJOPR, *ADD	*READ, *EXECUTE
	Program [1,2]	*USE	*READ, *EXECUTE
	Kolejka komunikatów [1,2]	*USE, *ADD	*READ, *EXECUTE
	Profil użytkownika QUSER	*USE	*READ, *EXECUTE
CHGSSND	Opis sesji	*OBJMGT, *READ, *UPD, *OBJOPR	*EXECUTE, *READ
	Kolejka zadań [1,2]	*USE	*EXECUTE
	Kolejka komunikatów [1,2]	*USE, *ADD	*EXECUTE
	Tabela sterująca formularzy [1,2]	*USE	*EXECUTE
	Profil użytkownika QUSER	*USE	*EXECUTE
CNLRJERDR	Opis sesji	*USE	*EXECUTE
	Kolejka komunikatów	*USE, *ADD	*EXECUTE
CNLRJEWTR	Opis sesji	*USE	*EXECUTE
	Kolejka komunikatów	*USE, *ADD	*EXECUTE
CRTFCT	Tabela sterująca formularzy		*READ, *ADD
CRTRJEBSCF	Zbiór BSC		*READ, *EXECUTE, *ADD
	Źródłowy zbiór fizyczny (DDS)	*READ	*EXECUTE
	Opis urządzenia	*READ	*EXECUTE
CRTRJECFG	Opis sesji		*READ, *ADD, *UPD, *OBJOPR
	Kolejka zadań		*READ, *ADD
	Opis zadania		*READ, *OBJOPR, *ADD
	Opis podsystemu		*READ, *OBJOPR, *ADD
	Kolejka komunikatów		*READ, *ADD
	Zbiór CMN		*READ, *EXECUTE, *ADD
	Zbiór BSC		*READ, *EXECUTE, *ADD
	Zbiór drukarkowy		*USE, *ADD

Komendy zadań uruchamianych zdalnie (Remote Job Entry - RJE)

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTRJECFG	Zbiór fizyczny		*EXECUTE, *ADD
	Profil użytkownika QUSER [3]	*USE	*EXECUTE
	Kolejka wyjściowa	*READ	*EXECUTE
	Tabela sterująca formularzy	*READ	*READ
	Opis urządzenia		*EXECUTE
	Opis kontrolera		*EXECUTE
	Opis linii		*EXECUTE
CRTRJECMNF	Zbiór komunikacyjny		*READ, *EXECUTE, *ADD
	Źródłowy zbiór fizyczny (DDS)	*READ	*EXECUTE
	Opis urządzenia	*READ	*EXECUTE
CRTSSND	Opis sesji		*READ, *ADD, *UPD, *OBJOPR
	Kolejka zadań [1,2]	*USE	*EXECUTE
	Kolejka komunikatów [1,2]	*USE, *ADD	*EXECUTE
	Tabela sterująca formularzy [1,2]	*USE	*EXECUTE
	Profil użytkownika QUSER	*USE	*EXECUTE
CVTRJEDTA	Tabela sterująca formularzy	*USE	*EXECUTE
	Zbiór wejściowy	*USE, *UPD	*EXECUTE
	Zbiór wyjściowy (RJE generuje podzbiór)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Zbiór wyjściowy (podano podzbiór)	*USE, *ADD	*EXECUTE
DLTFCT	Tabela sterująca formularzy	*OBJEXIST	*EXECUTE
DLTRJECFG	Opis sesji	*OBJEXIST	*EXECUTE
	Kolejka zadań	*OBJEXIST	*EXECUTE
	Zbiór BSC/CMN	*OBJEXIST, *OBJOPR	*EXECUTE
	Zbiór fizyczny	*OBJEXIST, *OBJOPR	*EXECUTE
	Zbiór drukarkowy	*OBJEXIST, OBJOPR	*EXECUTE
	Kolejka komunikatów	*OBJEXIST, *USE, *DLT	*EXECUTE
	Opis zadania	*OBJEXIST	*EXECUTE
	Opis podsystemu	*OBJEXIST, *USE	*EXECUTE
	Opis urządzenia [4]	*OBJEXIST	*EXECUTE
	Opis kontrolera [4]	*OBJEXIST	*EXECUTE
	Opis linii [4]	*OBJEXIST	*EXECUTE
DLTSSND	Opis sesji	*OBJEXIST	*EXECUTE
DSPRJECFG	Opis sesji	*READ	*EXECUTE
ENDRJESSN [5]	Opis sesji	*USE	*EXECUTE
RMVFCTE	Tabela sterująca formularzy	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
RMVRJECMNE	Opis sesji	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJERDRE	Opis sesji	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJEWTRE	Opis sesji	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
SNDRJECMD	Opis sesji	*USE	*EXECUTE
SBMRJEJOB	Opis sesji	*USE	*EXECUTE
	Zbiór wejściowy [6]	*USE	*EXECUTE
	Kolejka komunikatów	*USE, *ADD	*EXECUTE
	Obiekty związane z zadaniem [7]		
SNDRJECMD	Opis sesji	*USE	*EXECUTE
STRRJECSL	Opis sesji	*USE	*EXECUTE
	Kolejka komunikatów	*USE	*EXECUTE
STRRJERDR	Opis sesji	*USE	*USE
STRRJESSN [5]	Opis sesji	*USE	*USE, *ADD
	Program	*USE	*EXECUTE
	Profil użytkownika QUSER	*USE	*EXECUTE
	Obiekty związane z zadaniem [7]		*EXECUTE
STRRJEWTR	Opis sesji	*USE	*USE
	Program [1]	*USE	*READ, *EXECUTE
	Zbiór urządzenia [1]	*USE, *ADD	*READ, *EXECUTE
	Zbiór fizyczny [1] (RJE generuje podzbiory)	*OBJMGT, *USE, *ADD	*OBJOPR, *ADD
	Zbiór fizyczny [1] (podano podzbiór)	*READ, *ADD	*READ, *EXECUTE
	Kolejka komunikatów [1]	*USE, *ADD	*READ, *EXECUTE
	Profil użytkownika QUSER	*USE	*READ, *EXECUTE
WRKFCT [8]	Tabela sterująca formularzy	*USE	*EXECUTE
WRKRJESSN [8]	Opis sesji	*USE	*EXECUTE
WRKSSND [8]	Opis sesji	*CHANGE	*EXECUTE

1 Profil użytkownika QUSER do tego obiektu wymaga uprawnień.

2 Jeśli obiektu nie odnaleziono lub brak wymaganych uprawnień, wysyłany jest komunikat i działanie komendy nie jest przerywane.

3 To uprawnienie jest wymagane do tworzenia opisu zadania QRJESSN.

4 To uprawnienie jest wymagane jedynie wtedy, gdy podano parametr DLTCMN(*YES).

5 Użytkownik musi mieć uprawnienia specjalne *JOBCTL.

6 Za pomocą instrukcji sterującej .. READFILE zbiory wejściowe obejmują także zbiory wbudowane.

7 Należy przejrzeć uprawnienia wymagane dla komendy SBMJOB.

8 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

Komendy atrybutów ochrony

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CHGSECA [1]			
CHGSECAUD [2,3]			
CFGSYSSEC [1,2,3]			
DSPSECA			
DSPSECAUD [3]			
PRTSYSSECA [4]			

[1] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *SECADM.

[2] Do użycia tej komendy konieczne jest uprawnienie specjalne (*ALLOBJ).

[3] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *AUDIT.

[4] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *ALLOBJ lub *AUDIT.

Komendy pozycji uwierzytelniania serwera

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ADDSVRAUTE[1]			
CHGSVRAUTE[1]			
DSPSVRAUTE	Profil użytkownika	*READ	*EXECUTE
RMVSVRAUTE[1]			

[1] Jeśli profilem użytkownika dla tej operacji nie jest profil *CURRENT lub bieżący użytkownik zadania, użytkownik musi mieć uprawnienia specjalne *SECADM oraz uprawnienia *OBJMGT i *USE do profilu.

Komendy usług

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ADDTRCFTR[11]			
APYPTF (Q)	Biblioteka produktu	*OBJMGT	
CHGSRVA [3] (Q)			
CHKCMNTRC [3] (Q)			*EXECUTE
CHKPRDOPT (Q)	Wszystkie obiekty w opcji produktu [4]		

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CPYPTF[2](Q)	Źródłowy zbiór	*USE	*EXECUTE
	Docelowy zbiór[8]	Takie same wymagania, jak dla komendy SAVOBJ	Takie same wymagania, jak dla komendy SAVOBJ
	Opis urządzenia	*USE	*EXECUTE
	Program licencjonowany		*USE
	Komendy: CHKTAP, CPYFRMTAP, CPYTOTAP, CRTLIB, CRTSAVF, CRTTAPF i OVRTAPF	*USE	*EXECUTE
	Biblioteka QSRV	*USE	*EXECUTE
CPYPTFGRP[2] (Q)	Opis urządzenia	*USE	*EXECUTE
	Docelowy zbiór	*Takie same wymagania, jak dla komendy SAVOBJ	*Takie same wymagania, jak dla komendy SAVOBJ
	Źródłowy zbiór	*USE	*EXECUTE
	Komendy: CHKTAP, CRTLIB, CRTSAVF	*USE	*EXECUTE
DLTAPARDTA (Q)			
DLTCMNTRC [3] (Q)	NWID (ID sieci) lub opis linii	*USE	*EXECUTE
DLTPTF (Q)	Zbiór listu przewodniego [4]		*EXECUTE
	Zbiór składowania PTF [4]		*EXECUTE
DLTTRC (Q)	Komenda RMVM	*USE	
	Biblioteka QSYS	*EXECUTE	
	Zbiory baz danych	*OBJEXIST, *OBJOPR	
DMPJOB (Q)			*EXECUTE
DMPJOBINT (Q)			
DSPPTF (Q)	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
DSPSRVA (Q)			
DSPSRVSTS (Q)			
ENDCMNTRC [3] (Q)	NWID lub opis linii	*USE	*EXECUTE
ENDCPYSCN (Q)	Opis urządzenia	*USE	*EXECUTE
ENDSRVJOB (Q)			
ENDTRC (Q)	Biblioteka QSYS	*ADD, *EXECUTE	
	zbiory baz danych,	*OBJOPR, *OBJMGMT, *ADD, *DLT	
	Komendy: PTRTRC, DLTTRC	*USE	
INSPTF[9] (Q)			
LODPTF (Q)	Opis urządzenia	*USE	*EXECUTE
LODRUN [2]	Komenda RSTOBJ	*USE	*EXECUTE

Komendy usług

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
PRTCMNTRC [3] (Q)	NWID (ID sieci) lub opis linii	*USE	*EXECUTE
	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
PRTERRLOG (Q)	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
PRTINTDTA[12,13] (Q)			
PRTTRC (Q)	Biblioteka QSYS	*EXECUTE	
	Zbiory baz danych	*USE	
	Komenda DLTTRC	*USE	
RMVPTF (Q)	Biblioteka produktu	*OBJMGT	
RMVTRCFTR[11]			
RUNLPDA (Q)	Opis linii	*READ	*EXECUTE
SAVAPARDTA [6] (Q)	Komendy: CRTDUPOBJ, CRTLIB, CRTOUTQ, CRTSAVF, DLTF, DMPOBJ, DMPSYSOBJ, DSPCTLD, DSPDEVD, DSPHDWRSC, DSPJOB, DSPLIND, DSPLOG, DSPNWID, DSPPTF, DSPSFWRSC, OVRPRTF, PRTERRLOG, PRTINTDTA, SAV, SAVDLO, SAVLIB, SAVOJB, WRKACTJOB i WRKSYSVAL	*USE	*EXECUTE
	Istniejący problem [7]	*CHANGE	*EXECUTE
SNDPTFORD [10] (Q)			
SNDSRVRQS (Q)			
STRCMNTRC [3] (Q)	NWID (ID sieci) lub opis linii	*USE	*EXECUTE
STRCPYSCN	Kolejka zadań	*USE	*EXECUTE
	Opis urządzenia	*USE	*EXECUTE
	Zbiór wyjściowy, jeśli został podany	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
STRSRVJOB (Q)	Profil użytkownika zadania	*USE	*EXECUTE
STRSST [3] (Q)			
STRTRC (Q)		*READ, *WRITE	
TRCCNN[11]			
TRCCPIC (Q)			
TRCICF (Q)			
TRCINT[11] (Q)			
TRCJOB (Q)	Zbiór wyjściowy, jeśli został podany	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Program obsługi wyjścia, jeśli został podany	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
TRCTCPAPP[11] (Q)	Program obsługi wyjścia użytkownika	*USE	*EXECUTE
	Opis linii	*USE	
	Interfejs sieciowy	*USE	
	Serwer sieciowy	*USE	
VFYCMN (Q)	Opis linii [5]	*USE	*EXECUTE
	Opis kontrolera [5]	*USE	*EXECUTE
	ID sieci [5]	*USE	*EXECUTE
VFYLNKLPDA (Q)	Opis linii	*READ	*EXECUTE
VFYPRT (Q)	Opis urządzenia	*USE	*EXECUTE
VFYOPT (Q)	Opis urządzenia	*USE	*EXECUTE
VFYTAP[14] (Q)	Opis urządzenia	*USE, *OBJMGT	*EXECUTE
WRKCNTINF (Q)			
WRKFSTAF (Q)	QUSRSYS/QPVINDEX *USRIDX	*CHANGE	*USE
WRKFSTPCT (Q)	QUSRSYS/QPVPCTABLE *USRIDX	*CHANGE	*USE
WRKPRB [1, 10] (Q)	Linia, kontroler, NWID (ID sieci) i urządzenie - na podstawie analizy problemu	*USE, *ADD	*EXECUTE
WRKPTFGRP (Q)			
WRKSRVPVD (Q)			

1 Dla niektórych procedur analizy lub gdy składowane są rekordy protokołu błędów, wymagane są uprawnienia do komendy PRTERRLOG.

2 Stosowane są także wszystkie ograniczenia dla komendy RSTOBJ.

3 Do uruchomienia tej komendy wymagane są uprawnienia specjalne usługi (*SERVICE).

4 Wymienione obiekty są wykorzystywane przez komendę, ale uprawnienia do obiektów nie są sprawdzane. Uprawnienie do użycia komendy jest wystarczające do używania obiektów.

5 Do sprawdzanego obiektu komunikacyjnego wymagane są uprawnienia *USE.

6 Aby zeskładować zbiór buforowy, użytkownik musi mieć uprawnienia specjalne *SPLCTL.

7 Jeśli dla nowego problemu uruchamiana jest komenda SAVAPARDTA, tworzona jest unikalna biblioteka APAR dla tego problemu. Jeśli dla tego samego problemu ponownie uruchamiana jest komenda SAVAPARDTA (w celu zebrania dodatkowych informacji), użytkownik musi mieć uprawnienie do używania biblioteki APAR dla problemu.

8 Opcja dodawania nowego podzbioru do istniejącego zbioru wyjściowego nie jest poprawną opcją dla tej komendy.

9 Ta komenda ma takie same uprawnienia oraz ograniczenia, jak komendy APYPTF i LODPTF.

10 Aby uzyskać dostęp do opcji 1 i 3 ekranu ″Wybór opcji raportowania″ (w celu zebrania dodatkowych informacji), użytkownik musi mieć uprawnienia *USE do komendy SNDSRVRQS.

11 Aby użyć tej komendy, użytkownik musi mieć uprawnienie specjalne *SERVICE lub uprawnienie do używania funkcji usługi śledzenia OS/400 w Administrowaniu aplikacjami w programie iSeries Navigator. Komenda Zmiana informacji o użyciu funkcji (Change Function Usage Information - QSYCHFUI), o identyfikatorze QIBM_SERVICE_TRACE, może być stosowana do zmiany listy użytkowników uprawnionych do wykonania operacji śledzenia.

Komendy usług

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
[12] Aby użyć tej komendy, użytkownik musi mieć uprawnieni specjalne *SERVICE lub uprawnienie do używania funkcji Zrzut serwisowy (Service dump) OS/400 w Administrowaniu aplikacjami w programie iSeries Navigator. Komenda Zmiana informacji o użyciu funkcji (Change Function Usage Information - QSYCHFUI), o identyfikatorze QIBM_SERVICE_DUMP, może być stosowana do zmiany listy użytkowników uprawnionych do wykonania operacji zrzutu.			
[13] Ta komenda musi być wywołana z poziomu zadania drukowaniem danych wewnętrznych lub osoba wywołująca komendę musi działać z wykorzystaniem profilu użytkownika takiego samego, jak tożsamość użytkownika zadania, którego dane wewnętrzne są drukowane, lub osoba wywołująca komendę musi działać z wykorzystaniem profilu użytkownika, który ma uprawnienia specjalne kontroli zadania (*JOBCTL).			
[14] Gdy opis urządzenia jest przydzielany przez urządzenie biblioteki nośników, użytkownik musi mieć uprawnienie specjalne *IOSYSCFG.			

Komendy słownika sprawdzania pisowni

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTSPADCT	Słownik sprawdzania pisowni	*OBJEXIST	*EXECUTE
	Słownik - REPLACE(*NO)		*READ, *ADD
	Słownik - REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
DLTSPADCT	Słownik sprawdzania pisowni	*OBJEXIST	*EXECUTE
WRKSPADCT [1]	Słownik sprawdzania pisowni	Dowolne uprawnienia	*USE
[1] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.			

Komendy sfery sterowania

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDSOCE	Sfera sterowania [1]	*USE, *ADD	*EXECUTE
DSPSOCSTS			
RMVSOCE	Sfera sterowania [1]	*USE, *DLT	*EXECUTE
WRKSOC	Sfera sterowania [1]	*USE	*EXECUTE
[1] Sfera sterowania to zbiór fizyczny QUSRSYS/QAALSOC.			

Komendy zbioru buforowego

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Parametry kolejki wyjściowej			Uprawnienie specjalne	Wymagane uprawnienie	
		DSPDTA	AUTCHK	OPRCTL		Do obiektu	Do biblioteki
CHGSPLFA [1,2]	Kolejka wyjściowa [3]		*DTAAUT			*READ, *DLT, *ADD	
			*OWNER			Właściciel [4]	
				*YES	*JOBCTL		
CHGSPLFA [1], jeśli zbiór buforowy jest przenoszony	Początkowa kolejka wyjściowa [3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Właściciel [4]	
				*YES	*JOBCTL		
	Zbiór buforowy	*OWNER				Właściciel [6]	
	Docelowa kolejka wyjściowa [7]					*READ	*EXECUTE
				*YES	*JOBCTL		*EXECUTE
	Urządzenie docelowe					*USE	
CPYSPLF [1]	Zbiór bazy danych					Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Zbiór buforowy	*OWNER				Właściciel [6]	
	Kolejka wyjściowa [3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Właściciel [4]	
		*YES lub *NO		*YES	*JOBCTL		
DLTSPLF [1]	Kolejka wyjściowa [3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Właściciel [4]	
				*YES	*JOBCTL		
DSPSPLF [1]	Kolejka wyjściowa [3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Właściciel [4]	
		*YES lub *NO		*YES	*JOBCTL		
	Zbiór buforowy	*OWNER				Właściciel [6]	
HLDSPLF [1]	Kolejka wyjściowa [3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Właściciel [4]	
				*YES	*JOBCTL		
RCLSPLSTG (Q)							

Komenda	Obiekt odniesienia	Parametry kolejki wyjściowej			Uprawnienie specjalne	Wymagane uprawnienie	
		DSPDTA	AUTCHK	OPRCTL		Do obiektu	Do biblioteki
RLSSPLF [1, 8]	Kolejka wyjściowa [3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Właściciel [4]	
				*YES	*JOBCTL		
SNDNETSPLF [1,5]	Kolejka wyjściowa [3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Właściciel [4]	
		*YES lub *NO		*YES	*JOBCTL		
	Zbiór buforowy	*OWNER				Właściciel [6]	
WRKSPLF							

1 Użytkownicy zawsze są uprawnieni do kontrolowania własnych zbiorów buforowych.

2 Aby przenieść zbiór buforowy na początek kolejki wyjściowej (PRTSEQ(*NEXT)) lub zmienić jego priorytet na większy niż limit podany w profilu użytkownika, użytkownik musi mieć jedno z podanych uprawnień do kolejki wyjściowej lub uprawnienie specjalne *SPLCTL.

3 Jeśli użytkownik ma uprawnienia specjalne *SPLCTL, nie potrzebuje żadnych uprawnień do kolejki wyjściowej.

4 Użytkownik musi być właścicielem kolejki wyjściowej.

5 W przypadku wysyłania zbioru do użytkownika w tym samym systemie, użytkownik musi mieć uprawnienia *USE do kolejki wyjściowej odbiorcy oraz do biblioteki tej kolejki.

6 Użytkownik musi być właścicielem zbioru buforowego.

7 Jeśli użytkownik ma uprawnienia specjalne *SPLCTL, to nie potrzebuje uprawnień do docelowej kolejki wyjściowej, ale musi mieć uprawnienia *EXECUTE do jej biblioteki.

8 Jeśli zbiór buforowy został wstrzymany za pomocą komendy HLDJOB SPLFILE(*YES) oraz został odłączony od zadania, użytkownik musi mieć uprawnienia *USE do komendy RLSJOB i uprawnienia specjalne *JOBCTL lub musi być właścicielem zbioru buforowego.

Komendy opisu podsystemu

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ADDAJE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Opis zadania	*OBJOPR, *READ	*EXECUTE
ADDCMNE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Opis zadania	*OBJOPR, *READ	*EXECUTE
	Profil użytkownika	*USE	
ADDJOBQE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDPJE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Profil użytkownika	*USE	
	Opis zadania	*OBJOPR, *READ	*EXECUTE
ADDRTGE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
ADDWSE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Opis zadania	*OBJOPR, *READ	*EXECUTE
CHGAJE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Opis zadania	*OBJOPR, *READ	*EXECUTE
CHGCMNE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Opis zadania	*OBJOPR, *READ	*EXECUTE
	Profil użytkownika	*USE	
CHGJOBQE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
CHGPJE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Profil użytkownika	*USE	
	Opis zadania	*OBJOPR, *READ	*EXECUTE
CHGRTGE	Opis podsystemu	*OJBOPR, *OBJMGT, *READ	*EXECUTE
CHGSBSD [5]	Opis podsystemu	*OJBOPR, *OBJMGT, *READ	*EXECUTE
	zbiór ekranowy wpisywania się[4]	*USE	*EXECUTE
CHGWSE	Opis podsystemu	*OJBOPR, *OBJMGT, *READ	*EXECUTE
	Opis zadania	*OBJOPR, *READ	*EXECUTE
CRTSBSD [5] (Q)	Opis podsystemu		*READ, *ADD
	zbiór ekranowy wpisywania się[4]	*USE	*EXECUTE
DLTSBSD	Opis podsystemu	*OBJEXIST, *USE	*EXECUTE
DSPSBSD	Opis podsystemu	*OBJOPR, *READ	*EXECUTE
ENDSBS [1]			
PRTSBSDAUT [6]			
RMVAJE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVCMNE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVJOBQE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVPJE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE

Komendy opisu podsystemu

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
RMVRTGE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVWSE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
STRSBS [1]	Opis podsystemu	*USE	*EXECUTE
WRKSBS [2, 3]	Opis podsystemu	Dowolne uprawnienia	*USE
WRKSBSD [3]	Opis podsystemu	Dowolne uprawnienia	*USE

1 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne sterowania zadaniem (*JOBCTL).

2 Wymaga niektórych uprawnień (dowolnych z wyjątkiem *EXCLUDE)

3 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

4 Uprawnienie wymagane jest do zakończenia sprawdzania formatu zbioru ekranowego. Pozwala to przewidzieć, czy ekran będzie pracował poprawnie, gdy podsystem zostanie uruchomiony. Jeśli użytkownik nie jest uprawniony do zbioru ekranowego lub jego biblioteki, sprawdzanie formatu nie zostanie przeprowadzone.

5 Aby podać bibliotekę dla biblioteki podsystemu, użytkownik musi mieć uprawnienia specjalne *SECADM lub *ALLOBJ.

6 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *ALLOBJ lub *AUDIT.

Komendy systemowe

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
PWRDWNSYS[1]	Katalog obrazów (jeśli podano)	*USE	
Te komendy nie wymagają żadnych uprawnień do obiektu:			
CHGSHRPOOL DSPSYSSTS ENDSYS[1] RCLACTGRP[1]	RCLRSC RETURN RTVGRPA	SIGNOFF WRKSHRPOOL	WRKSYSSTS

1 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne sterowania zadaniem (*JOBCTL).

Komendy listy odpowiedzi systemowych

Te komendy nie wymagają uprawnień do obiektu:			
ADDRPYLE (Q)	CHGRPYLE (Q)	RMVRPYLE (Q)	WRKRPYLE

Komendy wartości systemowych

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Te komendy nie wymagają żadnych uprawnień do obiektów:			
CHGSYSVAL (Q) [1,2]	DSPSYSVAL[3]	RTVSYSVAL[3]	WRKSYSVAL [1,2, 3]

[1] Aby zmienić niektóre wartości, niezbędne są uprawnienia specjalne *ALLOBJ, *ALLOBJ i *SECADM, *AUDIT, *IOSYSCFG lub *JOBCTL.

[2] Aby używać tej komendy w stanie, w jakim została dostarczona przez IBM, użytkownik musi być wpisany jako użytkownik QPGMR, QSYSOPR, lub QSRV albo musi mieć uprawnienie specjalne *ALLOBJ.

[3] Aby wyświetlić lub odtworzyć wartości systemowe dotyczące kontroli, użytkownik musi mieć uprawnienie specjalne *AUDIT lub *ALLOBJ.

Komendy środowiska System/36

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGS36	Obiekt konfiguracyjny S/36 QS36ENV	*UPD	*EXECUTE
CHGS36A	Obiekt konfiguracyjny S/36 QS36ENV	*UPD	*EXECUTE
CHGS36PGMA	Program	*OBJMGT, *USE	*EXECUTE
CHGS36PRCA	Zbiór QS36PRC	*OBJMGT, *USE	*EXECUTE
CHGS36SRCA	Źródło	*OBJMGT, *USE	*EXECUTE
CRTMSGFMNU	Menu: REPLACE(*NO)		*READ, *ADD
	Menu: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD
	Wyświetlenie zbioru, jeśli istnieje	*ALL	*EXECUTE
	Zbiór komunikatów	*USE	*CHANGE
	Zbiór źródłowy QS36SRC	*ALL	*EXECUTE
CRTS36DSPF	Zbiór ekranowy: REPLACE(*NO)		*READ, *ADD
	Zbiór ekranowy: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD, *CHANGE
	Zbiór docelowy, gdy wartością parametru TOMBR nie jest *NONE	*ALL	*CHANGE
	Zbiór źródłowy QS36SRC	*USE	*EXECUTE
	Komenda Tworzenie zbioru ekranowego (Create Display File - CRTDSPF)	*OBJOPR	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTS36MNU	Menu: REPLACE(*NO)		*READ, *ADD, *CHANGE
	Menu: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD, *CHANGE
	Zbiór docelowy, gdy wartością parametru TOMBR nie jest *NONE	*ALL	*CHANGE
	Zbiór źródłowy QS36SRC	*USE	*EXECUTE
	Zbiór ekranowy, jeśli podano parametr REPLACE(*YES)	*ALL	*EXECUTE
	Zbiory komunikatów nazwane w źródle	*ALL	*EXECUTE
	Zbiór ekranowy		*CHANGE
	Komenda CRTMSGF	*OBJOPR, *OBJEXIST	*EXECUTE
	Komenda ADDMSGD	*OBJOPR	*EXECUTE
	Komenda CRTDSPF	*OBJOPR	*EXECUTE
CRTS36MSGF	Zbiór komunikatów: REPLACE(*NO)		*READ, *ADD, *CHANGE
	Zbiór komunikatów: REPLACE(*YES)	Więcej informacji znajduje się w zasadach ogólnych.	*READ, *ADD, *CHANGE
	Zbiór docelowy, gdy wartością parametru TOMBR nie jest *NONE	*ALL	*CHANGE
	Zbiór źródłowy QS36SRC	*USE	*EXECUTE
	Zbiór ekranowy, jeśli podano parametr REPLACE(*YES)	*ALL	*EXECUTE
	Zbiór komunikatów nazwany w źródle	*ALL	*EXECUTE
	Zbiór komunikatów nazwany w źródle, gdy parametr OPTION ma wartość *ADD lub *CHANGE	*CHANGE	*EXECUTE
	Zbiory komunikatów nazwane w źródle, gdy podano OPTION(*CREATE)	*ALL	*EXECUTE
	Komenda CRTMSGF	*OBJOPR, *OBJEXIST	*EXECUTE
	Komenda ADDMSGD	*OBJOPR	*EXECUTE
	Komenda CHGMSGD, gdy podano OPTION(*CHANGE)	*OBJOPR	*EXECUTE
DSPS36	Obiekt konfiguracyjny S/36 QS36ENV	*READ	*EXECUTE
EDTS36PGMA	Program, do zmiany atrybutów	*OBJMGT, *USE	*EXECUTE
	Program, do przeglądania atrybutów	*USE	*EXECUTE
EDTS36PRCA	Zbiór QS36PRC, do zmiany atrybutów	*OBJMGT, *USE	*EXECUTE
	Zbiór QS36PRC, do przeglądania atrybutów	*USE	*EXECUTE
EDTS36SRCA	Zbiór źródłowy QS36SRC, do zmiany atrybutów	*OBJMGT, *USE	*EXECUTE
	Zbiór źródłowy QS36SRC, do przeglądania atrybutów	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
RSTS36F (Q)	Źródłowy zbiór	*USE	*EXECUTE
	Docelowy zbiór	*ALL	Więcej informacji znajduje się w zasadach ogólnych.
	W oparciu o zbiór fizyczny, jeśli odtwarzany zbiór jest zbiorem logicznym (alternatywnie)	*CHANGE	*EXECUTE
	Zbiór urządzenia lub opis urządzenia	*USE	*EXECUTE
RSTS36FLR [1,2,3] (Q)	Folder S/36	*USE	*EXECUTE
	Do folderu	*CHANGE	*EXECUTE
	Zbiór urządzenia lub opis urządzenia	*USE	*EXECUTE
RSTS36LIBM (Q)	Źródłowy zbiór	*USE	*EXECUTE
	Docelowy zbiór	*ALL	Więcej informacji znajduje się w zasadach ogólnych.
	Zbiór urządzenia lub opis urządzenia	*USE	*EXECUTE
RTVS36A	Obiekt konfiguracyjny S/36 QS36ENV	*UPD	*EXECUTE
SAVS36F	Źródłowy zbiór	*USE	*EXECUTE
	Zbiór docelowy, gdy jest zbiorem fizycznym	*ALL	Więcej informacji znajduje się w zasadach ogólnych.
	Zbiór urządzenia lub opis urządzenia	*USE	*EXECUTE
SAVS36LIBM	Źródłowy zbiór	*USE	*EXECUTE
	Zbiór docelowy, gdy jest zbiorem fizycznym	*ALL	Więcej informacji znajduje się w zasadach ogólnych.
	Zbiór urządzenia lub opis urządzenia	*USE	*EXECUTE
WRKS36	Obiekt konfiguracyjny S/36 QS36ENV	*READ	*EXECUTE
WRKS36PGMA	Program, do zmiany atrybutów	*OBJMGT, *USE	*EXECUTE
	Program, do przeglądania atrybutów	*USE	*EXECUTE
WRKS36PRCA	Zbiór QS36PRC, do zmiany atrybutów	*OBJMGT, *USE	*EXECUTE
	Zbiór QS36PRC, do przeglądania atrybutów	*USE	*EXECUTE
WRKS36SRCA	Zbiór źródłowy QS36SRC, do zmiany atrybutów	*OBJMGT, *USE	*EXECUTE
	Zbiór źródłowy QS36SRC, do przeglądania atrybutów	*USE	*EXECUTE

1 Jeśli dokument ma być zastąpiony, wymagane są uprawnienia *ALL. Użytkownik musi mieć uprawnienie operacyjne i do danych dla folderu w przypadku odtwarzania nowych informacji do folderów albo musi posiadać uprawnienie *ALLOBJ.

2 Jeśli używane dla katalogu danych, wymagane są tylko uprawnienia do komendy.

3 Użytkownik musi być zarejestrowany w katalogu dystrybucyjnym systemu, jeśli folder źródłowy jest folderem dokumentów.

Komendy tabel

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTTBL	Tabela		*READ, *ADD, *EXECUTE
	Zbiór źródłowy	*USE	*EXECUTE
DLTTBL	Tabela	*OBJEXIST	*EXECUTE
WRKTBL [1]	Tabela	Dowolne uprawnienia	*USE

1 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

Komendy TCP/IP

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDTCPSVR[1]	Program do wywołania	*EXECUTE	*EXECUTE
CHGTCPSVR[1]	Program do wywołania	*EXECUTE	*EXECUTE
CVTTCPCL (Q)	Obiekty zbioru	*USE	*EXECUTE
ENDTCP (Q)	Opis linii [4]	*USE	*EXECUTE
	Opis kontrolera [4]	*USE	*EXECUTE
	Opis urządzenia [4]	*USE	*EXECUTE
	Obiekty zbioru	*USE	*EXECUTE
ENDTCPIFC (Q)	Obiekty zbioru	*USE	*EXECUTE
	Opis linii [4]	*USE	*EXECUTE
	Opis kontrolera [4]	*USE	*EXECUTE
	Opis urządzenia [4]	*USE	*EXECUTE
ENDTCPPTP	Opis linii [4]	*USE	*EXECUTE
	Opis kontrolera [4]	*USE	*EXECUTE
	Opis urządzenia [4]	*USE	*EXECUTE
	Obiekty zbioru	*USE	*EXECUTE
ENDTCPSRV (Q)	Obiekty zbioru	*USE	*EXECUTE
FTP	Obiekty zbioru	*USE	*EXECUTE
	Obiekty tabeli	*USE	*EXECUTE
LPR [2]	Obiekt dostosowania stacji roboczej	*USE	*EXECUTE
SETVTTBL	Obiekty tabeli	*USE	*EXECUTE
SNDTCPSPLF [2]	Obiekt dostosowania stacji roboczej	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
STRTCP (Q)	Obiekty zbioru	*USE	*EXECUTE
	Opis linii [4]	*USE	*EXECUTE
	Opis kontrolera [4]	*USE	*EXECUTE
	Opis urządzenia [4]	*USE	*EXECUTE
STRTCPFTP	Obiekty tabeli	*USE	*EXECUTE
	Obiekty zbioru	*USE	*EXECUTE
STRTCPIFC (Q)	Obiekty zbioru	*USE	*EXECUTE
	Opis linii [4]	*USE	*EXECUTE
	Opis kontrolera [4]	*USE	*EXECUTE
	Opis urządzenia [4]	*USE	*EXECUTE
STRTCPPTP	Opis linii [4]	*USE	*EXECUTE
	Opis kontrolera [4]	*USE	*EXECUTE
	Opis urządzenia [4]	*USE	*EXECUTE
	Obiekty zbioru	*USE	*EXECUTE
STRTCPSVR (Q)	Obiekty tabeli	*USE	*EXECUTE
	Obiekty zbioru	*USE	*EXECUTE
STRTCPTELN	Obiekty tabeli	*USE	*EXECUTE
	Obiekty zbioru	*USE	*EXECUTE
	Wirtualna stacja robocza [5]	*USE	*EXECUTE
TELNET	Obiekty tabeli	*USE	*EXECUTE
	Obiekty zbioru	*USE	*EXECUTE
	Wirtualna stacja robocza [5]	*USE	*EXECUTE

Te komendy nie wymagają żadnych uprawnień do obiektu:

ADDCOMSNMP [1]	CFGTCPSMTP	CHGVTMAP	RMVTCPRSI [1]
ADDNETTBLE [1]	CFGTCPSNMP	DSPVTMAP	RMVTCPRTE [1]
ADDPCLTBLE [1]	CFGTCPTELN	ENDTCPCNN	RMVTCPSVR [1]
ADDSRVTBLE [1]	CHGCOMSNMP [1]	MGRTCPHT [1]	RNMTCPHTE [1]
ADDTCPHTE [1]	CHGFTPA [1]	NETSTAT	SETVTMAP
ADDTCPIFC [1]	CHGLPDA [1]	PING	VFYTCPCNN
ADDTCPPORT [1]	CHGSMTPA [1]	RMVCOMSNMP [1]	WRKNAMSMTP [3]
ADDTCPRSI [1]	CHGSNMPA [1]	RMVNETTBLE [1]	WRKNETTBLE[1]
ADDTCPRTE [1]	CHGTCPA [1]	RMVPCLTBLE [1]	WRKPCLTBLE[1]
CFGTCP	CHGTCPHTE[1]	RMVSRVTBLE [1]	WRKSRVTBLE[1]
CFGTCPAPP	CHGTCPIFC[1]	RMVTCPHTE[1]	WRKTCPSTS
CFGTCPFTP [1]	CHGTCPRTE [1]	RMVTCPIFC[1]	
CFGTCPLPD [1]	CHGTELNA [1]	RMVTCPPORT [1]	

1 Do użycia tej komendy konieczne jest uprawnienie specjalne (*IOSYSCFG).

2 Komendy SNDTCPSPLF i LPR korzystają z tych samych kombinacji uprawnień obiektu odniesienia, z jakich korzysta komenda SNDNETSPLF.

3 Aby zmienić tabelę aliasów systemu lub inną tabelę aliasów profilu użytkownika, użytkownik musi mieć uprawnienia specjalne *SECADM.

4 Jeśli użytkownik ma uprawnienia specjalne *JOBCTL, nie potrzebuje podanych uprawnień do obiektu.

5 Jeśli użytkownik ma uprawnienia specjalne *JOBCTL, nie potrzebuje podanych uprawnień do obiektu w systemie zdalnym.

Komendy opsu strefy czasowej

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CHGTIMZON	Opis strefy czasowej	*CHANGE	*EXECUTE
CRTTIMZON	Opis strefy czasowej		*READ, *ADD
DLTTIMZON[1]	Opis strefy czasowej	*OBJEXIST	*EXECUTE
WRKTIMZON[2]	Opis strefy czasowej	*USE	*USE

[1] Opis strefy czasowej podany w wartości systemowej QTIMZON nie może być usunięty.

[2] Jeśli komunikat jest używany do podawania nazw skróconych i pełnych dla opisu strefy czasowej, użytkownik, aby zobaczyć nazwy skrócone i pełne musi mieć uprawnienia *USE do zbioru komunikatów oraz uprawnienia *EXECUTE do biblioteki zbioru komunikatów.

Komendy danych zamówienia aktualizacj

Te komendy mają uprawnienia publiczne *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
WRKORDINF	Zbiór QGPL/QMAHFILE	*CHANGE, *OBJALTER	*EXECUTE

Komendy indeksu użytkownika, kolejki użytkownika, przestrzeni użytkownika

Tabela 151.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
DLTUSRIDX	Indeks użytkownika	*OBJEXIST	*EXECUTE
DLTUSRQ	Kolejka użytkownika	*OBJEXIST	*EXECUTE
DLTUSRSPC	Przestrzeń użytkownika	*OBJEXIST	*EXECUTE

Komendy profilu użytkownika

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Szef ochrony może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ANZDFTPWD [3, 14, 15](Q)			
ANZPRFACT [3, 14, 15](Q)			
CHGACTPRFL [14](Q)			
CHGACTSCDE [3, 14, 15](Q)			
CHGDSTPWD [1]			
CHGEXPSCDE [3, 14, 15](Q)			
CHGPRF	Profil użytkownika	*OBJMGT, *USE	
	Program początkowy [2]	*USE	*EXECUTE
	Menu początkowe [2]	*USE	*EXECUTE
	Opis zadania [2]	*USE	*EXECUTE
	Kolejka komunikatów[2]	*USE	*EXECUTE
	Kolejka wyjściowa[2]	*USE	*EXECUTE
	Program obsługi klawisza ATTN [2]	*USE	*EXECUTE
	Biblioteka bieżąca [2]	*USE	*EXECUTE
CHGPWD			
CHGUSRAUD [11](Q)			
CHGUSRPRF [3]	Profil użytkownika	*OBJMGT, *USE	*EXECUTE
	Program początkowy [2]	*USE	*EXECUTE
	Menu początkowe [2]	*USE	*EXECUTE
	Opis zadania [2]	*USE	*EXECUTE
	Kolejka komunikatów[2]	*USE	*EXECUTE
	Kolejka wyjściowa[2]	*USE	*EXECUTE
	Program obsługi klawisza ATTN [2]	*USE	*EXECUTE
	Biblioteka bieżąca [2]	*USE	*EXECUTE
	Profil grupowy (GRPPRF lub SUPGRPPRF)[2,4]	*OBJMGT, *OBJOPR, *READ, *ADD, *UPD, *DLT	*EXECUTE
CHGUSRPRTI	Profil użytkownika	*CHANGE	
CHKPWD			

Komendy profilu użytkownika

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTUSRPRF [3, 12, 17]	Program początkowy	*USE	*EXECUTE
	Menu początkowe	*USE	*EXECUTE
	Opis zadania	*USE	*EXECUTE
	Kolejka komunikatów	*USE	*EXECUTE
	Kolejka wyjściowa	*USE	*EXECUTE
	Program obsługi klawisza ATTN	*USE	*EXECUTE
	Biblioteka bieżąca	*USE	*EXECUTE
	Profil grupowy (GRPPRF lub SUPGRPPRF)[4]	*OBJMGT, *OBJOPR, *READ, *ADD, *UPD, *DLT	*EXECUTE
CVTUSRCERT[3, 14]			
DLTUSRPRF [3,9]	Profil użytkownika	*OBJEXIST, *USE	*EXECUTE
	Kolejka komunikatów [5]	*OBJEXIST, *USE, *DLT	*EXECUTE
DSPACTPRFL [14](Q)			
DSPACTSCD [14](Q)			
DSPAUTUSR [6]	Profil użytkownika	*READ	
DSPEXPSCD [14](Q)			
DSPPGMADP	Profil użytkownika	*OBJMGT	
	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
DSPUSRPRF[19]	Profil użytkownika	*READ	*EXECUTE
	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
DSPUSRPRTI	Profil użytkownika	*USE	
GRTUSRAUT [7]	Profil użytkownika odniesienia	*READ	
	Obiekty, do których nadawane są uprawnienia	*OBJMGT	*EXECUTE
PRTPRFINT [14](Q)			
PRTUSRPRF [18]			
RSTAUT (Q) [8]			
RSTUSRPRF (Q) [8,10, 16]			
RTVUSRPRF[20]	Profil użytkownika	*READ	
RTVUSRPRTI	Profil użytkownika	*USE	
SAVSECDTA [8]	Zbiór składowania, jeśli jest pusty	*USE, *ADD	*EXECUTE
	Zbiór składowania, jeśli istnieją w nim rekordy	*OBJMGT, *USE, *ADD	*EXECUTE
WRKUSRPRF [13]	Profil użytkownika	Dowolne uprawnienia	

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
[1] Ta komenda może być uruchomiona tylko wtedy, gdy użytkownik wpisze się jako użytkownik QSECOFR.			
[2] Wymagane są uprawnienia tylko do obiektów, dla pól zmienianych w profilu użytkownika.			
[3] Wymagane jest uprawnienie specjalne *SECADM.			
[4] Uprawnienie *OBJMGT do profilu grupowego nie może pochodzić z uprawnień adoptowanych.			
[5] Kolejka komunikatów związana z profilem użytkownika jest usuwana, jeśli jej właścicielem jest ten profil. Aby usunąć kolejkę komunikatów, użytkownik uruchamiający komendę DLTUSRPRF musi mieć podane uprawnienia.			
[6] Na ekranie są tylko te profile użytkowników, do których użytkownik uruchamiający komendę ma podane uprawnienia.			
[7] Więcej informacji znajduje się w sekcji dotyczącej uprawnień dla komendy GRTOBJAUT.			
[8] Wymagane jest uprawnienie specjalne *SAVSYS.			
[9] Jeśli wybrana została opcja usuwania obiektów, których właścicielem jest profil użytkownika, aby przeprowadzić tę operację, użytkownik musi mieć odpowiednie uprawnienia. Jeśli wybrana została opcja przeniesienia prawa własności na inny profil użytkownika, użytkownik musi mieć odpowiednie uprawnienia do obiektów oraz do profilu użytkownika. Więcej informacji znajduje się w sekcji dotyczącej komendy CHGOBJOWN.			
[10] Aby podać parametr ALWOBJDIF(*ALL), użytkownik musi mieć uprawnienia specjalne *ALLOBJ.			
[11] Użytkownik musi mieć uprawnienia specjalne *AUDIT.			
[12] Użytkownik, dla którego tworzony jest profil, ma do niego następujące uprawnienia: *OBJMGT, *OBJOPR, *READ, *ADD, *DLT, *UPD, *EXECUTE.			
[13] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.			
[14] Do użycia tej komendy konieczne jest uprawnienie specjalne (*ALLOBJ).			
[15] Aby użyć tej komendy należy mieć uprawnienia specjalne *JOBCTL.			
[16] Aby podać wartość SECDTA(*PWDGRP), USRPRF(*ALL) lub OMITUSRPRF, użytkownik musi mieć uprawnienia specjalne *ALLOBJ i *SECADM.			
[17] Wykonując komendę CRTUSRPRF, nie można tworzyć profilu użytkownika (*USRPRF) w niezależnej puli dyskowej. Jednak jeśli użytkownik ma uprawnienia prywatne do obiektu na niezależnej puli dyskowej, jest właścicielem obiektu na niezależnej puli dyskowej lub jest w grupie podstawowej obiektu na niezależnej puli dyskowej, to nazwa profilu przechowywana jest na niezależnej puli dyskowej. Jeśli niezależna pula dyskowa przenoszona jest do innego systemu, uprawnienia prywatne, prawa własności do obiektu oraz pozycji grupy podstawowej będą dołączone w systemie docelowym do profilu o tej samej nazwie. Jeśli w systemie docelowym dany profil nie istnieje, to zostanie utworzony. Użytkownik nie będzie miał żadnych uprawnień specjalnych, a jego hasło będzie miało wartość *NONE.			
[18] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *ALLOBJ lub *AUDIT.			
[19] Aby bieżące wartości kontrolowania obiektu i akcji zostały wyświetlone, użytkownik musi mieć uprawnienie specjalne *ALLOBJ lub *AUDIT. W przeciwnym przypadku zostanie wyświetlona wartość *NOTAVL wskazująca, że wartości kontrolowania nie mogą być wyświetlone.			
[20] Aby pobrać bieżące wartości OBJAUD i AUDLVL kontrolowania obiektu, użytkownik musi mieć uprawnienie specjalne *ALLOBJ lub *AUDIT. W przeciwnym przypadku zostanie zwrócona wartość *NOTAVL wskazująca, że wartości nie mogą być pobrane.			

Komendy systemu plików użytkownika

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu
ADDMFS [1,2,3]	katalog_do_podłączenia	*DIR	″główny″	*W
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
CRTUDFS [1,2,6,7] (Q)	/dev/QASP*xx*	*DIR	″główny″	*RWX
DLTUDFS [1,2,4,5] (Q)	/dev/QASP*xx*	*DIR	″główny″	*RWX
	dowolny_obiekt_epfs		″główny″	*RWX, *OBJEXIST
DSPUDFS	jakieś_katalogixx	*DIR	″główny″	*RX
MOUNT [1,2,3]	katalog_do_podłączenia	*DIR	″główny″	*W
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
RMVMFS [1]				
UNMOUNT [1]				

1 Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

2 Parametr QASP*xx* ma wartość 01 (systemowa ASP) lub 02-16 w zależności od tego, która ASP użytkowników jest niezbędna. Jest to katalog, który zawiera podłączane *BLKSF.

3 Podłączany katalog (katalog_do_podłączenia) jest dowolnym katalogiem zintegrowanego systemu plików, który może być podłączany.

4 System plików UDFS może zawierać całe poddrzewo obiektów, tak że podczas usuwania systemu UDFS usuwane są wszystkie rodzaje obiektów, które mogą być przechowywane w tym systemie plików.

5 Aby używać komendy DLTUDFS, użytkownik musi mieć uprawnienia *OBJEXIST do każdego obiektu w systemie plików UDFS, gdyż w przeciwnym przypadku żaden obiekt nie zostanie usunięty.

6 Aby podać wartość dla parametru Opcja skanowania dla obiektów (Scanning option for objects - CRTOBJSCAN) inną niż *PARENT, użytkownik musi mieć uprawnienia specjalne do wszystkich obiektów (*ALLOBJ) i administratora ochrony (*SECADM).

7 Uprawnienia specjalne do kontroli (*AUDIT) wymagane są podczas podawania wartości innej niż *SYSVAL dla parametru Wartość kontroli dla obiektów (Auditing value for objects - CRTOBJAUD).

Komendy listy sprawdzania

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CRTVLDL	Lista weryfikacji		*ADD, *READ
DLTVLDL	Lista weryfikacji	*OBJEXIST	*EXECUTE

Komendy dostosowania stacji roboczej

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTWSCST	Zbiór źródłowy	*USE	*EXECUTE
	Obiekt dostosowania stacji roboczej, jeśli REPLACE(*NO)		*READ, *ADD
	Obiekt dostosowania stacji roboczej, jeśli REPLACE(*YES)	*OBJMGT, *OBJEXIST	*READ, *ADD
DLTWSCST	Obiekt dostosowania stacji roboczej	*OBJEXIST	*EXECUTE
RTVWSCST	Do pliku, jeśli plik istnieje i dodawany jest nowy podzbiór	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Do pliku, jeśli plik i podzbiór istnieją	*OBJOPR, *ADD, *DLT	*EXECUTE
	Do pliku, jeśli plik nie istnieje		*READ, *ADD

Komendy programu piszącego

Komenda	Obiekt odniesienia	Parametry kolejki wyjściowej		Uprawnienie specjalne	Wymagane uprawnienie	
		AUTCHK	**OPRCTL**		**Do obiektu**	**Do biblioteki**
CHGWTR [2, 4]	Bieżąca kolejka wyjściowa [1]	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel [3]	*EXECUTE
			*YES	*JOBCTL		
ENDWTR [1]	Kolejka wyjściowa	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel [3]	*EXECUTE
			*YES	*JOBCTL		
HLDWTR [1]	Kolejka wyjściowa	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel [3]	*EXECUTE
			*YES	*JOBCTL		
RLSWTR [1]	Kolejka wyjściowa	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel [3]	*EXECUTE
			*YES	*JOBCTL		
STRDKTWTR [1]	Kolejka wyjściowa	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel [3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Kolejka komunikatów				*OBJOPR, *ADD	*EXECUTE
	Opis urządzenia				*OBJOPR, *READ	

Komendy programu piszącego

Komenda	Obiekt odniesienia	Parametry kolejki wyjściowej		Uprawnienie specjalne	Wymagane uprawnienie	
		AUTCHK	OPRCTL		Do obiektu	Do biblioteki
STRPRTWTR [1]	Kolejka wyjściowa	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel [3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Kolejka komunikatów				*OBJOPR, *ADD	*EXECUTE
	Sterownik urządzenia zdefiniowanego przez użytkownika				*READ	*EXECUTE
	Program transformujący dane				*READ	*EXECUTE
	Program separatora				*READ	*EXECUTE
	Opis urządzenia				*OBJOPR, *READ	
STRRMTWTR [1]	Kolejka wyjściowa	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
	Kolejka komunikatów	*OWNER			Właściciel [3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
					*OBJOPR, *ADD	*EXECUTE
	Sterownik urządzenia użytkownika				*READ	*EXECUTE
	Przekształcanie danych użytkownika				*READ	*EXECUTE
WRKWTR						

1 Jeśli użytkownik ma uprawnienia specjalne *SPLCTL, nie potrzebuje żadnych uprawnień do kolejki wyjściowej.

2 Aby zmienić kolejkę wyjściową dla programu piszącego, użytkownik musi mieć jedno z podanych uprawnień do nowej kolejki wyjściowej.

3 Użytkownik musi być właścicielem kolejki wyjściowej.

4 Do biblioteki nowej kolejki wyjściowej użytkownik musi mieć uprawnienia *EXECUTE, nawet jeśli ma uprawnienia specjalne *SPLCTL.

Dodatek E. Działania na obiektach a kontrola

Ten dodatek opisuje operacje, które można wykonywać na obiektach systemu oraz zawiera informacje, czy są onekontrolowane. Lista ułożona jest według typów obiektów. Operacje pogrupowane są według tego, czy są kontrolowane, gdy parametr OBJAUD komendy CHGOBJAUD lub CHGDLOAUD ma wartość *ALL lub *CHANGE.

To, czy rekord kontroli dla działania zostanie zapisany, zależy od kombinacji wartości systemowych, wartości w profilu użytkownika przeprowadzającego działanie i wartości zdefiniowanej dla obiektu. Sekcja “Planowanie kontroli dostępu do obiektu” na stronie 256 opisuje, w jaki sposób skonfigurować kontrolę obiektów.

Operacje zapisane w tabelach wielkimi literami, na przykład CPYF, są komendami CL, chyba że oznaczone są jako funkcje API.

Operacje wspólne dla wszystkich typów obiektów:

- Odczyt

  CRTDUPOBJ
  Tworzenie duplikatu obiektu (Create Duplicate Object) - jeśli jako parametr *"z_obiektu"* podano *ALL.

  DMPOBJ
  Zrzut obiektu (Dump Object)

  DMPSYSOBJ
  Zrzut obiektu systemowego (Dump System Object)

  SAV Składowanie obiektu w katalogu (Save Object in Directory)

  SAVCHGOBJ
  Składowanie zmienionych obiektów (Save Changed Object)

  SAVLIB
  Składowanie biblioteki (Save Library)

  SAVOBJ
  Składowanie obiektu (Save Object)

  SAVSAVFDTA
  Składowanie danych zbioru składowania (Save Save File Data)

  SAVDLO
  Składowanie obiektu DLO (Save DLO Object)

  SAVLICPGM
  Składowanie programu licencjonowanego (Save Licensed Program)

  SAVSHF
  Składowanie półki (Save Bookshelf)

  Uwaga: Rekord kontroli dla operacji składowania będzie identyfikowany, jeśli składowanie wykonano z parametrem STG(*FREE).

- Zmiana

  APYJRNCHG
  Zastosowanie kronikowanych zmian (Apply Journaled Changes)

  CHGJRNOBJ
  Change Journaled Object (Zmiana kronikowanego obiektu)

Kontrola obiektów

CHGOBJD
Zmiana opisu obiektu (Change Object Description)

CHGOBJOWN
Zmiana właściciela obiektu (Change Object Owner)

CRTxxxxxx
Tworzenie obiektu (Create object)

Uwagi:

1. Jeśli dla biblioteki docelowej podano parametr *ALL lub *CHANGE, podczas tworzenia obiektu zapisywana jest pozycja ZC.
2. Jeśli dla kontrolowania działania aktywna jest wartość *CREATE, podczas tworzenia obiektu zapisywana jest pozycja CO.

DLTxxxxxx
Usunięcie obiektu (Delete object)

Uwagi:

1. Jeśli dla biblioteki zawierającej obiekt podano parametr *ALL lub *CHANGE, podczas usuwania obiektu zapisywana jest pozycja ZC.
2. Jeśli dla obiektu podano parametr *ALL lub *CHANGE, podczas usuwania obiektu zapisywana jest pozycja ZC.
3. Jeśli dla kontrolowania działania aktywna jest wartość *DELETE, podczas usuwania obiektu zapisywana jest pozycja DO.

ENDJRNxxx
Zakończenie kronikowania (End Journaling)

GRTOBJAUT
Nadanie uprawnień dla obiektu (Grant Object Authority)

Uwaga: Jeśli uprawnienia nadawane są w oparciu o obiekt odniesienia, dla obiektu odniesienia nie jest zapisywany rekord kontroli.

MOVOBJ
Przeniesienie obiektu (Move Object)

QjoEndJournal
Zakończenie kronikowania (End Journaling)

QjoStartJournal
Uruchomienie kronikowania (Start Journaling)

RCLSTG
Odzyskiwanie pamięci (Reclaim Storage)

- Jeśli obiekt jest chroniony przez uszkodzony *AUTL, rekord kontroli zostanie zapisany, gdy obiekt jest chroniony przez listę autoryzacji QRCLAUTL.
- Rekord kontroli jest zapisywany podczas przenoszenia obiektu do biblioteki QRCL.

RMVJRNCHG
Usuwanie kronikowanych zmian (Remove Journaled Changes)

RNMOBJ
Zmiana nazwy obiektu (Rename Object)

RST Odtworzenie obiektu w katalogu (Restore Object in Directory)

RSTCFG
Odtwarzanie obiektów konfiguracyjnych (Restore Configuration Objects)

RSTLIB
Odtworzenie biblioteki (Restore Library)

RSTLICPGM
Odtworzenie programu licencjonowanego (Restore Licensed Program)

RSTOBJ
Odtworzenie obiektu (Restore Object)

RVKOBJAUT
Odwołanie uprawnień dla obiektu (Revoke Object Authority)

STRJRNxxx
Uruchomienie kronikowania (Start Journaling)

- Operacje, które nie są kontrolowane

Podpowiedź (Prompt) [2]
Program przesłonięcia podpowiedzi dla komendy zmiany (jeśli istnieje)

CHKOBJ
Sprawdzenie obiektu (Check Object)

ALCOBJ
Przydzielenie obiektu (Allocate Object)

CPROBJ
Kompresja obiektu (Compress Object)

DCPOBJ
Dekompresja obiektu (Decompress Object)

DLCOBJ
Zwolnienie obiektu (Deallocate Object)

DSPOBJD
Wyświetlenie opisu obiektu (Display Object Description)

DSPOBJAUT
Wyświetlenie uprawnień dla obiektu (Display Object Authority)

EDTOBJAUT
Edycja uprawnień dla obiektu (Edit Object Authority)

Uwaga: Jeśli zmieniane są uprawnienia do obiektu a kontrola obiektu obejmuje *SECURITY lub obiekt jest kontrolowany, zapisywany jest rekord kontroli.

QSYCUSRA
Sprawdzenie uprawnień użytkownika do funkcji API obiektu

QSYLUSRA
Lista użytkowników autoryzowanych do funkcji API obiektu. Rekord kontroli nie jest zapisywany dla obiektów, których uprawnienia znajdują się na liście. Rekord kontroli zapisywany jest dla przestrzeni użytkownika, w której zostały umieszczone informacje.

QSYRUSRA
Odtwarzanie uprawnień użytkownika do funkcji API obiektu

RCLTMPSTG
Odzyskiwanie pamięci tymczasowej (Reclaim Temporary Storage)

---

2. Gdy wymagana jest podpowiedź dla komendy, program przesłonięcia podpowiedzi wyświetla bieżące wartości. Na przykład jeśli wpisana zostanie komenda CHGURSPRF USERA i naciśnięty zostanie klawisz F4 (podpowiedź), ekran Zmiana profilu użytkownika wyświetli bieżące wartości dla profilu użytkownika USERA.

RTVOBJD
Odtworzenie opisu obiektu (Retrieve Object Description)

SAVSTG
Składowanie pamięci (Save Storage) (tylko kontrola komendy SAVSTG)

WRKOBJLCK
Praca z blokadami obiektów (Work with Object Locks)

WRKOBJOWN
Praca z obiektami wg właścicieli (Work with Objects by Owner)

WRKxxx
Praca z komendami obiektu (Work with object commands)

Operacje dotyczące czasu odzyskiwania ścieżki dostępu:

Uwaga: Zmiany czasu odzyskiwania ścieżki dostępu są kontrolowane, gdy wartość systemowa kontroli działania (QAUDLVL) lub parametr kontroli działania (AUDLVL) w profilu użytkownika zawiera wartość *SYSMGT.

- Kontrolowane Operacje

  CHGRCYAP
  Zmiana odzyskiwania ścieżek dostępu (Change Recovery for Access Paths)

  EDTRCYAP
  Edycja odzyskiwania ścieżek dostępu (Edit Recovery for Access Paths)

- Operacje, które nie są kontrolowane

  DSPRCYAP
  Wyświetlenie odzyskiwania ścieżek dostępu (Display Recovery for Access Paths)

Operacje dotyczące tabeli alertów (*ALRTBL):

- Odczyt

  Brak

- Zmiana

  ADDALRD
  Dodanie opisu alertu (Add Alert Description)

  CHGALRD
  Zmiana opisu alertu (Change Alert Description)

  CHGALRTBL
  Zmiana tabeli alertów (Change Alert Table)

  RMVALRD
  Usuwanie opisu alertu (Remove Alert Description)

- Operacje, które nie są kontrolowane

  Drukowanie (Print)
  Drukowanie opisu alertu

  WRKALRD
  Praca z opisem alertu (Work with Alert Description)

  WRKALRTBL
  Praca z tabelami alertów (Work with Alert Table)

Operacje dotyczące listy autoryzacji (*AUTL):

- Odczyt

Brak

- Zmiana

  ADDAUTLE
  Dodanie pozycji listy autoryzacji (Add Authorization List Entry)

  CHGAUTLE
  Zmiana pozycji listy autoryzacji (Change Authorization List Entry)

  EDTAUTL
  Edycja listy autoryzacji (Edit Authorization List)

  RMVAUTLE
  Usunięcie pozycji listy autoryzacji (Remove Authorization List Entry)

- Operacje, które nie są kontrolowane

  DSPAUTL
  Wyświetlenie listy autoryzacji (Display Authorization List)

  DSPAUTLOBJ
  Wyświetlenie obiektów listy autoryzacji (Display Authorization List Objects)

  DSPAUTLDLO
  Wyświetlenie listy autoryzacji obiektu DLO (Display Authorization List DLO)

  RTVAUTLE
  Odtworzenie pozycji listy autoryzacji (Retrieve Authorization List Entry)

  QSYLATLO
  Wyświetlenie listy obiektów zabezpieczonych przez funkcję API *AUTL

  WRKAUTL
  Praca z listami autoryzacji (Work with authorization lists)

Operacje dotyczące magazynu uprawnień (*AUTHLR):

- Odczyt

  Brak

- Zmiana

  Powiązana
  Gdy jest używana do zabezpieczenia obiektu.

- Operacje, które nie są kontrolowane

  DSPAUTHLR
  Wyświetlenie magazynu uprawnień (Display Authority Holder)

Operacje dotyczące katalogu konsolidacji (*BNDDIR):

- Odczyt

  CRTPGM
  Tworzenie programu (Create Program)

  CRTSRVPGM
  Tworzenie programu usługowego (Create Service Program)

  RTVBNDSRC
  Odtworzenie źródła konsolidacji (Retrieve Binder Source)

  UPDPGM
  Aktualizacja programu (Update Program)

UPDSRVPGM
Aktualizacja programu usługowego (Update Service Program)

- Zmiana

ADDBNDDIRE
Dodanie pozycji do katalogu konsolidacji (Add Binding Directory Entries)

RMVBNDDIRE
Usuwanie pozycji katalogu konsolidacji (Remove Binding Directory Entries)

- Operacje, które nie są kontrolowane

DSPBNDDIR
Wyświetlenie zawartości katalogu konsolidacji (Display the contents of a binding directory)

WRKBNDDIR
Praca z katalogiem konsolidacji (Work with Binding Directory)

WRKBNDDIRE
Praca z pozycjami katalogu konsolidacji (Work with Binding Directory Entry)

Operacje dotyczące listy konfiguracji (*CFGL):

- Odczyt

CPYCFGL
Kopiowanie listy konfiguracji (Copy Configuration List). Pozycja zapisywana jest dla *źródłowej_listy_konfiguracji*

- Zmiana

ADDCFGLE
Dodanie pozycji do listy konfiguracji (Add Configuration List Entries)

CHGCFGL
Zmiana listy konfiguracji (Change Configuration List)

CHGCFGLE
Zmiana pozycji listy konfiguracji (Change Configuration List Entry)

RMVCFGLE
Usuwanie pozycji listy konfiguracji (Remove Configuration List Entry)

- Operacje, które nie są kontrolowane

DSPCFGL
Wyświetlenie listy konfiguracji (Display Configuration List)

WRKCFGL
Praca z listami konfiguracji (Work with Configuration Lists)

Operacje dotyczące plików specjalnych (*CHRSF):

Informacje dotyczące kontrolowania plików specjalnych (*CHRSF) zawiera sekcja Operacje dotyczące pliku strumieniowego (*STMF).

Operacje dotyczące formatu wykresu (*CHTFMT):

- Odczyt

Wyświetlenie (Display)
Komenda DSPCHT lub opcja F10 menu programu BGU

Drukowanie/nakreślanie (Print/Plot)
Komenda DSPCHT lub opcja F15 menu programu BGU

Składowanie/Tworzenie (Save/Create)
Składowanie lub tworzenie zbioru danych graficznych (GDF) za pomocą komendy CRTGDF lub opcji F13 menu programu BGU

- Zmiana

  Brak

- Operacje, które nie są kontrolowane

  Brak

Operacje dotyczące opisu żądania zmiany (*CRQD):

- Odczyt

  QFVLSTA
  Funkcja API List Change Request Description Activities

  QFVRTVCD
  Funkcja API Retrieve Change Request Description

  SBMCRQ
  Wprowadzenie żądania CRQ (Submit Change Request)

- Zmiana

  ADDCMDCRQA
  Dodanie działania CRQ komend (Add Command Change Request Activity)

  ADDOBJCRQA
  Dodanie działania CRQ obiektu (Add Object Change Request Activity)

  ADDPRDCRQA
  Dodanie działania CRQ produktu (Add Product Change Request Activity)

  ADDPTFCRQA
  Dodanie działania CRQ poprawki PTF (Add PTF Change Request Activity)

  ADDRSCCRQA
  Dodanie działania CRQ zasobu (Add Resource Change Request Activity)

  CHGCMDCRQA
  Zmiana działania CRQ komend (Change Command Change Request Activity)

  CHGCRQD
  Zmiana opisu CRQ (Change Change Request Description)

  CHGOBJCRQA
  Zmiana działania CRQ obiektu (Change Object Change Request Activity)

  CHGPRDCRQA
  Zmiana działania CRQ produktu (Change Product Change Request Activity)

  CHGPTFCRQA
  Zmiana działania CRQ poprawki PTF (Change PTF Change Request Activity)

  CHGRSCCRQA
  Zmiana działania CRQ zasobu (Change Resource Change Request Activity)

  QFVADDA
  Funkcja API Add Change Request Description Activity

  QFVRMVA
  Funkcja API Remove Change Request Description Activity

  RMVCRQDA
  Usuwanie działania CRQD (Remove Change Request Dscription Activity)

- Operacje, które nie są kontrolowane

  WRKCRQD
  Praca z opisami CRQ (Work with Change Request Description)

Operacje dotyczące opisu ustawień narodowych języka C (*CLD):

- Odczyt

  RTVCLDSRC
  Odtwarzanie źródła ustawień narodowych języka C (Retrieve C Locale Source)

  Setlocale
  Podczas działania programu w języku C, obiektu ustawień narodowych języka C można użyć korzystając z funkcji Setlocale.

- Zmiana

  Brak

- Operacje, które nie są kontrolowane

  Brak

Operacje dotyczące klasy (*CLS):

- Odczyt

  Brak

- Zmiana

  CHGCLS
  Zmiana klasy (Change Class)

- Operacje, które nie są kontrolowane

  Uruchomienie zadania (Job start)
  Kiedy jest używane przez zarządzanie pracą do uruchomienia zadania

  DSPCLS
  Wyświetlenie klasy (Display Class)

  WRKCLS
  Praca z klasami (Work with Classes)

Operacje dotyczące komendy (*CMD):

- Odczyt

  Uruchomienie (Run)
  Gdy komenda jest uruchamiana

- Zmiana

  CHGCMD
  Zmiana komendy (Change Command)

  CHGCMDDFT
  Zmiana wartości domyślnych komendy (Change Command Default)

- Operacje, które nie są kontrolowane

  DSPCMD
  Wyświetlenie komendy (Display Command)

  PRTCMDUSG
  Drukowanie użycia komend (Print Command Usage)

  QCDRCMDI
  Funkcja API Retrieve Command Information

WRKCMD
Praca z komendami (Work with Commands)

Przedstawione poniżej komendy używane są w programach CL do kontrolowania przetwarzania oraz manipulowania danymi programu. Ich użycie nie jest kontrolowane.

CALL [1]	ENDPGM	RCVF
CALLPRC	ENDRCV	RETURN
CHGVAR	GOTO	SNDF
COPYRIGHT	IF	SNDRCVF
DCL	MONMSG	TFRCTL
DCLF	PGM	WAIT
DO		
ELSE		
ENDDO		

[1] Komenda CALL jest kontrolowana, gdy zostanie uruchomiona interaktywnie. Nie jest kontrolowana w przypadku uruchamiania w programie CL.

Operacje dotyczące listy połączeń (*CNNL):

- Odczyt

  Brak

- Zmiana

  ADDCNNLE
  Dodanie pozycji do listy połączeń (Add Connection List Entry)

  CHGCNNL
  Zmiana listy połączeń (Change Connection List)

  CHGCNNLE
  Zmiana pozycji listy połączeń (Change Connection List Entry)

  RMVCNNLE
  Usuwanie pozycji z listy połączeń (Remove Connection List Entry)

  RNMCNNLE
  Zmiana nazwy pozycji listy połączeń (Rename Connection List Entry)

- Operacje, które nie są kontrolowane

  Kopiowanie (Copy)
  Opcja 3 komendy WRKCNNL

  DSPCNNL
  Wyświetlenie listy połączeń (Display Connection List)

  RTVCFGSRC
  Odtworzenie źródła listy połączeń (Retrieve source of connection list)

  WRKCNNL
  Praca z listami połączeń (Work with Connection List)

  WRKCNNLE
  Praca z pozycjami listy połączeń (Work with Connection List Entry)

Operacje dotyczące opisu klasy usług (*COSD):

- Odczyt

  Brak

- Zmiana

CHGCOSD
Zmiana opisu klasy usług (Change Class-of-Service Description)

- Operacje, które nie są kontrolowane

DSPCOSD
Wyświetlenie opisu klasy usług (Display Class-of-Service Description)

RTVCFGSRC
Odtworzenie źródła opisu klasy usług (Retrieve source of class-of-service description)

WRKCOSD
Kopiowanie opisu klasy usług (Copy class-of-service description)

WRKCOSD
Praca z opisami klasy usług (Work Class-of-Service Description)

Operacje dotyczące informacji po stronie komunikacyjnej (*CSI):

- Odczyt

DSPCSI
Wyświetlenie informacji po stronie komunikacyjnej (Display Communications Side Information)

Inicjowanie (Initialize)
Inicjowanie konwersacji (Initialize conversation)

- Zmiana

CHGCSI
Zmiana informacji po stronie komunikacyjnej (Change Communications Side Information)

- Operacje, które nie są kontrolowane

WRKCSI
Praca z informacjami po stronie komunikacyjnej (Work with Communications Side Information)

Operacje dotyczące międzysystemowej mapy produktów systemu (*CSPMAP):

- Odczyt

Odniesienie (Reference)
Gdy dotyczy aplikacji CSP

- Zmiana

Brak

- Operacje, które nie są kontrolowane

DSPCSPOBJ
Wyświetlenie obiektu CSP (Display CSP Object)

WRKOBJCSP
Praca z obiektami dla CSP (Work with Objects for CSP)

Operacje dotyczące międzysystemowej tabeli produktów (*CSPTBL):

- Odczyt

Odniesienie (Reference)
Gdy dotyczy aplikacji CSP

- Zmiana

Brak

- Operacje, które nie są kontrolowane

DSPCSPOBJ
Wyświetlenie obiektu CSP (Display CSP Object)

WRKOBJCSP
Praca z obiektami dla CSP (Work with Objects for CSP)

Operacje dotyczące opisu kontrolera (*CTLD):

- Odczyt

  SAVCFG
  Składowanie konfiguracji (Save Configuration)

  VFYCMN
  Testowanie łącza (Link test)

- Zmiana

  CHGCTLxxx
  Zmiana opisu kontrolera (Change controller description)

  VRYCFG
  Udostępnianie lub blokowanie opisu kontrolera (Vary controller description on or off)

- Operacje, które nie są kontrolowane

  DSPCTLD
  Wyświetlenie opisu kontrolera (Display Controller Description)

  ENDCTLRCY
  Zakończenie odzyskiwania kontrolera (End Controller Recovery)

  PRTDEVADR
  Drukowanie adresów urządzenia (Print Device Address)

  RSMCTLRCY
  Wznowienie odzyskiwania kontrolera (Resume Controller Recovery)

  RTVCFGSRC
  Odtworzenie źródła opisu kontrolera (Retrieve source of controller description)

  RTVCFGSTS
  Odtworzenie statusu opisu kontrolera (Retrieve controller description status)

  WRKCTLD
  Kopiowanie opisu kontrolera (Copy controller description)

  WRKCTLD
  Praca z opisem kontrolera (Work with Controller Description)

Operacje dotyczące opisu urządzenia (*DEVD):

- Odczyt

  Uzyskiwanie (Acquire)
  Najpierw należy uzyskać urządzenie podczas operacji otwierania lub jawnie uzyskać operację

  Przydzielanie (Allocate)
  Przydzielanie konwersacji (Allocate conversation)

  SAVCFG
  Składowanie konfiguracji (Save Configuration)

  STRPASTHR
  Uruchomienie sesji tranzytu (Start pass-through session)

  Uruchomienie drugiej sesji dla tranzytu pośredniego (Start of the second session for intermediate pass-through)

  VFYCMN
  Testowanie łącza (Link test)

Kontrola obiektów

- Zmiana

  CHGDEVxxx
  Zmiana opisu urządzenia (Change device description)

  HLDDEVxxx
  Wstrzymanie opisu urządzenia (Hold device description)

  RLSDEVxxx
  Zwolnienie opisu urządzenia (Release device description)

  QWSSETWS
  Zmiana ustawienia buforowania dla urządzenia (Change type-ahead setting for a device)

  VRYCFG
  Udostępnianie lub blokowanie opisu urządzenia (Vary device description on or off)
- Operacje, które nie są kontrolowane

  DSPDEVD
  Wyświetlenie opisu urządzenia (Display Device Description)

  DSPMODSTS
  Wyświetlenie statusu trybu (Display Mode Status)

  ENDDEVRCY
  Zakończenie odzyskiwania urządzenia (End Device Recovery)

  HLDCMNDEV
  Wstrzymanie urządzenia komunikacyjnego (Hold Communications Device)

  RLSCMNDEV
  Zwolnienie urządzenia komunikacyjnego (Release Communications Device)

  RSMDEVRCY
  Wznowienie odzyskiwania urządzenia (Resume Device Recovery)

  RTVCFGSRC
  Odtworzenie źródła opisu urządzenia (Retrieve source of device description)

  RTVCFGSTS
  Odtworzenie statusu opisu urządzenia (Retrieve device description status)

  WRKCFGSTS
  Praca ze statusem urządzenia (Work with device status)

  WRKDEVD
  Kopiowanie opisu urządzenia (Copy device description)

  WRKDEVD
  Praca z opisem urządzenia (Work with Device Description)

Operacje dotycząca katalogu (*DIR):

- Operacje odczytu/wyszukiwania

  access, accessx, QlgAccess, QlgAccessx
  Określenie dostępności zbioru (Determine file accessibility)

  CHGATR
  Zmiana atrybutu (Change Attribute)

  CPY Kopiowanie obiektu (Copy Object)

  DSPCURDIR
  Wyświetlenie bieżącego katalogu (Display Current Directory)

DSPLNK
Wyświetlenie dowiązań (Display Links)

faccessx
Określenie dostępności zbioru dla klasy użytkowników przez deskrytpor

getcwd, qlgGetcwd
Funkcja API Get Path Name of Current Directory

givedescriptor
Funkcja API Give File Access

Qp0lGetAttr, QlgGetAttr
Funkcje API Get attributes

Qp0lGetPathFromFileID, QlgGetPathFromFileID
Funkcje API Get Path From File Identifier

Qp0lProcessSubtree, QlgProcessSubtree
Funkcje API Process a Path Name

open, open64, QlgOpen, QlgOpen64, Qp0lOpen
Funkcje API Open File

Qp0lSetAttr, QlgSetAttr
Funkcje API Set Attributes

opendir, QlgOpendir
Funkcje API Open Directory

RTVCURDIR
Odtworzenie bieżącego katalogu (Retrieve Current Directory)

SAV Składowanie (Save)

WRKLNK
Praca z dowiązaniami (Work with Links)

- Zmiana

CHGATR
Zmiana atrybutów (Change Attributes)

CHGAUD
Zmiana kontroli (Change Auditing)

CHGAUT
Zmiana uprawnień (Change Authority)

CHGOWN
Zmiana właściciela (Change Owner)

CHGPGP
Zmiana grupy podstawowej (Change Primary Group)

chmod, QlgChmod
Funkcja API Change File Authorizations

chown, QlgChown
Funkcja API Change Owner and Group

CPY Kopiowanie (Copy)

CRTDIR
Tworzenie katalogu (Create Directory)

fchmod
Funkcja API Change File Authorizations by Descriptor

fchown
Funkcja API Change Owner and Group of File by Descriptor

givedescriptor
Funkcja API Give File Access

mkdir, QlgMkdir
Funkcja API Make Directory

MOV Przeniesienie (Move)

Qp0lRenameKeep, QlgRenameKeep
Funkcje API Rename File or Directory, Keep New

Qp0lRenameUnlink, QlgRenameUnlink
Funkcje API Rename File or Directory, Unlink New

Qp0lSetAttr, QlgSetAttr
Funkcja API Set Attribute

rmdir, QlgRmdir
Funkcja API Remove Directory

RMVDIR
Usuwanie katalogu (Remove Directory)

RNM Zmiana nazwy (Rename)

RST Odtwarzanie (Restore)

utime, QlgUtime
Funkcja API Set File Access and Modifcation Times

WRKAUT
Praca z uprawnieniami (Work with Authority)

WRKLNK
Praca z dowiązaniami (Work with Links)

- Operacje, które nie są kontrolowane
-

chdir, QlgChdir
Funkcja API Change Directory

CHGCURDIR
Zmiana bieżącego katalogu (Change Current Directory)

close Funkcja API Close File Descriptor

closedir
Funkcja API Close Directory

DSPAUT
Wyświetlenie uprawnień (Display Authority)

dup Funkcja API Duplicate Open File Descriptor

dup2 Funkcja API Duplicate Open File Descriptor to Another Descriptor

faccessx
Określenie dostępności zbioru dla klasy użytkowników przez deskrytpor

fchdir Zmiana bieżącego katalogu przez deskryptor

fcntl Funkcja API Perform File Control Command

fpathconf
Funkcja API Get Configurable Path Name Variables by Descriptor

fstat, fstat64
Funkcje API Get File Information by Descriptor

givedescriptor
Funkcja API Give File Access

ioctl Funkcja API Perform I/O Control Request

lseek, lseek64
Funkcje API Set File Read/Write Offset

lstat, lstat64, QlgLstat, QlgLstat64
Funkcje API Get File or Link Information

pathconf, QlgPathconf
Funkcja API Get Configurable Path Name Variables

readdir
Funkcja API Read Directory Entry

rewinddir
Funkcja API Reset Directory Stream

select Funkcja API Check I/O Status of Multiple File Descriptors

stat, QlgStat
Funkcja API Get File Information

takedescriptor
Funkcja API Take File Access

Operacje dotyczące serwera katalogów:

Uwaga: Operacje serwera katalogów są kontrolowane, jeśli wartość systemowa kontroli działania (QAUDLVL) lub parametr kontroli działania (AUDLVL) w profilu użytkownika zawiera wartość *OFCSRV.

- Kontrolowane Operacje

Dodawanie (Add)
Dodawanie nowych pozycji do katalogu

Zmiana (Change)
Zmiana szczegółów pozycji w katalogu

Usunięcie (Delete)
Usunięcie pozycji w katalogu

Zmiana nazwy (Rename)
Zmienianie nazwy pozycji w katalogu

Drukowanie (Print)
Wyświetlanie lub drukowanie szczegółów pozycji w katalogu

Wyświetlanie lub drukowanie szczegółów wydziału

Wyświetlanie lub drukowanie pozycji w katalogu jako wyniku wyszukiwania

RTVDIRE
Odtworzenie pozycji katalogu

Zbieranie (Collect)
Zbieranie danych pozycji katalogu za pomocą tworzenia cienia katalogu

Dostarczenie (Supply)
Dostarczenie danych pozycji katalogu za pomocą tworzenia cienia katalogu

- Operacje, które nie są kontrolowane

Komendy CL
Komendy CL, które działają na katalogu, mogą być kontrolowane oddzielnie za pomocą funkcji kontrolowania obiektu.

Uwaga: Niektóre komendy CL katalogu powodują powstanie rekordu kontroli, ponieważ wykonują funkcje, które są kontrolowane przez wartość kontolowania działania *OFCSRV, takie jak dodawanie pozycji w katalogu.

CHGSYSDIRA
Zmiana atrybutów katalogu systemowego (Change System Directory Attributes)

Wydziały (Departments)
Dodawanie, zmiana, usunięcie lub wyświetlenie danych katalogu wydziału

Opisy (Descriptions)
Przypisywanie opisu do różnych pozycji katalogu za pomocą opcji 8 z panelu WRKDIR.

Dodawanie, zmiana lub usunięcie opisów pozycji katalogu

Listy dystrybucyjne (Distribution lists)
Dodawanie, zmiana, zmiana nazwy lub usunięcie list dystrybucyjnych

ENDDIRSHD
Zakończenie tworzenia cienia katalogu (End Directory Shadowing)

Lista (List)
Wyświetlanie lub drukowanie listy pozycji katalogu, które nie zawierają szczegółów pozycji katalogu, na przykład za pomocą komendy WRKDIRE lub przycisku F4 do wybrania pozycji w celu wysłania uwagi.

Położenia (Locations)
Dodawanie, zmiana, usunięcie lub wyświetlenie danych o położeniu katalogu

Pseudonim (Nickname)
Dodawanie, zmiana, zmiana nazwy lub usunięcie pseudonimów

Wyszukiwanie (Search)
Wyszukiwanie pozycji katalogu

STRDIRSHD
Uruchomienie tworzenia cienia katalogu (Start Directory Shadowing)

Operacje dotyczące obiektu biblioteki dokumentów (*DOC lub *FLR):

- Odczyt

CHKDOC
Sprawdzenie pisowni dokumentu (Check document spelling)

CPYDOC
Kopiowanie dokumentu (Copy Document)

DMPDLO
Zrzut obiektu DLO (Dump DLO)

DSPDLOAUD
Wyświetlenie kontroli DLO (Display DLO Auditing)

Uwaga: Jeśli informacje kontroli wyświetlane są dla wszystkich dokumentów w folderze oraz dla folderu określono kontrolowanie obiektu, zapisywany jest rekord kontroli. Wyświetlanie informacji kontroli obiektu dla pojedynczych dokumentów nie powoduje zapisania rekordu kontroli.

DSPDLOAUT
Wyświetlenie uprawnień dla DLO (Display DLO Authority)

DSPDOC
Wyświetlenie dokumentu (Display Document)

DSPHLPDOC
Wyświetlenie dokumentu pomocy (Display Help Document)

EDTDLOAUT
Edycja uprawnień dla DLO (Edit DLO Authority)

MRGDOC
Scalanie dokumentu (Merge Document)

PRTDOC
Drukowanie dokumentu (Print Document)

QHFCPYSF
Funkcja API Copy Stream File

QHFGETSZ
Funkcja API Get Stream File Size

QHFRDDR
Funkcja API Read Directory Entry

QHFRDSF
Funkcja API Read Stream File

RTVDOC
Odtworzenie dokumentu (Retrieve Document)

SAVDLO
Składowanie obiektu DLO (Save DLO)

SAVSHF
Składowanie półki (Save Bookshelf)

SNDDOC
Wysłanie dokumentu (Send Document)

SNDDST
Wysłanie dystrybucji (Send Distribution)

WRKDOC
Praca z dokumentami (Work with Documents)

Uwaga: Dla folderu zawierającego dokumentu zapisywana jest pozycja odczytu.

- Zmiana

ADDDLOAUT
Dodanie uprawnień dla DLO (Add DLO Authority)

ADDOFCENR
Dodanie rejestracji biurowej (Add Office Enrollment)

CHGDLOAUD
Zmiana kontroli DLO (Change DLO Auditing)

CHGDLOAUT
Zmiana uprawnień dla DLO (Change DLO Authority)

CHGDLOOWN
Zmiana prawa własności dla DLO (Change DLO Ownership)

Kontrola obiektów

CHGDLOPGP
Zmiana grupy podstawowej DLO (Change DLO Primary Group)

CHGDOCD
Zmiana opisu dokumentu (Change Document Description)

CHGDSTD
Zmiana opisu dystrybucji (Change Distribution Description)

CPYDOC [3]
Kopiowanie dokumentu (Copy Document)

Uwaga: Jeśli dokument docelowy już istnieje, zapisywana jest pozycja zmiany.

CRTFLR
Tworzenie folderu (Create Folder)

CVTTOFLR [3]
Konwersja do folderu (Convert to Folder)

DLTDLO [3]
Usunięcie obiektu DLO (Delete DLO)

DLTSHF
Usunięcie półki (Delete Bookshelf)

DTLDOCL [3]
Usunięcie listy dokumentów (Delete Document List)

DLTDST [3]
Usunięcie dystrybucji (Delete Distribution)

EDTDLOAUT
Edycja uprawnień dla DLO (Edit DLO Authority)

EDTDOC
Edycja dokumentu (Edit Document)

FILDOC [3]
Zapisanie dokumentu (File Document)

GRTACCAUT
Nadanie uprawnień dla kodu dostępu (Grant Access Code Authority)

GRTUSRPMN
Nadanie uprawnień specjalnych użytkowników (Grant User Permission)

MOVDOC [3]
Przeniesienie dokumentu (Move Document)

MRGDOC [3]
Scalanie dokumentu (Merge Document)

PAGDOC
Stronicowanie dokumentu (Paginate Document)

QHFCHGAT
Funkcja API Change Directory Entry Attributes

QHFSETSZ
Funkcja API Set Stream File Size

---

3. Jeśli dokument docelowy dla operacji znajduje się w folderze, pozycja zmiany zapisywana jest zarówno dla dokumentu jak i dla folderu.

QHFWRTSF
Funkcja API Write Stream File

QRYDOCLIB [3]
Zapytanie o biblioteki dokumentów (Query Document Library)

Uwaga: Jeśli zastępowany jest odszukany istniejący dokument, zapisywana jest pozycja zmiany.

RCVDST [3]
Pobranie dystrybucji (Receive Distribution)

RGZDLO
Reorganizacja obiektu DLO (Reorganize DLO)

RMVACC
Usunięcie kodu dostępu dla wszystkich obiektów DLO, do których jest on podłączony

RMVDLOAUT
Usuwanie uprawnień dla DLO (Remove DLO authority)

RNMDLO [3]
Zmiana nazwy obiektu DLO (Rename DLO)

RPLDOC
Zastąpienie dokumentu (Replace Document)

RSTDLO [3]
Odtworzenie obiektu DLO (Restore DLO)

RSTSHF
Odtwarzanie półki (Restore Bookshelf)

RTVDOC
Odtworzenie dokumentu (pobranie) (Retrieve Document (check out))

RVKACCAUT
Odwołanie uprawnień dla kodów dostępu (Revoke Access Code Authority)

RVKUSRPMN
Odwołanie uprawnień specjalnych użytkowników (Revoke User Permission)

SAVDLO[3]
Składowanie obiektu DLO (Save DLO)

- Operacje, które nie są kontrolowane

ADDACC
Dodanie kodu dostępu (Add Access Code)

DSPACC
Wyświetlenie kodów dostępu (Display Access Code)

DSPUSRPMN
Wyświetlenie uprawnień specjalnych użytkowników (Display User Permission)

QHFCHGFP
Funkcja API Change File Pointer

QHFCLODR
Funkcja API Close Directory

QHFCLOSF
Funkcja API Close Stream File

QHFFRCSF
Funkcja API Force Buffered Data

QHFLULSF
Funkcja API Lock/Unlock Stream File Range

QHFRTVAT
Funkcja API Retrieve Directory Entry Attributes

RCLDLO
Odzyskiwanie dokumentu DLO (Reclaim DLO) (*ALL lub *INT)

WRKDOCLIB
Praca z bibliotekami dokumentów (Work with Document Library)

WRKDOCPRTQ
Praca z kolejką wydruków dokumentów (Work with Document Print Queue)

Operacje dotyczące obszaru danych (*DTAARA):

- Odczyt

  DSPDTAARA
  Wyświetlenie obszaru danych (Display Data Area)

  RCVDTAARA
  Pobranie obszaru danych (Receive Data Area) (komenda S/38)

  RTVDTAARA
  Odtworzenie obszaru danych (Retrieve Data Area)

  QWCRDTAA
  Funkcja API Retrieve Data Area

- Zmiana

  CHGDTAARA
  Zmiana obszaru danych (Change Data Area)

  SNDDTAARA
  Wysłanie obszaru danych (Send Data Area)

- Operacje, które nie są kontrolowane

  Obszary danych (Data Areas)
  Lokalny obszar danych, grupowy obszar danych, obszar danych PIP (Program Initialization Parameter - parametr inicjalizacyjny programu)

  WRKDTAARA
  Praca z obszarami danych (Work with Data Area)

Operacje dotycząca narzędzia IDDU (*DTADCT):

- Odczyt

  Brak

- Zmiana

  Tworzenie (Create)
  Słownik danych i definicje danych

  Zmiana (Change)
  Słownik danych i definicje danych

  Kopiowanie (Copy)
  Definicje danych (zapisane jako tworzone)

  Usunięcie (Delete)
  Słownik danych i definicje danych

Zmiana nazwy (Rename)
Definicje danych

- Operacje, które nie są kontrolowane

Wyświetlenie (Display)
Słownik danych i definicje danych

LNKDTADFN
Utworzenie i usunięcie dowiązań definicji zbioru (Linking and unlinking file definitions)

Drukowanie (Print)
Słownik danych, definicje danych oraz informacje o miejscu używania definicji danych

Operacje dotyczące kolejki danych (*DTAQ):

- Odczyt

QMHRDQM
Funkcja API Retrieve Data Queue Message

- Zmiana

QRCVDTAQ
Funkcja API Receive Data Queue

QSNDDTAQ
Funkcja API Send Data Queue

QCLRDTAQ
Funkcja API Clear Data Queue

- Operacje, które nie są kontrolowane

WRKDTAQ
Praca z kolejkami danych (Work with Data Queue)

QMHQRDQD
Funkcja API Retrieve Data Queue Description

Operacje dotyczące opisu edycji (*EDTD):

- Odczyt

DSPEDTD
Wyświetlenie opisu edycji (Display Edit Description)

QECCVTEC
Funkcja API Edit code expansion (za pomocą procedury QECEDITU)

- Zmiana

Brak

- Operacje, które nie są kontrolowane

WRKEDTD
Praca z opisami edycji (Work with Edit Descriptions)

QECEDT
Funkcja API Edit

QECCVTEW
Funkcja API do tłumaczenia Edit Work na Edit Mask

Operacje dotyczące rejestrowania wyjścia (*EXITRG):

- Odczyt

QUSRTVEI
Funkcja API Retrieve Exit Information

QusRetrieveExitInformation
Funkcja API Retrieve Exit Information

- Zmiana

ADDEXITPGM
Dodanie programu obsługi wyjścia (Add Exit Program)

QUSADDEP
Funkcja API Add Exit Program

QusAddExitProgram
Funkcja API Add Exit Program

QUSDRGPT
Funkcja API Deregister Exit Point

QusDeregisterExitPoint
Funkcja API Deregister Exit Point

QUSRGPT
Funkcja API Register Exit Point

QusRegisterExitPoint
Funkcja API Register Exit Point

QUSRMVEP
Funkcja API Remove Exit Program

QusRemoveExitProgram
Funkcja API Remove Exit Program

RMVEXITPGM
Usuwanie programu obsługi wyjścia (Remove Exit Program)

WRKREGINF
Praca z informacjami rejestracyjnymi (Work with Registration Information)

- Operacje, które nie są kontrolowane

Brak

Operacje dotyczące tabeli sterującej formularzy (*FCT):

- Dla obiektu typu *FCT operacje odczytu lub zmiany nie są kontrolowane.

Operacje dotyczące zbioru (*FILE):

- Odczyt

CPYF Kopiowanie zbioru (Copy File) (korzysta z operacji otwierania)

Otwieranie (Open)
Otwarcie zbioru do odczytu

DSPPFM
Wyświetlenie podzbioru fizycznego (Display Physical File Member) (korzysta z operacji otwierania)

Otwieranie (Open)
Otwarcie terminali MRT po otwarciu początkowym

CRTBSCF
Tworzenie zbioru BSC (Create BSC File) (korzysta z operacji otwierania)

CRTCMNF
Tworzenie zbioru komunikacyjnego (Create Communications File) (korzysta z operacji otwierania)

CRTDSPF
Tworzenie zbioru ekranowego (Create Display File) (korzysta z operacji otwierania)

CRTICFF
Tworzenie zbioru ICF (Create ICF File) (korzysta z operacji otwierania)

CRTMXDF
Tworzenie zbioru MXS (Create MXD File) (korzysta z operacji otwierania)

CRTPRTF
Tworzenie zbioru drukarkowego (Create Printer File) (korzysta z operacji otwierania)

CRTPF
Tworzenie zbioru fizycznego (Create Physical File) (korzysta z operacji otwierania)

CRTLF
Tworzenie zbioru logicznego (Create Logical File) (korzysta z operacji otwierania)

DSPMODSRC
Wyświetlenie kodu źródłowego modułu (Display Module Source) (korzysta z operacji otwierania)

STRDBG
Uruchomienie debugera (Start Debug) (korzysta z operacji otwierania)

QTEDBGS
Funkcja API Retrieve View Text

- Zmiana

Otwieranie (Open)
Otwieranie zbioru do modyfikacji

ADDBSCDEVE
(S/38E) Dodanie pozycji urządzenia BSC do zbioru MXD

ADDCMNDEVE
(S/38E) Dodanie pozycji urządzenia komunikacyjnego do zbioru MXD

ADDDSPDEVE
(S/38E) Dodanie pozycji terminalu do zbioru MXD

ADDICFDEVE
(S/38E) Dodanie pozycji urządzenia ICF do zbioru MXD

ADDLFM
Dodanie podzbioru zbioru logicznego (Add Logical File Member)

ADDPFCST
Dodanie ograniczenia zbioru fizycznego (Add Physical File Constraint)

ADDPFM
Dodanie podzbioru do zbioru fizycznego (Add Physical File Member)

ADDPFTRG
Dodanie wyzwalacza zbioru fizycznego (Add Physical File Trigger)

ADDPFVLM
Dodanie podzbioru o zmiennej długości do zbioru fizycznego (Add Physical File Variable Length Member)

APYJRNCHGX
Zastosowanie rozszerzenia zmian kroniki (Apply Journal Changes Extend)

CHGBSCF
Zmiana funkcji Bisync (Change Bisync function)

Kontrola obiektów

CHGCMNF
(S/38E) Zmiana zbioru komunikacyjnego (Change Communications File)

CHGDDMF
Zmiana zbioru DDM (Change DDM File)

CHGDKTF
Zmiana zbioru dyskietkowego (Change Diskette File)

CHGDSPF
Zmiana zbioru ekranowego (Change Display File)

CHGICFDEVE
Zmiana pozycji zbioru urządzenia ICF (Change ICF Device File Entry)

CHGICFF
Zmiana zbioru ICF (Change ICF File)

CHGMXDF
(S/38E) Zmiana zbioru MXD (Change Mixed Device File)

CHGLF
Zmiana zbioru logicznego (Change Logical File)

CHGLFM
Zmiana podzbioru logicznego (Change Logical File Member)

CHGPF
Zmiana zbioru fizycznego (Change Physical File)

CHGPFCST
Zmiana ograniczenia zbioru fizycznego (Change Physical File Constraint)

CHGPFM
Zmiana podzbioru fizycznego (Change Physical File Member)

CHGPRTF
Zmiana GQle drukarki (Change Printer Device GQle)

CHGSAVF
Zmiana zbioru składowania (Change Save File)

CHGS36PRCA
Zmiana atrybutów procedury S/36 (Change S/36 Procedure Attributes)

CHGS36SRCA
Zmiana atrybutów źródłowych S/36 (Change S/36 Source Attributes)

CHGTAPF
Zmiana zbioru napędu taśm (Change Tape Device File)

CLRPFM
Usuwanie zawartości podzbioru fizycznego (Clear Physical File Member)

CPYF Kopiowanie zbioru (Copy File) (otwieranie zbioru do modyfikacji, takich jak dodawanie rekordów, usuwanie zawartości podzbioru lub składowanie podzbioru)

EDTS36PRCA
Edycja atrybutów procedury S/36 (Edit S/36 Procedure Attributes)

EDTS36SRCA
Edycja atrybutów źródłowych S/36 (Edit S/36 Source Attributes)

INZPFM
Inicjowanie zawartości podzbioru zbioru fizycznego (Initialize Physical File Member)

JRNAP
(S/38E) Uruchomienie kronikowania ścieżek dostępu (Start Journal Access Path) (pozycja na zbiór)

JRNPF
(S/38E) Uruchomienie kronikowania zbioru fizycznego (Start Journal Physical File) (pozycja na zbiór)

RGZPFM
Reorganizacja podzbioru zbioru fizycznego (Reorganize Physical File Member)

RMVBSCDEVE
(S/38E) Usuwanie pozycji urządzenia BSC ze zbioru MXD (Remove BSC Device Entry from a mixed dev file)

RMVCMNDEVE
(S/38E) Usuwanie pozycji urządzenia CMN ze zbioru MXD (Remove CMN Device Entry from a mixed dev file)

RMVDSPDEVE
(S/38E) Usuwanie pozycji urządzenia DSP ze zbioru MXD (Remove DSP Device Entry from a mixed dev file)

RMVICFDEVE
(S/38E) Usuwanie pozycji urządzenia ICF ze zbioru ICM (Remove ICF Device Entry from an ICM dev file)

RMVM
Usuwanie podzbioru (Remove Member)

RMVPFCST
Usuwanie ograniczenia zbioru fizycznego (Remove Physical File Constraint)

RMVPFTGR
Usuwanie wyzwalacza zbioru fizycznego (Remove Physical File Trigger)

RNMM
Zmiana nazwy podzbioru (Rename Member)

WRKS36PRCA
Praca z atrybutami procedury S/36 (Work with S/36 Procedure Attributes)

WRKS36SRCA
Praca z atrybutami źródłowymi S/36 (Work with S/36 Source Attributes)

- Operacje, które nie są kontrolowane

DSPCPCST
Wyświetlenie sprawdzania ograniczeń w toku (Display Check Pending Constraints)

DSPFD
Wyświetlenie opisu zbioru (Display File Description)

DSPFFD
Wyświetlenie opisu pól zbioru (Display File Field Description)

DSPDBR
Wyświetlenie relacji bazy danych (Display Database Relations)

DSPPGMREF
Wyświetlenie odniesień programu (Display Program File References)

EDTCPCST
Edycja sprawdzania ograniczeń w toku (Edit Check Pending Constraints)

OVRxxx
Przesłonięcie zbioru (Override file)

RTVMBRD
Odtworzenie opisu podzbioru (Retrieve Member Description)

WRKPFCST
Praca z ograniczeniami zbioru fizycznego (Work with Physical File Constraints)

WRKF
Praca ze zbiorami (Work with File)

Operacje dotyczące zbiorów FIFO (*FIFO):

- Informacje dotyczące kontroli zbiorów *FIFO zawiera sekcja Operacje dotyczące pliku strumieniowego (*STMF).

Operacje dotyczące folderu (*FLR):

- Patrz Operacje dotyczące obiektu biblioteki dokumentów (*DOC lub *FLR)

Operacje dotyczące zasobu czcionki (*FNTRSC):

- Odczyt

  Drukowanie (Print)
  Drukowanie zbioru buforowego, który odnosi się do zasobu czcionki
- Zmiana

  Brak
- Operacje, które nie są kontrolowane

  WRKFNTRSC
  Praca z zasobami czcionek (Work with Font Resource)

  Drukowanie (Print)
  Odniesienie do zasobu czcionki podczas tworzenia zbioru buforowego

Operacje dotyczące definicji formularza (*FORMDF):

- Odczyt

  Drukowanie (Print)
  Drukowanie zbioru buforowego, który odnosi się do definicji formularza
- Zmiana

  Brak
- Operacje, które nie są kontrolowane

  WRKFORMDF
  Praca z definicjami formularzy (Work with Form Definition)

  Drukowanie (Print)
  Odniesienie do definicji formularza podczas tworzenia zbioru buforowego

Operacje dotyczące obiektu filtru (*FTR):

- Odczyt

  Brak
- Zmiana

  ADDALRACNE
  Dodanie pozycji działania dla alertu (Add Alert Action Entry)

  ADDALRSLTE
  Dodanie pozycji wyboru alertu (Add Alert Selection Entry)

ADDPRBACNE
Dodanie pozycji działania dla problemu (Add Problem Action Entry)

ADDPRBSLTE
Dodanie pozycji wyboru problemu (Add Problem Selection Entry)

CHGALRACNE
Zmiana pozycji działania dla alertu (Change Alert Action Entry)

CHGALRSLTE
Zmiana pozycji wyboru alertu (Change Alert Selection Entry)

CHGPRBACNE
Zmiana pozycji działania dla problemu (Change Problem Action Entry)

CHGPRBSLTE
Zmiana pozycji wyboru problemu (Change Problem Selection Entry)

CHGFTR
Zmiana filtru (Change Filter)

RMVFTRACNE
Usuwanie pozycji działania dla alertu (Remove Alert Action Entry)

RMVFTRSLTE
Usuwanie pozycji wyboru alertu (Remove Alert Selection Entry)

WRKFTRACNE
Praca z pozycją działania dla alertu (Work Alert Action Entry)

WRKFTRSLTE
Praca z pozycją wyboru alertu (Work Alert Selection Entry)

- Operacje, które nie są kontrolowane

  WRKFTR
  Praca z filtrami (Work with Filters)

  WRKFTRACNE
  Praca z pozycjami działań filtru (Work with Filter Action Entries)

  WRKFTRSLTE
  Praca z pozycjami wyboru filtru (Work with Filter Selection Entries)

Operacje dotyczące zestawu symboli graficznych (*GSS):

- Odczyt

  Załadowany (Loaded)
  Gdy jest załadowany

  Czcionka (Font)
  Gdy jest używany jako czcionka w zbiorze drukarkowym opisanym zewnętrznie

- Zmiana

  Brak

- Operacje, które nie są kontrolowane

  WRKGSS
  Praca ze zestawem symboli graficznych (Work with Graphic Symbol Set)

Operacje dotyczące słownika zestawu znaków dwubajtowych (*IGCDCT):

- Odczyt

  DSPIGCDCT
  Wyświetlenie słownika IGC (Display IGC Dictionary)

- Zmiana

  EDTIGCDCT
  Edycja słownika IGC (Edit IGC Dictionary)

Operacje dotyczące sortowania zestawu znaków dwubajtowych (*IGCSRT):

- Odczyt

  CPYIGCSRT
  Kopiowanie tabeli sortowania IGC (Copy IGC Sort) (*z_obiektu_*ICGSRT*)

  Konwersja (Conversion)
  Konwersja do formatu V3R1, jeśli jest konieczna

  Drukowanie (Print)
  Drukowanie znaku w celu zarejestrowania w tabeli sortowania (opcja 1 z menu CGU)

  Drukowanie przed usunięciem znaku z tabeli sortowania (opcja 2 z menu CGU)

- Zmiana

  CPYIGCSRT
  Kopiowanie tebeli sortowania IGC (Copy IGC Sort) (*do_obiektu_*ICGSRT*)

  Konwersja (Conversion)
  Konwersja do formatu V3R1, jeśli jest konieczna

  Tworzenie (Create)
  Tworzenie znaku zdefiniowanego przez użytkownika (opcja 1 z menu CGU)

  Usunięcie (Delete)
  Usunięcie znaku zdefiniowanego przez użytkownika (opcja 2 z menu CGU)

  Aktualizowanie (Update)
  Aktualizowanie aktywnej tabeli sortowania (opcja 5 z menu CGU)

- Operacje, które nie są kontrolowane

  FMTDTA
  Sortowanie rekordów lub pól w zbiorze

Operacje dotyczące tabeli zestawu znaków dwubajtowych (*IGCTBL):

- Odczyt

  CPYIGCTBL
  Kopiowanie tabeli IGC (Copy IGC Table)

  STRFMA
  Uruchomienie FMA (Start Font Management Aid)

- Zmiana

  STRFMA
  Uruchomienie FMA (Start Font Management Aid)

- Operacje, które nie są kontrolowane

  CHKIGCTBL
  Sprawdzanie tabeli IGC (Check IGC Table)

Operacje dotyczące opisu zadania (*JOBD):

- Odczyt

  Brak

- Zmiana

CHGJOBD
Zmiana opisu zadania (Change Job Description)

- Operacje, które nie są kontrolowane

DSPJOBD
Wyświetlenie opisu zadania (Display Job Description)

WRKJOBD
Praca z opisami zadań (Work with Job Descriptions)

QWDRJOBD
Funkcja API Retrieve Job Description

Zadanie wsadowe (Batch job)
Kiedy jest używane do uruchomienia zadania

Operacje dotyczące kolejki zadań (*JOBQ):

- Odczyt

Brak

- Zmiana

Pozycja (Entry)
Gdy pozycja jest umieszczana lub usuwana z kolejki

CLRJOBQ
Usuwanie zawartości kolejki zadań (Clear Job Queue)

HLDJOBQ
Wstrzymanie kolejki zadań (Hold Job Queue)

RLSJOBQ
Zwolnienie kolejki zadań (Release Job Queue)

- Operacje, które nie są kontrolowane

ADDJOBQE “Opisy podsystemów” na stronie 185
Dodanie pozycji kolejki zadań (Add Job Queue Entry)

CHGJOB
Zmiana zadania (Change Job) z zadania JOBQ na inne zadanie JOBQ

CHGJOBQE “Opisy podsystemów” na stronie 185
Zmiana pozycji kolejki zadań (Change Job Queue Entry)

QSPRJOBQ
Odtworzenie informacji kolejki zadań

RMVJOBQE “Opisy podsystemów” na stronie 185
Usuwanie pozycji kolejki zadań (Remove Job Queue Entry)

TFRJOB
Transfer Zadania (Transfer Job)

TFRBCHJOB
Transfer zadania wsadowego (Transfer Batch Job)

WRKJOBQ
Praca z kolejką zadań (Work with Job Queue) dla określonej kolejki zadań

WRKJOBQ
Praca z kolejką zadań (Work with Job Queue) dla wszystkich kolejek zadań

---

4. Jeśli dla opisu podsystemu (*SBSD) określono kontrolowanie obiektu, zapisywany jest obiekt kontroli.

Operacje dotyczące obiektu programu do planowania zadań (*JOBSCD):

- Odczyt

  Brak

- Zmiana

  ADDJOBSCDE
  Dodanie pozycji harmonogramu zadań (Add Job Schedule Entry)

  CHGJOBSCDE
  Zmiana pozycji harmonogramu zadań (Change Job Schedule Entry)

  RMVJOBSCDE
  Usuwanie pozycji harmonogramu zadań (Remove Job Schedule Entry)

  HLDJOBSCDE
  Wstrzymanie pozycji harmonogramu zadań (Hold Job Schedule Entry)

  RLSJOBSCDE
  Zwolnienie pozycji harmonogramu zadań (Release Job Schedule Entry)

- Operacje, które nie są kontrolowane

  Wyświetlenie (Display)
  Wyświetlenie szczegółów pozycji zaplanowanego zadania

  WRKJOBSCDE
  Praca z pozycjami harmonogramu zadań (Work with Job Schedule Entries)

  Praca z ...
  Praca z poprzednio wprowadzonymi zadaniami z pozycji harmonogramu zadań

  QWCLSCDE
  Funkcja API List job schedule entry

Operacje dotyczące kroniki (*JRN):

- Odczyt

  CMPJRNIMG
  Porównanie obrazów kroniki (Compare Journal Images)

  DSPJRN
  Wyświetlenie kroniki (Display Journal Entry) dla kronik użytkownika

  QJORJIDI
  Odtwarzanie informacji identyfikatora kroniki (JID) (Retrieve Journal Identifier (JID) Information)

  QjoRetrieveJournalEntries
  Odtworzenie pozycji kroniki (Retrieve Journal Entries)

  RCVJRNE
  Pobranie pozycji kroniki (Receive Journal Entry)

  RTVJRNE
  Odtworzenie pozycji kroniki (Retrieve Journal Entry)

- Zmiana

  ADDRMTJRN
  Dodanie zdalnej kroniki (Add Remote Journal)

  APYJRNCHG
  Zastosowanie kronikowanych zmian (Apply Journaled Changes)

  APYJRNCHGX
  Zastosowanie rozszerzenia zmian kroniki (Apply Journal Changes Extend)

CHGJRN
Zmiana kroniki (Change Journal)

CHGRMTJRN
Zmiana zdalnej kroniki (Change Remote Journal)

ENDJRNxxx
Zakończenie kronikowania (End Journaling)

JRNAP
(S/38E) Uruchomienie kronikowania ścieżek dostępu (Start Journal Access Path)

JRNPF
(S/38E) Uruchomienie kronikowania zbioru fizycznego (Start Journal Physical File)

QjoAddRemoteJournal
Funkcja API Add Remote Journal

QjoChangeJournalState
Funkcja API Change Journal State

QjoEndJournal
Funkcja API End Journaling

QjoRemoveRemoteJournal
Funkcja API Remove Remote Journal

QJOSJRNE
Funkcja API Send Journal Entry (pozycje użytkownika można wysyłać tylko za pomocą funkcji API QJOSJRNE)

QjoStartJournal
Funkcja API Start Journaling

RMVJRNCHG
Usuwanie kronikowanych zmian (Remove Journaled Changes)

RMVRMTJRN
Usuwanie zdalnej kroniki (Remove Remote Journal)

SNDJRNE
Wysłanie pozycji do kroniki (Send Journal Entry) (pozycje użytkownika można wysyłać tylko za pomocą komendy SNDJRNE)

STRJRNxxx
Uruchomienie kronikowania (Start Journaling)

- Operacje, które nie są kontrolowane

DSPJRN
Wyświetlenie pozycji kroniki (Display Journal Entry) dla wewnętrznych kronik systemowych, JRN(*INTSYSJRN)

DSPJRNA
(S/38E) Praca z atrybutami kroniki (Work with Journal Attributes)

DSPJRNMNU
(S/38E) Praca z kroniką (Work with Journal)

QjoRetrieveJournalInformation
Funkcja API Retrieve Journal Information

WRKJRN
Praca z kroniką (Work with Journal) (w środowisku S/38 - DSPJRNMNU)

WRKJRNA
Praca z atrybutami kroniki (Work with Journal Attributes) (w środowisku S/38 - DSPJRNA)

Kontrola obiektów

Operacje dotyczące dziennika (*JRNRCV):

- Odczyt

  Brak

- Zmiana

  CHGJRN
  Zmiana kroniki (Change Journal) (podczas podłączania nowych dzienników)

- Operacje, które nie są kontrolowane

  DSPJRNRCVA
  Wyświetlenie atrybutów dziennika (Display Journal Receiver Attributes)

  QjoRtvJrnReceiverInformation
  Funkcja API Retrieve Journal Receiver Information

  WRKJRNRCV
  Praca z dziennikami (Work with Journal Receiver)

Operacje dotyczące biblioteki (*LIB):

- Odczyt

  DSPLIB
  Wyświetlenie biblioteki (Display Library) (gdy nie jest pusta; jeśli jest pusta, nie jest przeprowadzana żadna kontrola.)

  Odnajdywanie (Locate)
  Gdy ma być odszukany obiekt

  Uwagi:

  1. Dla pojedynczej komendy, w przypadku biblioteki, może być zapisanych klika pozycji kontroli. Na przykład podczas otwierania zbioru pozycja kroniki kontroli ZR jest zapisywana za każdym razem, gdy system odszuka zbiór lub każdy podzbiór tego zbioru.
  2. Jeśli funkcja odszukiwania nie zostanie wykonana pomyślnie, nie jest zapisywana żadna pozycja kontroli. Na przykład uruchomiono komendę korzystając z ogólnego parametru:

     ```
     DSPOBJD OBJECT(AR*/*ALL) +
     OBJTYPE(*FILE)
     ```

     Jeśli biblioteka, której nazwa rozpoczyna się od liter “AR” nie zawiera żadnego zbioru rozpoczynającego się od “WRK”, nie jest dla niej zapisywany żaden rekord kontroli.

- Zmiana

  Lista bibliotek (Library list)
  Dodawanie biblioteki do listy bibliotek

  CHGLIB
  Zmiana biblioteki (Change Library)

  CLRLIB
  Usuwanie zawartości biblioteki (Clear Library)

  MOVOBJ
  Przeniesienie obiektu (Move Object)

  RNMOBJ
  Zmiana nazwy obiektu (Rename Object)

  Dodawanie (Add)
  Dodawanie obiektu do biblioteki

  Usunięcie (Delete)
  Usunięcie obiektu z biblioteki

- Operacje, które nie są kontrolowane

  Brak

Operacje dotyczące opisu linii (*LIND):

- Odczyt

  SAVCFG
  Składowanie konfiguracji (Save Configuration)

  RUNLPDA
  Uruchomienie komend operacyjnych LPDA-2 (Run LPDA-2 operational commands)

  VFYCMN
  Testowanie łącza (Link test)

  VFYLNKLPDA
  Testowanie łącza LPDA-2 (LPDA-2 link test)

- Zmiana

  CHGLINxxx
  Zmiana opisu linii (Change Line Description)

  VRYCFG
  Udostępnienie/zablokowanie opisu linii (Vary on/off line description)

- Operacje, które nie są kontrolowane

  ANSLIN
  Linia odpowiedzi (Answer Line)

  Kopiowanie (Copy)
  Opcja 3 komendy WRKLIND

  DSPLIND
  Wyświetlenie opisu linii (Display Line Description)

  ENDLINRCY
  Zakończenie odzyskiwania linii (End Line Recovery)

  RLSCMNDEV
  Zwolnienie urządzenia komunikacyjnego (Release Communications Device)

  RSMLINRCY
  Wznowienie odzyskiwania linii (Resume Line Recovery)

  RTVCFGSRC
  Odtworzenie źródła opisu linii (Retrieve Source of line description)

  RTVCFGSTS
  Odtworzenie statusu opisu linii (Retrieve line description status)

  WRKLIND
  Praca z opisami linii (Work with Line Descriptions)

  WRKCFGSTS
  Praca ze statusem opisu linii (Work with line description status)

Operacje dotyczące usług pocztowych:

Uwaga: Operacje usług pocztowych są kontrolowane, jeśli wartość systemowa kontroli działania (QAUDLVL) lub parametr kontroli działania (AUDLVL) w profilu użytkownika zawiera wartość *OFCSRV.

- Kontrolowane Operacje

Zmiana (Change)
Zmiany katalogu dystrybucyjnego systemu

W imieniu (On behalf)
Praca w imieniu innego użytkownika

Uwaga: Praca w imieniu innego użytkownika jest kontrolowana, jeśli wartość AUDLVL profilu użytkownika lub wartość systemowa QAUDLVL ma wartość *SECURITY.

Otwieranie (Open)
Rekord kontroli jest zapisywany podczas otwierania protokołu poczty

- Operacje, które nie są kontrolowane

Zmiana (Change)
Szczegóły zmiany pozycji poczty

Usunięcie (Delete)
Usunięcie pozycji poczty

Wprowadzanie (File)
Wprowadzanie pozycji poczty do dokumentu lub folderu

Uwaga: Po wprowadzeniu pozycja poczty staje się obiektem biblioteki dokumentów (document library object - DLO). Dla obiektu DLO można określić kontrolowanie obiektu.

Przekazanie (Forward)
Przekazywanie pozycji poczty

Drukowanie (Print)
Drukowanie pozycji poczty

Uwaga: Drukowanie pozycji poczty może być kontrolowane za pomocą poziomu kontroli *SPLFDTA lub *PRTDTA.

Odbieranie (Receive)
Odbieranie pozycji poczty

Odpowiadanie (Reply)
Odpowiadanie na pozycję poczty

Wysyłanie (Send)
Wysyłanie pozycji poczty

Przeglądanie (View)
Przeglądanie pozycji poczty

Operacje dotyczące menu (*MENU):

- Odczyt

Wyświetlenie (Display)
Wyświetlanie menu przy użyciu komendy GO MENU lub okna dialogowego UIM

- Zmiana

CHGMNU
Zmiana menu (Change Menu)

- Operacje, które nie są kontrolowane

Powrót (Return)
Powracanie do menu - w stosie menu - które było już wyświetlane

DSPMNUA
Wyświetlenie atrybutów menu (Display Menu Attributes)

WRKMNU
Praca z menu (Work with Menu)

Operacje dotyczące opisu trybu (*MODD):

- Odczyt

  Brak

- Zmiana

  CHGMODD
  Zmiana opisu trybu (Change Mode Description)

- Operacje, które nie są kontrolowane

  CHGSSNMAX
  Zmiana maksymalnej liczby sesji (Change session maximum)

  DSPMODD
  Wyświetlenie opisu trybu (Display Mode Description)

  ENDMOD
  Zakończenie trybu (End Mode)

  STRMOD
  Uruchomienie trybu (Start Mode)

  WRKMODD
  Praca z opisami trybów (Work with Mode Descriptions)

Operacje dotyczące obiektu modułu (*MODULE):

- Odczyt

  CRTPGM
  Pozycja kontroli dla każdego obiektu modułu używanego podczas CRTPGM.

  CRTSRVPGM
  Pozycja kontroli dla każdego obiektu modułu używanego podczas CRTSRVPGM.

  UPDPGM
  Pozycja kontroli dla każdego obiektu modułu używanego podczas UPDPGM.

  UPDSRVPGM
  Pozycja kontroli dla każdego obiektu modułu używanego podczas UPDSRVPGM.

- Zmiana

  CHGMOD
  Zmiana modułu (Change Module)

- Operacje, które nie są kontrolowane

  DSPMOD
  Wyświetlenie modułu (Display Module)

  RTVBNDSRC
  Odtworzenie źródła konsolidacji (Retrieve Binder Source)

  WRKMOD
  Praca z modułami (Work with Module)

Operacje dotyczące zbioru komunikatów (*MSGF):

- Odczyt

  DSPMSGD
  Wyświetlenie opisu komunikatu (Display Message Description)

MRGMSGF
Scalanie zbiorów komunikatów (Merge Message File) ze zbioru

Drukowanie (Print)
Drukowanie opisu komunikatu

RTVMSG
Odtworzenie informacji ze zbioru komunikatów

QMHRTVM
Funkcja API Retrieve Message

WRKMSGD
Praca z opisami komunikatów (Work with Message Description)

- Zmiana

ADDMSGD
Dodanie opisu komunikatu (Add Message Description)

CHGMSGD
Zmiana opisu komunikatu (Change Message Description)

CHGMSGF
Zmiana zbioru komunikatów (Change Message File)

MRGMSGF
Scalanie zbiorów komunikatów (Merge Message File) (do zbioru i zastąpienie MSGF)

RMVMSGD
Usuwanie opisu komunikatu (Remove Message Description)

- Operacje, które nie są kontrolowane

OVRMSGF
Przesłonięcie zbioru komunikatów (Override Message File)

WRKMSGF
Praca ze zbiorami komunikatów (Work with Message File)

QMHRMFAT
Funkcja API Retrieve Message File Attributes

Operacje dotyczące kolejki komunikatów (*MSGQ):

- Odczyt

QMHLSTM
Funkcja API List Nonprogram Messages

QMHRMQAT
Funkcja API Retrieve Nonprogram Message Queue Attributes

DSPLOG
Wyświetlenie protokołu (Display Log)

DSPMSG
Wyświetlenie komunikatów (Display Message)

Drukowanie (Print)
Drukowanie komunikatów

RCVMSG
Pobranie komunikatu (Receive Message) RMV(*NO)

QMHRCVM
Funkcja API Receive Nonprogram Messages, gdy działanie komunikatu nie ma wartości *REMOVE.

- Zmiana

  CHGMSGQ
  Zmiana kolejki komunikatów (Change Message Queue)

  CLRMSGQ
  Usuwanie zawartości kolejki komunikatów (Clear Message Queue)

  RCVMSG
  Pobranie komunikatu (Receive Message) RMV(*YES)

  QMHRCVM
  Funkcja API Receive Nonprogram Messages, gdy działanie komunikatu ma wartość *REMOVE.

  RMVMSG
  Usuwanie komunikatu (Remove Message)

  QMHRMVM
  Funkcja API Remove Nonprogram Messages

  SNDxxxMSG
  Wysyłanie komunikatu (Send a Message) do kolejki komunikatów

  QMHSNDBM
  Funkcja API Send Break Message

  QMHSNDM
  Funkcja API Send Nonprogram Message

  QMHSNDRM
  Funkcja API Send Reply Message

  SNDRPY
  Wysłanie odpowiedzi (Send Reply)

  WRKMSG
  Praca z komunikatami (Work with Message)
- Operacje, które nie są kontrolowane

  WRKMSGQ
  Praca z kolejkami komunikatów (Work with Message Queue)

  Programowanie (Program)
  Programowanie działania kolejki komunikatów

Operacje dotyczące grupy węzłów (*NODGRP):

- Odczyt

  DSPNODGRP
  Wyświetlenie grupy węzłów (Display Node Group)
- Zmiana

  CHGNODGRPA
  Zmiana grupy węzłów (Change Node Group)

Operacje dotyczące listy węzłów (*NODL):

- Odczyt

  QFVLSTNL
  Listowanie pozycji listy węzłów (List node list entries)
- Zmiana

  ADDNODLE
  Dodanie pozycji listy węzłów (Add Node List Entry)

RMVNODLE
Usuwanie pozycji listy węzłów (Remove Node List Entry)

- Operacje, które nie są kontrolowane

WRKNODL
Praca z listą węzłów (Work with Node List)

WRKNODLE
Praca z pozycjami listy węzłów (Work with Node List Entries)

Operacje dotyczące opisu NetBIOS (*NTBD):

- Odczyt

SAVCFG
Składowanie konfiguracji (Save Configuration)

- Zmiana

CHGNTBD
Zmiana opisu NetBIOS (Change NetBIOS Description)

- Operacje, które nie są kontrolowane

Kopiowanie (Copy)
Opcja 3 komendy WRKNTBD

DSPNTBD
Wyświetlenie opisu NetBIOS (Display NetBIOS Description)

RTVCFGSRC
Odtworzenie konfiguracji źródłowej (Retrieve Configuration Source) opisu NetBIOS

WRKNTBD
Praca z opisami NetBIOS (Work with NetBIOS Description)

Operacje dotyczące interfejsu sieciowego (*NWID):

- Odczyt

SAVCFG
Składowanie konfiguracji (Save Configuration)

- Zmiana

CHGNWIISDN
Zmiana opisu interfejsu sieciowego (Change Network Interface Description)

VRYCFG
Udostępnianie lub blokowanie opisu interfejsu sieciowego (Vary network description on or off)

- Operacje, które nie są kontrolowane

Kopiowanie (Copy)
Opcja 3 komendy WRKNWID

DSPNWID
Wyświetlenie opisu interfejsu sieciowego (Display Network Interface Description)

ENDNWIRCY
Zakończenie odzyskiwania interfejsu sieciowego (End Network Interface Recovery)

RSMNWIRCY
Wznowienie odzyskiwania interfejsu sieciowego (Resume Network Interface Recovery)

RTVCFGSRC
Odtworzenie źródła opisu interfejsu sieciowego (Retrieve Source of Network Interface Description)

RTVCFGSTS
Odtworzenie statusu opisu interfejsu sieciowego (Retrieve Status of Network Interface Description)

WRKNWID
Praca z opisami interfejsów sieciowych (Work with Network Interface Description)

WRKCFGSTS
Praca ze statusem opisu interfejsu sieciowego (Work with network interface description status)

Operacje dotyczące opisu serwera sieciowego (*NWSD):

- Odczyt

  SAVCFG
  Składowanie konfiguracji (Save Configuration)

- Zmiana

  CHGNWSD
  Zmiana opisu serwera sieciowego (Change Network Server Description)

  VRYCFG
  Zmiana statusu konfiguracji (Vary Configuration)

- Operacje, które nie są kontrolowane

  Kopiowanie (Copy)
  Opcja 3 komendy WRKNWSD

  DSPNWSD
  Wyświetlenie opisu serwera sieciowego (Display Network Server Description)

  RTVCFGSRC
  Odtworzenie konfiguracji źródłowej dla *NWSD (Retrieve Configuration Source for *NWSD)

  RTVCFGSTS
  Odtworzenie statusu konfiguracji dla *NWSD (Retrieve Configuration Status for *NWSD)

  WRKNWSD
  Praca z opisami serwerów sieciowych (Work with Network Server Description)

Operacje dotyczące kolejki wyjściowej (*OUTQ):

- Odczyt

  STRPRTWTR
  Uruchomienie programu piszącego drukarki dla OUTQ (Start a Printer Writer to an OUTQ)

  STRRMTWTR
  Uruchomienie zdalnego programu piszącego dla OUTQ (Start a Remote Writer to an OUTQ)

- Zmiana

  Umieszczenie (Placement)
  Gdy pozycja jest umieszczana lub usuwana z kolejki

  CHGOUTQ
  Zmiana kolejki wyjściowej (Change Output Queue)

  CHGSPLFA [5]
  Zmiana atrybutów zbioru buforowego (Change Spooled File Attributes), jeśli obiekt przenoszony jest do innej kolejki wyjściowej i ta kolejka jest kontrolowana

  CLROUTQ
  Usuwanie zawartości kolejki wyjściowej (Clear Output Queue)

  DLTSPLF [5]
  Usunięcie zbioru buforowego (Delete Spooled File)

HLDOUTQ
Wstrzymanie kolejki wyjściowej (Hold Output Queue)

RLSOUTQ
Zwolnienie kolejki wyjściowej (Release Output Queue)

- Operacje, które nie są kontrolowane

CHGSPLFA [5]
Zmiana atrybutów zbioru buforowego (Change Spooled File Attributes)

CPYSPLF [5]
Kopiowanie zbioru buforowego (Copy Spooled File)

Tworzenie (Create)[5]
Tworzenie zbioru buforowego

DSPSPLF [5]
Wyświetlenie zbioru buforowego (Display Spooled File)

HLDSPLF [5]
Wstrzymanie zbioru buforowego (Hold Spooled File)

QSPROUTQ
Odtwarzanie informacji kolejki wyjściowej (Retrieve output queue information)

RLSSPLF [5]
Zwolnienie zbioru buforowego (Release Spooled File)

SNDNETSPLF [5]
Wysłanie sieciowego zbioru buforowego (Send Network Spooled File)

WRKOUTQ
Praca z kolejką wyjściową (Work with Output Queue)

WRKOUTQD
Praca z opisem kolejki wyjściowej (Work with Output Queue Description)

WRKSPLF
Praca ze zbiorami buforowymi (Work with Spooled File)

WRKSPLFA
Praca z atrybutami zbiorów buforowych (Work with Spooled File Attributes)

Operacje dotyczące nakładek (*OVL):

- Odczyt

Drukowanie (Print)
Drukowanie zbioru buforowego, który odnosi się do nakładki

- Zmiana

Brak

- Operacje, które nie są kontrolowane

WRKOVL
Praca z nakładkami (Work with overlay)

Drukowanie (Print)
Odniesienie do nakładki podczas tworzenia zbioru buforowego

Operacje dotyczące definicji strony (*PAGDFN):

---

5. Kontrola ma miejsce również wtedy, gdy kontrolowanie działania (wartość systemowa QAUDLVL lub wartość AUDLVL w profilu użytkownika) obejmuje *SPLFDTA.

- Odczyt

  Drukowanie (Print)
  Drukowanie zbioru buforowego, który odnosi się do definicji strony
- Zmiana

  Brak
- Operacje, które nie są kontrolowane

  WRKPAGDFN
  Praca z definicjami stron (Work with Page Definition)

  Drukowanie (Print)
  Odniesienie do definicji formularza podczas tworzenia zbioru buforowego

Operacje dotyczące segmentu strony (*PAGSEG):

- Odczyt

  Drukowanie (Print)
  Drukowanie zbioru buforowego, który odnosi się do segmentu strony
- Zmiana

  Brak
- Operacje, które nie są kontrolowane

  WRKPAGSEG
  Praca z segmentami stron (Work with Page Segment)

  Drukowanie (Print)
  Odniesienie do segmentu strony podczas tworzenia zbioru buforowego

Operacje dotyczące grupy deskryptorów wydruków (*PDG):

- Odczyt

  Otwieranie (Open)
  Gdy grupa deskryptorów wydruków jest otwierana do odczytu za pomocą funkcji API PrintManager lub słowa CPI.
- Zmiana

  Otwieranie (Open)
  Gdy grupa deskryptorów wydruków jest otwierana do wprowadzania zmian za pomocą funkcji API PrintManager* lub słowa CPI.
- Operacje, które nie są kontrolowane

  CHGPDGPRF
  Zmiana profilu grupy deskryptorów wydruków (Change Print Descriptor Group Profile)

  WRKPDG
  Praca z grupą deskryptorów wydruków (Work with Print Descriptor Group)

Operacje dotyczące programów (*PGM):

- Odczyt

  Aktywowanie (Activation)
  Aktywowanie programu

  Wywołanie (Call)
  Wywoływanie programu, który nie był jeszcze aktywowany

  ADDPGM
  Dodanie programu do debugowania (Add program to debug)

QTEDBGS
Funkcja API Qte Register Debug View

QTEDBGS
Funkcja API Qte Retrieve Module Views

RUN Uruchomienie programu w środowisku S/36

RTVCLSRC
Odtworzenie źródła CL (Retrieve CL Source)

STRDBG
Uruchomienie debugera (Start Debug)

- Tworzenie

CRTPGM
Tworzenie programu (Create Program)

UPDPGM
Aktualizacja programu (Update Program)

- Zmiana

CHGCSPPGM
Zmiana programu CSP/AE (Change CSP/AE Program)

CHGPGM
Zmiana programu (Change Program)

CHGS36PGMA
Zmiana atrybutów programu System/36 (Change S/36 Program Attributes)

EDTS36PGMA
Edycja atrybutów programu System/36 (Edit S/36 Program Attributes)

WRKS36PGMA
Praca z atrybutami programu S/36 (Work with S/36 Program Attributes)

- Operacje, które nie są kontrolowane

ANZPGM
Analiza programów (Analyze Program)

DMPCLPGM
Zrzut programu CL (Dump CL Program)

DSPCSPOBJ
Wyświetlenie obiektu CSP (Display CSP Object)

DSPPGM
Wyświetlenie programu (Display Program)

PRTCMDUSG
Drukowanie użycia komend (Print Command Usage)

PRTCSPAPP
Drukowanie aplikacji CSP (Print CSP Application)

PRTSQLINF
Drukowanie informacji SQL (Print SQL Information)

QBNLPGMI
Funkcja API List ILE Program Information

QCLRPGMI
Funkcja API Retrieve Program Information

STRCSP
Uruchomienie narzędzi CSP (Start CSP Utilities)

TRCCSP
Śledzenie aplikacji CSP (Trace CSP Application)

WRKOBJCSP
Praca z obiektami dla CSP (Work with Objects for CSP)

WRKPGM
Praca z programami (Work with Program)

Operacje dotyczące panelu grupowego (*PNLGRP):

- Odczyt

  ADDSCHIDXE
  Dodanie pozycji indeksu wyszukiwania (Add Search Index Entry)

  QUIOPNDA
  Funkcja API Open Panel Group for Display

  QUIOPNPA
  Funkcja API Open Panel Group for Print

  QUHDSPH
  Funkcja API Display Help

- Zmiana

  Brak

- Operacje, które nie są kontrolowane

  WRKPNLGRP
  Praca z panelami grupowymi (Work with Panel Group)

Operacje dotyczące dostępności produktu (*PRDAVL):

- Zmiana

  WRKSPTPRD
  Praca z obsługiwanymi produktami (Work with Supported Products), podczas dodawania lub usuwania obsługi

- Operacje, które nie są kontrolowane

  Odczytywanie (Read)
  Żadne operacje odczytu nie są kontrolowane

Operacje dotyczące definicji produktu (*PRDDFN):

- Zmiana

  ADDPRDLICI
  Dodanie informacji licencyjnych produktu (Add Product License Information)

  WRKSPTPRD
  Praca z obsługiwanymi produktami (Work with Supported Products), podczas dodawania lub usuwania obsługi

- Operacje, które nie są kontrolowane

  Odczytywanie (Read)
  Żadne operacje odczytu nie są kontrolowane

Operacje dotyczące ładowania produktu (*PRDLOD):

- Zmiana

Zmiana (Change)
Stan ładowania produktu, lista bibliotek dla ładowania produktu, lista folderów dla ładowania produktu, język podstawowy

- Operacje, które nie są kontrolowane

Odczytywanie (Read)
Żadne operacje odczytu nie są kontrolowane

Operacje dotyczące formularza menedżera zapytań (*QMFORM):

- Odczyt

STRQMQRY
Uruchomienie zapytania menedżera zapytań (Start Query Management Query)

RTVQMFORM
Odtworzenie formularza menedżera zapytań (Retrieve Query Management Form)

Uruchomienie (Run)
Uruchomienie zapytania

Eksportowanie (Export)
Eksportowanie formularza menedżera zapytań

Drukowanie (Print)
Drukowanie formularza menedżera zapytań

Drukowanie raportu menedżera zapytań za pomocą formularza

Używanie (Use)
Dostęp do formularza za pomocą opcji 2, 5, 6 lub 9 lub funkcji F13 menu programu SQL/400 Query Manager.

- Zmiana

CRTQMFORM
Tworzenie formularza menedżera zapytań (Create Query Management Form)

Importowanie (Import)
Importowanie formularza menedżera zapytań

Składowanie (Save)
Składowanie formularza za pomocą opcji menu lub komendy

Kopiowanie (Copy)
Opcja 3 komendy Praca z formularzami menedżera zapytań (Work with Query Manager Forms)

- Operacje, które nie są kontrolowane

Praca z (Work with)
Gdy formularze *QMFORM są wyświetlane na ekranie Praca z

Aktywny (Active)
Każda operacja formularza, która jest wykonywana dla formularza 'aktywnego'.

Operacje dotyczące zapytania menedżera zapytań (*QMQRY):

- Odczyt

RTVQMQRY
Odtworzenie zapytania menedżera zapytań (Retrieve Query Manager Query)

Uruchomienie (Run)
Uruchomienie zapytania menedżera zapytań

STRQMQRY
Uruchomienie zapytania menedżera zapytań (Start Query Manager Query)

Eksportowanie (Export)
Eksportowanie zapytania menedżera zapytań

Drukowanie (Print)
Drukowanie zapytania menedżera zapytań

Używanie (Use)
Dostęp do zapytania za pomocą funkcji F13 lub opcji 2, 5, 6 lub 9 funkcji Praca z zapytaniami menedżera zapytań (Work with Query Manager queries)

- Zmiana

CRTQMQRY
Tworzenie zapytania menedżera zapytań (Create Query Management Query)

Przekształcanie (Convert)
Opcja 10 (Przekształć na SQL) funkcji Praca z zapytaniami menedżera zapytań (Work with Query Manager Queries)

Kopiowanie (Copy)
Opcja 3 komendy Praca z zapytaniami menedżera zapytań (Work with Query Manager Queries)

Składowanie (Save)
Składowanie zapytania za pomocą menu lub komendy

- Operacje, które nie są kontrolowane

Praca z (Work with)
Gdy zapytania *QMFORM są wyświetlane na ekranie Praca z

Aktywny (Active)
Każda operacja zapytania, która jest wykonywana dla zapytania 'aktywnego'.

Operacje dotyczące definicji zapytania (*QRYDFN):

- Odczyt

ANZQRY
Analiza zapytania (Analyze Query)

Zmiana (Change)
Zmiana zapytania za pomocą ekranu podpowiedzi komendy WRKQRY lub QRY.

Wyświetlenie (Display)
Wyświetlenie zapytania za pomocą ekranu podpowiedzi WRKQRY

Eksportowanie (Export)
Eksportowanie formularza za pomocą menedżera zapytań

Eksportowanie (Export)
Eksportowanie zapytania za pomocą menedżera zapytań

Drukowanie (Print)
Drukowanie definicji zapytania za pomocą ekranu podpowiedzi WRKQRY

Drukowanie formularza menedżera zapytań

Drukowanie zapytania menedżera zapytań

Drukowanie raportu menedżera zapytań

QRYRUN
Uruchomienie zapytania (Run Query)

RTVQMFORM
Odtworzenie formularza menedżera zapytań (Retrieve Query Management Form)

RTVQMQRY
Odtworzenie zapytania menedżera zapytań (Retrieve Query Management Query)

Uruchomienie (Run)
Uruchomienie zapytania za pomocą ekranu podpowiedzi WRKQRY

Uruchomienie (komenda Menedżer zapytań)

RUNQRY
Uruchomienie zapytania (Run Query)

STRQMQRY
Uruchomienie zapytania menedżera zapytań (Start Query Management Query)

Wprowadzenie (Submit)
Wprowadzenie zapytania (uruchomienie żądania) do zadania wsadowego za pomocą ekranu podpowiedzi WRKQRY lub Wyjście z zapytania (Exit This Query)

- Zmiana

  Zmiana (Change)
  Składowanie zmienionego zapytania za pomocą programu licencjonowanego Query/400

- Operacje, które nie są kontrolowane

  Kopiowanie (Copy)
  Kopiowanie zapytania za pomocą opcji 3 ekranu “Praca z zapytaniami” (Work with Queries)

  Tworzenie (Create)
  Tworzenie zapytania za pomocą opcji 1 ekranu “Praca z zapytaniami” (Work with Queries)

  Usunięcie (Delete)
  Usunięcie zapytania za pomocą opcji 4 ekranu “Praca z zapytaniami” (Work with Queries)

  Uruchomienie (Run)
  Uruchomienie zapytania za pomocą opcji 1 ekranu “Wyjście z zapytania” (Exit this Query), podczas tworzenia lub zmiany zapytania za pomocą programu licencjonowanego Query/400. Interaktywne uruchomienie zapytania za pomocą PF5 podczas tworzenia, wyświetlania lub zmieniania zapytania za pomocą programu licencjonowanego Query/400

  DLTQRY
  Usunięcie zapytania (Delete a query)

Operacje dotyczące tabeli konwersji kodów odniesienia (*RCT):

- Odczyt

  Brak

- Zmiana

  Brak

- Operacje, które nie są kontrolowane

  Brak

Operacje dotyczące listy odpowiedzi:

Uwaga: Operacje wykonywane na listach odpowiedzi są kontrolowane, jeśli wartość systemowa kontroli działania (QAUDLVL) lub parametr kontroli działania (AUDLVL) w profilu użytkownika zawiera wartość *SYSMGT.

- Kontrolowane Operacje

  ADDRPYLE
  Dodanie pozycji listy odpowiedzi (Add Reply List Entry)

CHGRPYLE
Zmiana pozycji listy odpowiedzi (Change Reply List Entry)

RMVRPYLE
Usuwanie pozycji listy odpowiedzi (Remove Reply List Entry)

WRKRPYLE
Praca z pozycjami listy odpowiedzi (Work with Reply List Entry)

- Operacje, które nie są kontrolowane

  Brak

Operacje dotyczące opisu podsystemu (*SBSD):

- Odczyt

  ENDSBS
  Zakończenie pracy podsystemu (End Subsystem)

  STRSBS
  Uruchomienie podsystemu (Start Subsystem)

- Zmiana

  ADDAJE
  Dodanie pozycji zadania autostartu (Add Autostart Job Entry)

  ADDCMNE
  Dodanie pozycji komunikacji (Add Communications Entry)

  ADDJOBQE
  Dodanie pozycji kolejki zadań (Add Job Queue Entry)

  ADDPJE
  Dodanie pozycji zadania prestartu (Add Prestart Job Entry)

  ADDRTGE
  Dodanie pozycji routingu (Add Routing Entry)

  ADDWSE
  Dodanie pozycji stacji roboczej (Add Workstation Entry)

  CHGAJE
  Zmiana pozycji zadania autostartu (Change Autostart Job Entry)

  CHGCMNE
  Zmiana pozycji komunikacji (Change Communications Entry)

  CHGJOBQE
  Zmiana pozycji kolejki zadań (Change Job Queue Entry)

  CHGPJE
  Zmiana pozycji zadania prestartu (Change Prestart Job Entry)

  CHGRTGE
  Zmiana pozycji routingu (Change Routing Entry)

  CHGSBSD
  Zmiana opisu podsystemu (Change Subsystem Description)

  CHGWSE
  Zmiana pozycji stacji roboczej (Change Workstation Entry)

  RMVAJE
  Usuwanie pozycji zadania autostartu (Remove Autostart Job Entry)

RMVCMNE
Usuwanie pozycji komunikacji (Remove Communications Entry)

RMVJOBQE
Usuwanie pozycji kolejki zadań (Remove Job Queue Entry)

RMVPJE
Usuwanie pozycji zadania prestartu (Remove Prestart Job Entry)

RMVRTGE
Usuwanie pozycji routingu (Remove Routing Entry)

RMVWSE
Usuwanie pozycji stacji roboczej (Remove Workstation Entry)

- Operacje, które nie są kontrolowane

DSPSBSD
Wyświetlenie opisu podsystemu (Display Subsystem Description)

QWCLASBS
Funkcja API List Active Subsystem

QWDLSJBQ
Funkcja API List Subsystem Job Queue

QWDRSBSD
Funkcja API Retrieve Subsystem Description

WRKSBSD
Praca z opisami podsystemów (Work with Subsystem Description)

WRKSBS
Praca z podsystemami (Work with Subsystem)

WRKSBSJOB
Praca z zadaniami podsystemu (Work with Subsystem Job)

Operacje dotyczące indeksu wyszukiwania informacji (*SCHIDX):

- Odczyt

STRSCHIDX
Uruchomienie wyszukiwania indeksowego (Start Index Search)

WRKSCHIDXE
Praca z pozycjami indeksu wyszukiwania (Work with Search Index Entry)

- Zmiana (kontrolowana gdy OBJAUD ma wartość *CHANGE lub *ALL)

ADDSCHIDXE
Dodanie pozycji indeksu wyszukiwania (Add Search Index Entry)

CHGSCHIDX
Zmiana indeksu wyszukiwania (Change Search Index)

RMVSCHIDXE
Usuwanie pozycji indeksu wyszukiwania (Remove Search Index Entry)

- Operacje, które nie są kontrolowane

WRKSCHIDX
Praca z indeksami wyszukiwania (Work with Search Index)

Operacje dotyczące gniazda lokalnego (*SOCKET):

- Odczyt

connect
Dowiązywanie stałego miejsca docelowego do gniazda i ustanawianie połączenia.

DSPLNK
Wyświetlenie dowiązań (Display Links)

givedescriptor
Funkcja API Give File Access

Qp0lGetPathFromFileID
Funkcja API Get Path Name of Object from File ID

Qp0lRenameKeep
Funkcja API Rename File or Directory, Keep New

Qp0lRenameUnlink
Funkcja API Rename File or Directory, Unlink New

sendmsg
Wysyłanie datagramu w trybie bezpołączeniowym. Może używać wielu buforów.

sendto Wysyłanie datagramu w trybie bezpołączeniowym.

WRKLNK
Praca z dowiązaniami (Work with Links)

- Zmiana

ADDLNK
Dodanie dowiązania (Add Link)

bind Ustanowienie adresu lokalnego dla gniazda.

CHGAUD
Zmiana kontroli (Change Auditing)

CHGAUT
Zmiana uprawnień (Change Authority)

CHGOWN
Zmiana właściciela (Change Owner)

CHGPGP
Zmiana grupy podstawowej (Change Primary Group)

CHKIN
Zwrot (Check In)

CHKOUT
Pobranie (Check Out)

chmod Funkcja API Change File Authorizations

chown Funkcja API Change Owner and Group

givedescriptor
Funkcja API Give File Access

link Funkcja API Create Link to File

Qp0lRenameKeep
Funkcja API Rename File or Directory, Keep New

Qp0lRenameUnlink
Funkcja API Rename File or Directory, Unlink New

RMVLNK
Usuwanie dowiązania (Remove Link)

RNM Zmiana nazwy (Rename)

RST Odtwarzanie (Restore)

unlink Funkcja API Remove Link to File

utime Funkcja API Set File Access and Modifcation Times

WRKAUT
Praca z uprawnieniami (Work with Authority)

WRKLNK
Praca z dowiązaniami (Work with Links)

- Operacje, które nie są kontrolowane

close Funkcja API Close File

Uwaga: Zamykanie nie jest kontrolowane, ale jeśli w programie obsługi wyjścia close scan_related nastąpiła awaria lub modyfikacja, wtedy rekord kontroli jest obcinany.

DSPAUT
Wyświetlenie uprawnień (Display Authority)

dup Funkcja API Duplicate Open File Descriptor

dup2 Funkcja API Duplicate Open File Descriptor to Another Descriptor

fcntl Funkcja API Perform File Control Command

fstat Funkcja API Get File Information by Descriptor

fsync Funkcja API Synchronize Changes to File

ioctl Funkcja API Perform I/O Control Request

lstat Funkcja API Get File or Link Information

pathconf
Funkcja API Get Configurable Path Name Variables

read Funkcja API Read from File

readv Funkcja API Read from File (Vector)

select Funkcja API Check I/O Status of Multiple File Descriptors

stat Funkcja API Get File Information

takedescriptor
Funkcja API Take File Access

write Funkcja API Write to File

writev Funkcja API Write to File (Vector)

Operacje dotyczące słownika sprawdzania pisowni (*SPADCT):

- Odczyt

Sprawdzanie (Verify)
Funkcja sprawdzania pisowni

Sprawdzanie (Aid)
Funkcja sprawdzania pisowni

Dzielenie słów (Hyphenation)
Funkcja dzielenia słów

Łączenie słów (Dehyphenation)
Funkcja łączenia słów

Synonimy (Synonyms)
Funkcja synonimów

Podstawa (Base)
Używanie słownika jako podstawy podczas tworzenia innego słownika

Sprawdzanie (Verify)
Używanie jako słownika sprawdzającego podczas tworzenia innego słownika

Odtwarzanie (Retrieve)
Odtwarzanie źródła listy słów zatrzymania (Retrieve Stop Word List Source)

Drukowanie (Print)
Drukowanie listy słów zatrzymania (Print Stop Word List Source)

- Zmiana

  CRTSPADCT
  Tworzenie słownika pisowni (Create Spelling Aid Dictionary) za pomocą opcji REPLACE(*YES)

- Operacje, które nie są kontrolowane

  Brak

Operacje dotyczące zbiorów buforowych:

Uwaga: Działania na zbiorach buforowych są kontrolowane, jeśli wartość systemowa kontroli działania (QAUDLVL) lub parametr kontroli działania (AUDLVL) w profilu użytkownika zawiera wartość *SPLFDTA.

- Kontrolowane Operacje

  Dostęp (Access)
  Każdy dostęp przez użytkownika, który nie jest właścicielem zbioru buforowego, w tym:
  - CPYSPLF,
  - DSPSPLF,
  - SNDNETSPLF,
  - SNDTCPSPLF,
  - STRRMTWTR,
  - funkcja API QSPOPNSP.

  Zmiana (Change)
  Zmienianie następujących atrybutów zbioru buforowego:
  - COPIES,
  - DEV,
  - FORMTYPE,
  - RESTART,
  - PAGERANGE.

  Tworzenie (Create)
  Tworzenie zbioru buforowego za pomocą operacji drukowania

  Tworzenie zbioru buforowego za pomocą funkcji API QSPCRTSP

  Usunięcie (Delete)
  Usunięcie zbioru buforowego za pomocą następujących poleceń:
  - drukowania zbioru buforowego przez drukarkę lub program piszący dyskietek,
  - usuwania zawartości kolejki wyjściowej (CLROUTQ),

- usuwania zbioru buforowego za pomocą komendy DLTSPLF lub opcji usunięcia z ekranu zbiorów buforowych,
- usunięcia zbiorów buforowych po zakończeniu zadania (ENDJOB SPLFILE(*YES)),
- usunięcia zbiorów buforowych po zakończeniu zadania drukowania (ENDPJ SPLFILE(*YES)),
- wysyłania zbioru buforowego do zdalnego systemu za pomocą zdalnego programu piszącego.

Wstrzymanie (Hold)
Wstrzymanie zbioru buforowego za pomocą następujących poleceń:
- komendy HLDSPLF,
- używania opcji wstrzymania ekranu zbiorów buforowych,
- drukowania zbioru buforowego, który ma wartość SAVE(*YES),
- wysyłania zbioru buforowego do zdalnego systemu za pomocą zdalnego programu piszącego, gdy podano wartość SAVE(*YES) dla zbioru buforowego,
- wstrzymania za pomocą programu piszącego po wystąpieniu błędu podczas przetwarzania zbioru buforowego.

Odczytywanie (Read)
Odczytywanie zbioru buforowego przez drukarkę lub program piszący dyskietek.

Zwalnianie (Release)
Zwalnianie zbioru buforowego

Operacje dotyczące pakietu SQL (*SQLPKG):

- Odczyt

  Uruchomienie (Run)
  Gdy obiekt *SQLPKG jest uruchomiony

- Zmiana

  Brak

- Operacje, które nie są kontrolowane

  PRTSQLINF
  Drukowanie informacji SQL (Print SQL Information)

Operacje dotyczące programu usługowego (*SRVPGM):

- Odczyt

  CRTPGM
  Pozycja kontroli dla każdego programu usługowego używanego podczas CRTPGM

  CRTSRVPGM
  Pozycja kontroli dla każdego programu usługowego używanego podczas CRTSRVPGM

  QTEDBGS
  Funkcja API Register Debug View

  QTEDBGS
  Funkcja API Retrieve Module Views

  RTVBNDSRC
  Odtworzenie źródła konsolidacji (Retrieve Binder Source)

  UPDPGM
  Pozycja kontroli dla każdego programu usługowego używanego podczas wykonywania komendy UPDPGM

UPDSRVPGM
Pozycja kontroli dla każdego programu usługowego używanego podczas wykonywania komendy UPDSRVPGM

- Tworzenie

CRTSRVPGM
Tworzenie programu usługowego (Create Service Program)

UPDSRVPGM
Aktualizacja programu usługowego (Update Service Program)

- Zmiana

CHGSRVPGM
Zmiana programu usługowego (Change Service Program)

- Operacje, które nie są kontrolowane

DSPSRVPGM
Wyświetlenie programu usługowego (Display Service Program)

PRTSQLINF
Drukowanie informacji SQL (Print SQL Information)

QBNLSPGM
Funkcja API List Service Program Information

QBNRSPGM
Funkcja API Retrieve Service Program Information

WRKSRVPGM
Praca z programami usługowymi (Work with Service Programs)

Operacje dotyczące opisu sesji (*SSND):

- Dla obiektów typu *SSND operacje odczytu lub zmiany nie są kontrolowane.

Operacje dotyczące przestrzeni pamięci serwera (*SVRSTG):

- Dla obiektu typu *SVRSTG operacje odczytu lub zmiany nie są kontrolowane.

Operacje dotyczące pliku strumieniowego (*STMF):

- Odczyt

CPY Kopiowanie (Copy)

DSPLNK
Wyświetlenie dowiązań (Display Links)

givedescriptor
Funkcja API Give File Access

MOV Przeniesienie (Move)

open, open64, QlgOpen, QlgOpen64, Qp0lOpen
Funkcje API Open File

SAV Składowanie (Save)

WRKLNK
Praca z dowiązaniami (Work with Links)

- Zmiana

ADDLNK
Dodanie dowiązania (Add Link)

Kontrola obiektów

CHGAUD
Zmiana kontroli (Change Auditing)

CHGAUT
Zmiana uprawnień (Change Authority)

CHGOWN
Zmiana właściciela (Change Owner)

CHGPGP
Zmiana grupy podstawowej (Change Primary Group)

CHKIN
Zwrot (Check In)

CHKOUT
Pobranie (Check Out)

chmod, QlgChmod
Funkcje API Change File Authorizations

chown, QlgChown
Funkcje API Change Owner and Group

CPY Kopiowanie (Copy)

creat, creat64, QlgCreat, QlgCreat64
Funkcje API Create New File lub Rewrite Existing File

fchmod
Funkcja API Change File Authorizations by Descriptor

fchown
Funkcja API Change Owner and Group of File by Descriptor

givedescriptor
Funkcja API Give File Access

link Funkcja API Create Link to File

MOV Przeniesienie (Move)

open, open64, QlgOpen, QlgOpen64, Qp0lOpen
Funkcje API When opened for write

Qp0lGetPathFromFileID, QlgGetPathFromFileID
Funkcje API Get Path Name of Object from File ID

Qp0lRenameKeep, QlgRenameKeep
Funkcje API Rename File or Directory, Keep New

Qp0lRenameUnlink, QlgRenameUnlink
Funkcje API Rename File or Directory, Unlink New

RMVLNK
Usuwanie dowiązania (Remove Link)

RNM Zmiana nazwy (Rename)

RST Odtwarzanie (Restore)

unlink, QlgUnlink
Funkcje API Remove Link to File

utime, QlgUtime
Funkcje API Set File Access and Modifcation Times

WRKAUT
Praca z uprawnieniami (Work with Authority)

WRKLNK
Praca z dowiązaniami (Work with Links)

- Operacje, które nie są kontrolowane

close Funkcja API Close File

DSPAUT
Wyświetlenie uprawnień (Display Authority)

dup Funkcja API Duplicate Open File Descriptor

dup2 Funkcja API Duplicate Open File Descriptor to Another Descriptor

faccessx
Określenie dostępności zbioru (Determine file accessibility)

fclear, fclear64
Usuwanie zawartości zbioru (Clear a file)

fcntl Funkcja API Perform File Control Command

fpathconf
Funkcja API Get Configurable Path Name Variables by Descriptor

fstat, fstat64
Funkcje API Get File Information by Descriptor

fsync Funkcja API Synchronize Changes to File

ftruncate, ftruncate64
Funkcje API Truncate File

ioctl Funkcja API Perform I/O Control Request

lseek, lseek64
Funkcje API Set File Read/Write Offset

lstat, lstat64
Funkcje API Get File or Link Information

pathconf, QlgPathconf
Funkcje API Get Configurable Path Name Variables

pread, pread64
Funkcje API Read from Descriptor with Offset

pwrite, pwrite64
Funkcje API Write to Descriptor with Offset

read Funkcja API Read from File

readv Funkcja API Read from File (Vector)

select Funkcja API Check I/O Status of Multiple File Descriptors

stat, stat64, QlgStat, QlgStat64
Funkcje API Get File Information

takedescriptor
Funkcja API Take File Access

write Funkcja API Write to File

writev Funkcja API Write to File (Vector)

Operacje dotyczące dowiązania symbolicznego (*SYMLNK):

- Odczyt

  CPY Kopiowanie (Copy)

  DSPLNK
  Wyświetlenie dowiązań (Display Links)

  MOV Przeniesienie (Move)

  readlink
  Funkcja API Read Value of Symbolic Link

  SAV Składowanie (Save)

  WRKLNK
  Praca z dowiązaniami (Work with Links)

- Zmiana

  CHGOWN
  Zmiana właściciela (Change Owner)

  CHGPGP
  Zmiana grupy podstawowej (Change Primary Group)

  CPY Kopiowanie (Copy)

  MOV Przeniesienie (Move)

  Qp0lRenameKeep, QlgRenameKeep
  Funkcje API Rename File or Directory, Keep New

  Qp0lRenameUnlink, QlgRenameUnlink
  Funkcje API Rename File or Directory, Unlink New

  RMVLNK
  Usuwanie dowiązania (Remove Link)

  RNM Zmiana nazwy (Rename)

  RST Odtwarzanie (Restore)

  symlink, QlgSymlink
  Funkcje API Make Symbolic Link

  unlink, QlgUnlink
  Funkcje API Remove Link to File

  WRKLNK
  Praca z dowiązaniami (Work with Links)

- Operacje, które nie są kontrolowane

  lstat, lstat64, QlgLstat, QlgLstat64
  Funkcje API Link Status

Operacje dotyczące opisu maszyny S/36 (*S36):

- Odczyt

  Brak

- Zmiana

  CHGS36
  Zmiana konfiguracji S/36 (Change S/36 configuration)

  CHGS36A
  Zmiana atrybutów konfiguracyjnych S/36 (Change S/36 configuration attributes)

SET Procedura SET

CRTDEVXXX
Gdy urządzenie dodawane jest do tabeli konfiguracji

DLTDEVD
Gdy urządzenie jest usuwane z tabeli konfiguracji

RNMOBJ
Zmiana nazwy opisu urządzenia (Rename device description)

- Operacje, które nie są kontrolowane

DSPS36
Wyświetlenie konfiguracji S/36 (Display S/36 configuration)

RTVS36A
Wczytanie atrybutów konfiguracyjnych S/36 (Retrieve S/36 Configuration Attributes)

STRS36
Uruchomienie S/36 (Start S/36)

ENDS36
Zakończenie S/36 (End S/36)

Operacje dotyczące tabeli (*TBL):

- Odczyt

QDCXLATE
Konwersja łańcucha znaków (Translate character string)

QTBXLATE
Konwersja łańcucha znaków (Translate character string)

QLGRTVSS
Wczytywanie tabeli kolejności sortowania

CRTLF
Konwersja tabeli podczas wykonywania komendy CRTLF

Odczytywanie (Read)
Tabeli kolejności sortowania należy używać podczas uruchamiania dowolnej komendy, która może określić kolejność sortowania

- Zmiana

Brak

- Operacje, które nie są kontrolowane

WRKTBL
Praca z tabelami (Work with tables)

Operacje dotyczące indeksu użytkownika (*USRIDX):

- Odczyt

QUSRTVUI
Funkcja API Retrieve user index entries

- Zmiana

QUSADDUI
Funkcja API Add User Index Entries

QUSRMVUI
Funkcja API Remove User Index Entries

- Operacje, które nie są kontrolowane

Dostęp (Access)
Bezpośredni dostęp do indeksu użytkownika za pomocą instrukcji MI (dozwolony tylko dla indeksu użytkownika w domenie użytkownika w bibliotece podanej w wartości systemowej QALWUSRDMN).

QUSRUIAT
Funkcja API Retrieve User Index Attributes

Operacje dotyczące profilu użytkownika (*USRPRF):

- Odczyt

  Brak

- Zmiana

  CHGPRF
  Zmiana profilu (Change Profile)

  CHGPWD
  Zmiana hasła (Change Password)

  CHGUSRPRF
  Zmiana profilu użytkownika (Change User Profile)

  CHKPWD
  Sprawdzenie hasła (Check Password)

  DLTUSRPRF
  Usunięcie profilu użytkownika (Delete User Profile)

  GRTUSRAUT
  Nadanie uprawnień użytkownika (Grant User Authority) (*dla_profilu_użytkownika*)

  QSYCHGPW
  Funkcja API Change Password

  RSTUSRPRF
  Odtworzenie profili użytkowników (Restore User Profiles)

- Operacje, które nie są kontrolowane

  DSPPGMADP
  Wyświetlenie programów adoptujących (Display Programs that Adopt)

  DSPUSRPRF
  Wyświetlenie profilu użytkownika (Display User Profile)

  GRTUSRAUT
  Nadanie uprawnień użytkownika (Grant User Authority) (*z_profilu_użytkownika*)

  PRTPRFINT
  Drukowanie wewnętrznych danych profilu (Print Profile Internals)

  PRTUSRPRF
  Drukowanie profilu użytkownika (Print User Profile)

  QSYCUSRS
  Funkcja API Check User Special Authorities

  QSYLOBJA
  Funkcja API List Authorized Objects

  QSYLOBJP
  Funkcja API List Objects That Adopt

  QSYRUSRI
  Funkcja API Retrieve User Information

RTVUSRPRF
Odtwarzanie profilu użytkownika (Retrieve User Profile)

WRKOBJOWN
Praca z posiadanymi obiektami (Work with Owned Objects)

WRKUSRPRF
Praca z profilami użytkowników (Work with User Profiles)

Operacje dotyczące kolejki użytkownika (*USRQ):

- Dla obiektu typu *USRQ, operacje odczytu lub zmiany nie są kontrolowane.
- Operacje, które nie są kontrolowane

  Dostęp (Access)
  Bezpośredni dostęp do kolejek użytkownika za pomocą instrukcji MI (dozwolony tylko dla kolejki użytkownika w domenie użytkownika w bibliotece podanej w wartości systemowej QALWUSRDMN).

Operacje dotyczące przestrzeni użytkownika (*USRSPC):

- Odczyt

  QUSRTVUS
  Funkcja API Retrieve User Space
- Zmiana

  QUSCHGUS
  Funkcja API Change User Space

  QUSCUSAT
  Funkcja API Change User Space Attributes
- Operacje, które nie są kontrolowane

  Dostęp (Access)
  Bezpośredni dostęp do przestrzeni użytkownika za pomocą instrukcji MI (dozwolony tylko dla przestrzeni użytkownika w domenie użytkownika w bibliotekach podanych w wartości systemowej QALWUSRDMN).

  QUSRUSAT
  Funkcja API Retrieve User Space Attributes

Operacje dla listy weryfikacji (*VLDL):

- Odczyt

  QSYFDVLE
  Funkcja API Find Validation List Entry
- Zmiana

  QSYADVLE
  Funkcja API Add Validation List Entry

  QSYCHVLE
  Funkcja API Change Validation List Entry

  QSYRMVLE
  Funkcja API Remove Validation List Entry
- Operacje, które nie są kontrolowane

  Dostęp (Access)
  Bezpośredni dostęp do przestrzeni użytkownika za pomocą instrukcji MI (dozwolony tylko dla przestrzeni użytkownika w domenie użytkownika w bibliotekach podanych w wartości systemowej QALWUSRDMN).

  QUSRUSAT
  Funkcja API Retrieve User Space Attributes

Kontrola obiektów

Operacje dotyczące obiektu dopasowania stacji roboczej (*WSCST):

- Odczyt

  Udostępnianie (Vary)
  Gdy dopasowywane urządzenie jest udostępniane

  RTVWSCST
  Odtworzenie źródła obiektu dopasowania stacji roboczej (Retrieve Workstation Customizing Object Source) (tylko wtedy, gdy dla typu urządzenia podano wartość *TRANSFORM)

  SNDTCPSPLF
  Wysłanie zbioru buforowego TCP/IP (Send TCP/IP Spooled File) (tylko wtedy, gdy podano wartość TRANSFORM(*YES))

  STRPRTWTR
  Uruchomienie programu piszącego drukarki (Start Printer Writer) (tylko dla zbiorów buforowych, które są drukowane na dopasowanej drukarce za pomocą funkcji hosta do konwersji wydruku)

  STRRMTWTR
  Uruchomienie zdalnego programu piszącego (Start Remote Writer) (tylko wtedy, gdy dla kolejki wyjściowej podano wartości CNNTYPE(*IP) i TRANSFORM(*YES))

  Drukowanie (Print)
  Gdy dane wyjściowe drukowane są bezpośrednio (nie są buforowane) na dopasowanej drukarce za pomocą funkcji hosta do konwersji wydruku

- Zmiana

  Brak

- Operacje, które nie są kontrolowane

  Brak

Dodatek F. Przeglądanie pozycji kroniki kontroli

Ten dodatek zawiera informacje dotyczące rozmieszczenia wszystkich typów pozycji z kodem kroniki T znajdujących się w kronice kontroli (QAUDJRN). Te pozycje kontrolowane są przez zdefiniowaną przez użytkownika kontrolę działania i obiektu. System zapisuje w kronice kontroli dodatkowe pozycje, dla zdarzeń takich jak IPL systemu lub składowanie dziennika. Rozmieszczenie tych typów pozycji można znaleźć w temacie Zarządzanie kroniką w Centrum informacyjnym.

Tabela 154 na stronie 508 zawiera rozmieszczenie pól, które są wspólne dla wszystkich typów pozycji, gdy dla komendy DSPJRN podano parametr OUTFILFMT(*TYPE2). Taki układ, o nazywie QJORDJE2, zdefiniowany jest w zbiorze QADSPJR2 w bibliotece QSYS.

Uwaga: Formaty wyjściowe TYPE2 i *TYPE4 nie są już aktualizowane, dlatego IBM zaleca zaprzestanie korzystania z formatów *TYPE2 i *TYPE4 i używanie tylko formatów *TYPE5.

Tabela 153 na stronie 507 zawiera rozmieszczenie pól, które są wspólne dla wszystkich typów pozycji, gdy dla komendy DSPJRN podano parametr OUTFILFMT(*TYPE4). Taki układ, o nazywie QJORDJE4, zdefiniowany jest w zbiorze QADSPJR4 w bibliotece QSYS. Format wyjściowy *TYPE4 obejmuje wszystkie informacje *TYPE2 oraz informacje dotyczące identyfikatorów kroniki, wyzwalaczy i ograniczeń referencyjnych.

Tabele od Tabela 156 na stronie 510 do Tabela 229 na stronie 614 prezentują układy dla modelowych zbiorów wyjściowych bazy danych udostępniane w celu definiowania danych wejściowych. Za pomocą komendy CRTDUPOBJ można tworzyć pusty zbiór wyjściowy z takim samym układem, jak jeden z modelowych zbiorów wyjściowych bazy danych. Za pomocą komendy DSPJRN można kopiować do zbioru wyjściowego wybrane pozycje kroniki kontroli w celu przeprowadzenia analizy. Sekcja “Analizowanie pozycji kroniki kontroli za pomocą programu Query lub programu użytkownika” na stronie 265 udostępnia przykłady używania modelowych zbiorów wyjściowych bazy danych. Można także zapoznać się z tematem Zarządzanie kroniką.

Tabela 152 zawiera rozmieszczenie pól, które są wspólne dla wszystkich typów pozycji, gdy dla komendy DSPJRN podano parametr OUTFILFMT(*TYPE5). Taki układ, o nazywie QJORDJE5, zdefiniowany jest w zbiorze QADSPJR5 w bibliotece QSYS. Format *TYPE5 obejmuje wszystkie informacje *TYPE4 oraz informacje dotyczące biblioteki programu, nazwę urządzenia ASP programu, numer urządzenia ASP programu, dziennik, bibliotekę dziennika, nazwę urządzenia ASP dziennika, numer urządzenia ASP dziennika, numer ramienia, identyfikator wątku, rodzinę adresów, port zdalny oraz adres zdalny.

Tabela 152. Standardowe pola nagłówkowe dla pozycji kroniki kontroli. Format rekordu QJORDJE5 (*TYPE5)

Pozycja (Offset)	Pole	Format	Opis
1	Długość pozycji	Zoned(5,0)	Całkowita długość pozycji kroniki łącznie z polem długości pozycji.
6	Numer kolejny	Char(20)	Stosowany dla każdej pozycji kroniki. Dla każdej nowej lub odtwarzanej kroniki początkowa wartość ustawiana jest na 1. Opcjonalnie resetowana da 1 gdy podłączany jest nowy dziennik.
26	Kod kroniki	Char(1)	Zawsze T.
27	Typ pozycji	Char(2)	Listę typów pozycji oraz opisy zawiera Tabela 155 na stronie 509.
29	Datownik pozycji	Char(26)	Data i godzina dodania pozycji w formacie SAA.
55	Nazwa zadania	Char(10)	Nazwa zadania, która spowodowała wygenerowanie pozycji.
65	Nazwa użytkownika	Char(10)	Nazwa profilu użytkownika związanego z zadaniem[1].
75	Numer zadania	Zoned(6,0)	Numer zadania.

Tabela 152. Standardowe pola nagłówkowe dla pozycji kroniki kontroli (kontynuacja). Format rekordu QJORDJE5 (*TYPE5)

Pozycja (Offset)	Pole	Format	Opis
81	Nazwa programu	Char(10)	Nazwa programu, który utworzył pozycję kroniki. Może to być także nazwa programu usługowego lub częściowa nazwa pliku klasy użytego w kompilowanym programie języka Java. Jeśli aplikacja lub program CL nie powoduje powstania pozycji, pole zawiera nazwę programu systemowego, takiego jak QCMD. Pola ma wartość *NONE jeśli spełniony jest jeden z następujących warunków: • nazwa programu nie odnosi się do tego typu pozycji, • nazwa programu nie jest dostępna.
91	Biblioteka programu	Char(10)	Nazwa biblioteki zawierającej program, który dodał pozycję kroniki.
101	Urządzenie ASP programu	Char(10)	Nazwa urządzenia puli ASP zawierającej program, który dodał pozycję kroniki.
111	Numer ASP programu	Zoned(5,0)	Numer puli ASP zawierającej program, który dodał pozycję kroniki.
116	Nazwa obiektu	Char(10)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
126	Biblioteka obiektów	Char(10)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
136	Nazwa podzbioru	Char(10)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
146	Count/RRN	Char(20)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
166	Flaga	Char(1)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
167	Identyfikator cyklu zatwierdzania	Char(20)	Używana dla obiektów kronikowanych. Nieużywany dla pozycji kroniki kontroli.
187	Profil użytkownika	Char(10)	Nazwa bieżącego profilu użytkownika[1].
197	Nazwa systemu	Char(8)	Nazwa systemu.
205	Identyfikator kroniki	Char(10)	Używany do kronikowania zbioru. Nieużywany dla pozycji kroniki kontroli.
215	Ograniczenie referencyjne	Char(1)	Używane do kronikowania zbioru. Nieużywane dla pozycji kroniki kontroli.
216	Wyzwalacz	Char(1)	Używany do kronikowania zbioru. Nieużywany dla pozycji kroniki kontroli.
217	Dane niepełne	Char(1)	Używane do kronikowania zbioru. Nieużywane dla pozycji kroniki kontroli.
218	Ignorowanie przez APY/ RMVJRNCHG	Char(1)	Używane do kronikowania zbioru. Nieużywane dla pozycji kroniki kontroli.
219	Zminimalizowane ESD	Char(1)	Używane do kronikowania zbioru. Nieużywane dla pozycji kroniki kontroli.
220	Indykator obiektu	Char(1)	Używany do kronikowania zbioru. Nieużywany dla pozycji kroniki kontroli.
221	Numer kolejny w systemie	Char(20)	Liczba przypisywana przez system każdej pozycji kroniki.
241	Dziennik	Char(10)	Nazwa dziennika przechowującego pozycję kroniki.
251	Biblioteka dziennika	Char(10)	Nazwa biblioteki dziennika przechowującego pozycję kroniki.
261	Urządzenie ASP dziennika	Char(10)	Nazwa urządzenia puli ASP, w której przechowywany jest dziennik.
271	Numer ASP dziennika	Zoned(5,0)	Numer puli ASP, w której przechowywany jest dziennik zawierający pozycję kroniki.
276	Numer ramienia	Zoned(5,0)	Numer ramienia dysku, które ma dostęp do pozycji kroniki.
281	Identyfikator wątku	Hex(8)	Identyfikuje wątek w procesie, który dodaje pozycję kroniki.
289	Wersja szesnastkowa identyfikatora wątku	Char(16)	Możliwa do wyświetlenia wersja szesnastkowa identyfikatora wątku.
305	Rodzina adresów	Char(1)	Format adresu zdalnego dla danej pozycji kroniki.
306	Port zdalny	Zoned(5,0)	Numer portu adresu zdalnego związanego z pozycją kroniki.
311	Adres zdalny	Char(46)	Adres zdalny związany z pozycją kroniki.
357	Logiczna jednostka pracy	Char(39)	Używana do kronikowania zbioru. Nieużywana dla pozycji kroniki kontroli.
396	ID transakcji	Char(140)	Używany do kronikowania zbioru. Nieużywany dla pozycji kroniki kontroli.

Tabela 152. Standardowe pola nagłówkowe dla pozycji kroniki kontroli (kontynuacja). Format rekordu QJORDJE5 (*TYPE5)

Pozycja (Offset)	Pole	Format	Opis
536	Zastrzeżone	Char(20)	Używane do kronikowania zbioru. Nieużywane dla pozycji kroniki kontroli.
556	Indykatory wartości pustej (Null)	Char(50)	Używane do kronikowania zbioru. Nieużywane dla pozycji kroniki kontroli.
606	Długość danych pozycji	Binary(5)	Długość danych pozycji.

Uwaga: Trzy pola począwszy od pozycji 55 oznaczają nazwę zadania systemowego. W większości przypadków pole Nazwa użytkownika na pozycji 65 oraz Nazwa profilu użytkownika na pozycji 187 mają taką samą wartość. Dla zadań prestartu, pole Nazwa profilu użytkownika zawiera nazwę użytkownika uruchamiającego transakcję. Dla niektórych zadań, jako nazwę użytkownika, oba te pola mają wartość QSYS. Pole Nazwa profilu użytkownika w danych pozycji zawiera aktualnego użytkownika, który spowodował powstanie pozycji. Jeśli do zamiany profili użytkowników używana jest funkcja API, pole Nazwa profilu użytkownika zawiera nazwę nowego (zamienionego) profilu użytkownika.

Tabela 153. Standardowe pola nagłówkowe dla pozycji kroniki kontroli. Format rekordu QJORDJE4 (*TYPE4)

Pozycja (Offset)	Pole	Format	Opis
1	Długość pozycji	Zoned(5,0)	Całkowita długość pozycji kroniki łącznie z polem długości pozycji.
6	Numer kolejny	Zoned(10,0)	Stosowany dla każdej pozycji kroniki. Dla każdej nowej lub odtwarzanej kroniki początkowa wartość ustawiana jest na 1. Opcjonalnie resetowana da 1 gdy podłączany jest nowy dziennik.
16	Kod kroniki	Char(1)	Zawsze T.
17	Typ pozycji	Char(2)	Listę typów pozycji oraz opisy zawiera Tabela 155 na stronie 509.
19	Datownik pozycji	Char(26)	Data i godzina dodania pozycji w formacie SAA.
45	Nazwa zadania	Char(10)	Nazwa zadania, która spowodowała wygenerowanie pozycji.
55	Nazwa użytkownika	Char(10)	Nazwa profilu użytkownika związanego z zadaniem[1].
65	Numer zadania	Zoned(6,0)	Numer zadania.
71	Nazwa programu	Char(10)	Nazwa programu, który utworzył pozycję kroniki. Może to być także nazwa programu usługowego lub częściowa nazwa pliku klasy użytego w kompilowanym programie języka Java. Jeśli aplikacja lub program CL nie powoduje powstania pozycji, pole zawiera nazwę programu systemowego, takiego jak QCMD. Pola ma wartość *NONE jeśli spełniony jest jeden z następujących warunków: • nazwa programu nie odnosi się do tego typu pozycji, • nazwa programu nie jest dostępna.
81	Nazwa obiektu	Char(10)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
91	Nazwa biblioteki	Char(10)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
101	Nazwa podzbioru	Char(10)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
111	Count/RRN	Zoned(10)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
121	Flaga	Char(1)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
122	Identyfikator cyklu zatwierdzania	Zoned(10)	Używana dla obiektów kronikowanych. Nieużywany dla pozycji kroniki kontroli.
132	Profil użytkownika	Char(10)	Nazwa bieżącego profilu użytkownika[1].
142	Nazwa systemu	Char(8)	Nazwa systemu.
150	Zastrzeżone	Char(10)	Używane do kronikowania zbioru. Nieużywane dla pozycji kroniki kontroli.
160	Ograniczenie referencyjne	Char(1)	Używane do kronikowania zbioru. Nieużywane dla pozycji kroniki kontroli.
161	Wyzwalacz	Char(1)	Używany do kronikowania zbioru. Nieużywany dla pozycji kroniki kontroli.
162	(Obszar zastrzeżony)	Char(8)	
170	Indykatory wartości pustej (Null)	Char(50)	Używane do kronikowania zbioru. Nieużywane dla pozycji kroniki kontroli.

Tabela 153. Standardowe pola nagłówkowe dla pozycji kroniki kontroli (kontynuacja). Format rekordu QJORDJE4 (*TYPE4)

Pozycja (Offset)	Pole	Format	Opis
220	Długość danych pozycji	Binary (4)	Długość danych pozycji.
	Uwaga: Trzy pola począwszy od pozycji 45 oznaczają nazwę zadania systemowego. W większości przypadków pole Nazwa użytkownika na pozycji 55 oraz Nazwa profilu użytkownika na pozycji 132 mają taką samą wartość. Dla zadań prestartu, pole Nazwa profilu użytkownika zawiera nazwę użytkownika uruchamiającego transakcję. Dla niektórych zadań, jako nazwę użytkownika, oba te pola mają wartość QSYS. Pole Nazwa profilu użytkownika w danych pozycji zawiera aktualnego użytkownika, który spowodował powstanie pozycji. Jeśli do zamiany profili użytkowników używana jest funkcja API, pole Nazwa profilu użytkownika zawiera nazwę nowego (zamienionego) profilu użytkownika.		

Tabela 154. Standardowe pola nagłówkowe dla pozycji kroniki kontroli. Format rekordu QJORDJE2 (*TYPE2)

Pozycja (Offset)	Pole	Format	Opis
1	Długość pozycji	Zoned(5,0)	Całkowita długość pozycji kroniki łącznie z polem długości pozycji.
6	Numer kolejny	Zoned(10,0)	Stosowany dla każdej pozycji kroniki. Dla każdej nowej lub odtwarzanej kroniki początkowa wartość ustawiana jest na 1. Opcjonalnie resetowana da 1 gdy podłączany jest nowy dziennik.
16	Kod kroniki	Char(1)	Zawsze T.
17	Typ pozycji	Char(2)	Listę typów pozycji oraz opisy zawiera Tabela 155 na stronie 509.
19	Datownik	Char(6)	Data systemowa wprowadzenia pozycji.
25	Godzina pozycji	Zoned(6,0)	Godzina systemowa wprowadzenia pozycji.
31	Nazwa zadania	Char(10)	Nazwa zadania, która spowodowała wygenerowanie pozycji.
41	Nazwa użytkownika	Char(10)	Nazwa profilu użytkownika związanego z zadaniem[1].
51	Numer zadania	Zoned(6,0)	Numer zadania.
57	Nazwa programu	Char(10)	Nazwa programu, który utworzył pozycję kroniki. Może to być także nazwa programu usługowego lub częściowa nazwa pliku klasy użytego w kompilowanym programie języka Java. Jeśli aplikacja lub program CL nie powoduje powstania pozycji, pole zawiera nazwę programu systemowego, takiego jak QCMD. Pola ma wartość *NONE jeśli spełniony jest jeden z następujących warunków: • nazwa programu nie odnosi się do tego typu pozycji, • nazwa programu nie jest dostępna.
67	Nazwa obiektu	Char(10)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
77	Nazwa biblioteki	Char(10)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
87	Nazwa podzbioru	Char(10)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
97	Count/RRN	Zoned(10)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
107	Flaga	Char(1)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
108	Identyfikator cyklu zatwierdzania	Zoned(10)	Używana dla obiektów kronikowanych. Nieużywany dla pozycji kroniki kontroli.
118	Profil użytkownika	Char(10)	Nazwa bieżącego profilu użytkownika[1].
128	Nazwa systemu	Char(8)	Nazwa systemu.
136	(Obszar zastrzeżony)	Char(20)	

1 Trzy pola począwszy od pozycji 31 oznaczają nazwę zadania systemowego. W większości przypadków pole *Nazwa użytkownika* na pozycji 41 oraz *Nazwa profilu użytkownika* na pozycji 118 mają taką samą wartość. Dla zadań prestartu, pole *Nazwa profilu użytkownika* zawiera nazwę użytkownika uruchamiającego transakcję. Dla niektórych zadań, jako nazwę użytkownika, oba te pola mają wartość QSYS. Pole *Nazwa profilu użytkownika* w danych pozycji zawiera aktualnego użytkownika, który spowodował powstanie pozycji. Jeśli do zamiany profili użytkowników używana jest funkcja API, pole *Nazwa profilu użytkownika* zawiera nazwę nowego (zamienionego) profilu użytkownika.

Tabela 155. Typy pozycji kroniki kontroli (QAUDJRN).

Typ pozycji	Opis
AD	Kontrolowanie zmian
AF	Błąd uprawnień
AP	Uzyskiwanie uprawnienia adoptowanego
AU	Zmiany atrybutu
CA	Zmiany uprawnień
CD	Kontrola łańcucha komendy
CO	Tworzenie obiektu
CP	Zmiana, utworzenie lub odtworzenie profilu użytkownika
CQ	Zmiana obiektu *CRQD
CU	Operacje klastra
CV	Sprawdzanie połączenia
CY	Konfigurowanie szyfrowania
DI	Serwer katalogów
DO	Usunięcie obiektu
DS	Reset hasła ochrony narzędzi DST
EV	Zmienne środowiskowe systemu
GR	Rekord ogólny
GS	Opis gniazda został przekazany do innego zadania
IP	Komunikacja międzyprocesorowa
IR	Operacje reguł IP
IS	Zarządzanie ochroną internetową
JD	Zmiany w parametrach użytkownika opisu zadania
JS	Operacje wpływające na zadania
KF	Zbiór pliku kluczy
LD	Dowiązywanie, usuwanie dowiązania lub wyszukiwanie pozycji katalogu
ML	Działania poczty usług biurowych
NA	Zmiana atrybutu sieciowego
ND	Naruszenie filtru przeszukiwania katalogów sieci APPN
NE	Naruszenie filtru APPN punktu końcowego
OM	Zmiana nazwy lub przeniesienie obiektu
OR	Odtworzenie obiektu
OW	Zmiana prawa własności do obiektu
O1	(Dostęp optyczny) Pojedynczy zbiór lub katalog
O2	(Dostęp optyczny) Podwójny zbiór lub katalog
O3	(Dostęp optyczny) Wolumin
PA	Zmieniono program w celu adoptowania uprawnień
PG	Zmiana grupy podstawowej obiektu
PO	Wydrukowano dane wyjściowe
PS	Zmiana profilu
PW	Niepoprawne hasło
RA	Zmiana uprawnień podczas odtwarzania
RJ	Odtwarzanie opisu zadania z podaniem profilu użytkownika
RO	Zmiana właściciela obiektu podczas odtwarzania
RP	Odtwarzanie programu adoptującego uprawnienia
RQ	Odtwarzanie obiektu *CRQD
RU	Odtwarzanie uprawnień profilu użytkownika
RZ	Zmiana grupy podstawowej podczas odtwarzania
SD	Zmiany w katalogu dystrybucyjnym systemu
SE	Zmieniono pozycje routingu podsystemu
SF	Działania na zbiorach buforowych
SG	Sygnały asynchroniczne

Tabela 155. Typy pozycji kroniki kontroli (QAUDJRN). (kontynuacja)

Typ pozycji	Opis
SK	Bezpieczne połączenia przez gniazdo
SM	Zmiany zarządzania systemami
SO	Działania informacji użytkownika ochrony serwera
ST	Użycie narzędzi serwisowych
SV	Zmieniono wartość systemową
VA	Zmiana listy kontroli dostępu
VC	Uruchomienie lub zakończenie połączenia
VF	Zamykanie zbiorów serwera
VL	Przekroczono limit konta
VN	Logowanie i wylogowywanie z sieci
VO	Działania listy sprawdzania
VP	Błąd hasła sieciowego
VR	Dostęp do zasobu sieciowego
VS	Uruchomienie lub zakończenie sesji serwera
VU	Zmiana profilu sieciowego
VV	Zmiana statusu usługi
X0	Uwierzytelnianie w sieci
YC	Dostęp do obiektu DLO (zmiana)
YR	Dostęp do obiektu DLO (odczyt)
ZC	Dostęp do obiektu (zmiana)
ZM	Metoda dostępu SOM
ZR	Dostęp do obiektu (odczyt)

Tabela 156. Pozycje kroniki AD (kontrolowanie zmiany). Zbiór opisów pól QASYADJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	**D** Komenda CHGDLOAUD **O** Komenda CHGAUD **S** Atrybut skanowania został zmieniony za pomocą komendy CHGATR lub funkcji API Qp0lSetAttr albo podczas tworzenia obiektu. **U** Komenda CHGUSRAUD
157	225	611	Nazwa obiektu	Char(10)	Nazwa obiektu, dla którego została zmieniona kontrola.
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki dla obiektu.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Wartość kontroli obiektu	Char(10)	Jeśli typem pozycji jest D, O lub U, pole zawiera podaną wartość kontroli. Jeśli typem pozycji jest S, pole zawiera wartość atrybutu skanowania.
195	263	649	CHGUSRAUD *CMD	Char(1)	Y = komendy kontroli dla danego użytkownika.
196	264	650	CHGUSRAUD *CREATE	Char(1)	Y = zapis rekordu kontroli, gdy dany użytkownik tworzy obiekt.
197	265	651	CHGUSRAUD *DELETE	Char(1)	Y = zapis rekordu kontroli, gdy dany użytkownik usuwa obiekt.

Tabela 156. Pozycje kroniki AD (kontrolowanie zmiany) (kontynuacja). Zbiór opisów pól QASYADJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
198	266	652	CHGUSRAUD *JOBDTA	Char(1)	Y = zapis rekordu kontroli, gdy dany użytkownik zmienia zadanie.
199	267	653	CHGUSRAUD *OBJMGT	Char(1)	Y = zapis rekordu kontroli, gdy dany użytkownik przenosi lub zmienia nazwę obiektu.
200	268	654	CHGUSRAUD *OFCSRV	Char(1)	Y = zapis rekordu kontroli, gdy dany użytkownik wykonuje funkcje biurowe.
201	269	655	CHGUSRAUD *PGMADP	Char(1)	Y = zapis rekordu kontroli, gdy dany użytkownik uzyskuje uprawnienia za pomocą uprawnień adoptowanych.
202	270	656	CHGUSRAUD *SAVRST	Char(1)	Y = zapis rekordu kontroli, gdy dany użytkownik składuje lub odtwarza obiekty.
203	271	657	CHGUSRAUD *SECURITY	Char(1)	Y = zapis rekordu kontroli, gdy dany użytkownik wykonuje działania związane z ochroną.
204	272	658	CHGUSRAUD *SERVICE	Char(1)	Y = zapis rekordu kontroli, gdy dany użytkownik wykonuje funkcje usług.
205	273	659	CHGUSRAUD *SPLFDTA	Char(1)	Y = zapis rekordu kontroli, gdy dany użytkownik manipuluje zbiorami buforowymi.
206	274	660	CHGUSRAUD *SYSMGT	Char(1)	Y = zapis rekordu kontroli, gdy dany użytkownik wprowadza zmiany zarządzania systemami.
207	275	661	CHGUSRAUD *OPTICAL	Char(1)	Y = zapis rekordu kontroli, gdy dany użytkownik uzyskuje dostęp do urządzeń optycznych.
208	276	662	(Obszar zastrzeżony)	Char(19)	
227	295	681	Nazwa DLO	Char(12)	Nazwa obiektu DLO, dla którego została zmieniona kontrola.
239	307	693	(Obszar zastrzeżony)	Char(8)	
247	315	701	Ścieżka folderu	Char(63)	Ścieżka folderu.
310			(Obszar zastrzeżony)	Char(20)	
	378	764	(Obszar zastrzeżony)	Char(18)	
	396	782	Długość nazwy obiektu [1]	Binary(4)	Długość nazwy obiektu.
330	398	784	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.
334	402	788	Identyfikator kraju lub regionu nazwy obiektu[1]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
336	404	790	Identyfikator języka nazwy obiektu[1]	Char(3)	Identyfikator języka dla nazwy obiektu.
339	407	793	(Obszar zastrzeżony)	Char(3)	
342	410	796	Identyfikator pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
358	426	812	Identyfikator pliku obiektu[1,2]	Char(16)	Identyfikator pliku obiektu.
374	442	828	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	954	1340	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.

Tabela 156. Pozycje kroniki AD (kontrolowanie zmiany) (kontynuacja). Zbiór opisów pól QASYADJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	970	1356	Nazwa puli ASP [5]	Char(10)	Nazwa urządzenia puli ASP.
	980	1366	Numer puli ASP [5]	Char(5)	Numer urządzenia puli ASP.
	985	1371	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	989	1375	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	991	1377	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	994	1380	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.
	996	1382	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	997	1383	Identyfikator pliku o dostępie pośrednim[3]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	1013	1399	Bezwzględna nazwa ścieżki[4]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

1 Te pola używane są tylko dla obiektów w systemach plików QOpenSys, "root" oraz użytkownika.

2 Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

3 Gdy indykator bezwzględnej nazwy ścieżki (pozycja 996) ma wartość ″N″, to pole będzie zawierało identyfikator pola o dostępie pośrednim dla nazwy ścieżki. Gdy wskaźnikiem bezwzględnej nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

4 Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

5 Jeśli obiekt znajduje się w bibliotece, jest to informacja puli ASP biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja obiektu.

Tabela 157. Pozycje kroniki AF (Uprawnienie). Zbiór opisów pól QASYAFJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 na stronie 507 na stronie 507 na stronie 507 i Tabela 154 na stronie 508.

Tabela 157. Pozycje kroniki AF (Uprawnienie) (kontynuacja). Zbiór opisów pól QASYAFJE/J4/J5

Pozycja (Offset)						
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**	
156	224	610	Rodzaj naruszenia[1]	Char(1)	**A**	Brak uprawnienia do obiektu
					B	Instrukcja ograniczona
					C	Błąd sprawdzenia (patrz J5 pozycja 639)
					D	Użycie nieobsługiwanego interfejsu, błąd domeny obiektu
					E	Błąd ochrony pamięci sprzętowej, naruszenie przestrzeni stałej programu
					F	Błąd autoryzacji ICAPI
					G	Błąd uwierzytelniania ICAPI
					H	Skanowanie programu obsługi wyjścia (patrz J5 pozycja 639)
					I[7]	Systemowe dziedziczenie Java nie jest dozwolone
					J	Błąd profilu wprowadzenia zadania
					N	Znacznik profilu nie jest znacznikiem regenerowalnym
					O	Błąd uprawnień do obiektu optycznego
					P	Błąd przełączania profilu
					R	Błąd ochrony sprzętu
					S	Domyślna próba wpisania się
					T	Brak uprawnień do portu TCP/IP
					U	Żądanie uprawnień specjalnych użytkownika nie jest poprawne
					V	Znacznik profilu nie jest poprawny do generowania nowego znacznika profilu
					W	znacznik profilu nie jest poprawny dla funkcji przełączania
					X	Naruszenie systemu — patrz J5 pozycja 723 dla kodów naruszenia
					Y	Brak uprawnień do bieżącego pola JUID podczas wykonywania operacji usuwania zawartości pola JUID.
					Z	Brak uprawnień do bieżącego pola JUID podczas wykonywania operacji ustawiania pola JUID.
157	225	611	Nazwa obiektu[1, 5]	Char(10)	Nazwa obiektu.	
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki, której znajduje się obiekt lub numer poprawki do Licencjonowanego Kodu Wewnętrznego, której zastosowanie nie powiodło się.[11]	
177	245	631	Typ obiektu	Char(8)	Typ obiektu.	

Tabela 157. Pozycje kroniki AF (Uprawnienie) (kontynuacja). Zbiór opisów pól QASYAFJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
185	253	639	Działanie błędu sprawdzania	Char(1)	Działanie podjęte po wykryciu błędu sprawdzania, ustawiane tylko jeśli typ naruszenia (J5 pozycja 610) to C lub H. **A** Konwersja obiektu nie doszła do skutku lub nie powiodła się. Ustawienie wartości systemowej QALWOBJRST umożliwia odtwarzanie obiektu. Użytkownik przeprowadzający odtwarzanie nie miał uprawnień specjalnych *ALLOBJ a poziom ochrony systemu jest ustawiony na 10, 20 lub 30. Dlatego wszystkie uprawnienia do obiektu zostały zachowane. **B** Konwersja obiektu nie doszła do skutku lub nie powiodła się. Ustawienie wartości systemowej QALWOBJRST umożliwia odtwarzanie obiektu. Użytkownik przeprowadzający odtwarzanie nie miał uprawnień specjalnych *ALLOBJ a poziom ochrony systemu jest ustawiony na 40 lub wyższy. Dlatego wszystkie uprawnienia do obiektu zostały odebrane. **C** Konwersja obiektu zakończona pomyślnie. Konwertowana kopia została odtworzona. **D** Konwersja obiektu nie doszła do skutku lub nie powiodła się. Ustawienie wartości systemowej QALWOBJRST umożliwia odtwarzanie obiektu. Użytkownik przeprowadzający odtwarzanie miał uprawnienia specjalne *ALLOBJ. Dlatego wszystkie uprawnienia do obiektu zostały zachowane. **E** Wykryto błąd podczas instalowania systemu. **F** Obiekt nie został odtworzony ponieważ podpis nie ma formatu OS/400. **G** Podczas sprawdzania systemu znaleziono niepodpisany obiekt systemowy lub dziedziczący. **H** Podczas sprawdzania systemu znaleziono niepodpisany obiekt stanu użytkownika. **I** Podczas sprawdzania systemu wykryto niezgodność między obiektem a jego podpisem. **J** Podczas sprawdzania systemu nie znaleziono certyfikatu IBM. **K** Podczas sprawdzania systemu znaleziono niepoprawny format podpisu. **M** Programu obsługi wyjścia skanowania zmodyfikował skanowany obiekt **X** Program obsługi wyjścia skanowania żądał obiektu oznaczonego jako mającego błąd podczas skanowania
186	254	640	Nazwa zadania	Char(10)	Nazwa zadania.
196	264	650	Nazwa użytkownika	Char(10)	Nazwa użytkownika zadania.
206	274	660	Numer zadania	Zoned(6,0)	Numer zadania.
212	280	666	Nazwa programu	Char(10)	Nazwa programu.
222	290	676	Biblioteka programu	Char(10)	Nazwa biblioteki, w której znajduje się program.

Tabela 157. Pozycje kroniki AF (Uprawnienie) (kontynuacja). Zbiór opisów pól QASYAFJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
232	300	686	Profil użytkownika [2]	Char(10)	Nazwa użytkownika, który spowodował błąd uprawnień.
242	310	696	Nazwa stacji roboczej	Char(10)	Nazwa lub typ stacji roboczej.
252	320	706	Numer instrukcji programu	Zoned(7,0)	Numer instrukcji programu.
259	327	713	Nazwa pola	Char(10)	Nazwa pola.
269	337	723	Kod naruszenia operacji	Char(3)	Rodzaj naruszenia operacji, ustawiany tylko wtedy, gdy rodzaj naruszenia (J5 pozycja 610) to X. **HCA** Profil użytkownika narzędzi serwisowych nie ma uprawnień do wykonywania operacji konfigurowania sprzętu (QYHCHCOP). **LIC** Wskazuje, że poprawka do Licencjonowanego Kodu Wewnętrznego nie została zastosowana z powodu naruszenia podpisu. **SFA** Brak autoryzacji do aktywowania atrybutu środowiska dla dostępu do pliku systemowego. **CMD** Próbowano użyć komendy, która została zablokowana przez administratora systemu.
272	340	726	Użytkownik biurowy	Char(10)	Nazwa użytkownika biurowego.
282	350	736	Nazwa DLO	Char(12)	Nazwa obiektu biblioteki dokumentów.
294	362	748	(Obszar zastrzeżony)	Char(8)	
302	370	756	Ścieżka folderu	Char(63)	Ścieżka do folderu.
365	433	819	Praca w imieniu użytkownika	Char(10)	Użytkownik pracujący w imieniu innego użytkownika.
375			(Obszar zastrzeżony)	Char(20)	
	443	829	(Obszar zastrzeżony)	Char(18)	
	461	847	Długość nazwy obiektu [3]	Binary(4)	Długość nazwy obiektu.
395	463	849	Identyfikator CCSID nazwy obiektu[3]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.
399	467	853	Identyfikator kraju lub regionu nazwy obiektu[3]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
401	469	855	Identyfikator języka nazwy obiektu[3]	Char(3)	Identyfikator języka dla nazwy obiektu.
404	472	858	(Obszar zastrzeżony)	Char(3)	
407	475	861	Identyfikator pliku nadrzędnego[3,4]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
423	491	877	Identyfikator pliku obiektu[3,4]	Char(16)	Identyfikator pliku obiektu.
439	507	893	Nazwa obiektu[3,6]	Char(512)	Nazwa obiektu.

Tabela 157. Pozycje kroniki AF (Uprawnienie) (kontynuacja). Zbiór opisów pól QASYAFJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1019	1405	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	1035	1421	Nazwa puli ASP [10]	Char(10)	Nazwa urządzenia puli ASP.
	1045	1431	Numer puli ASP [10]	Char(5)	Numer urządzenia puli ASP.
	1050	1436	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	1054	1440	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	1056	1442	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	1059	1445	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.
	1061	1447	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	1062	1448	Identyfikator pliku o dostępie pośrednim [8]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	1078	1464	Bezwzględna nazwa ścieżki [9]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.
		6466	Nazwa puli ASP biblioteki programu	Char(10)	Nazwa puli ASP dla biblioteki programu
		6476	Numer puli ASP biblioteki programu	Char(5)	Numer puli ASP dla biblioteki programu

Tabela 157. Pozycje kroniki AF (Uprawnienie) (kontynuacja). Zbiór opisów pól QASYAFJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
[1]	Gdy rodzaj naruszenia ma miejsce dla opisu ″G″, nazwa obiektu składa się z nazwy obiektu *SRVPGM zawierającego wyjście, dla którego wykryty został błąd. Więcej informacji na temat rodzajów naruszeń zawiera Tabela 126 na stronie 243.				
[2]	To pole zawiera nazwę użytkownika, który spowodował powstanie pozycji. Może to być użytkownik QSYS, w następujących przypadkach: • dla rekordów *TYPE2 pozycje 41 i 118, • dla rekordów *TYPE4 pozycje 55 i 132, • dla rekordów *TYPE5 pozycje 65 i 187.				
[3]	Te pola używane są tylko dla obiektów w systemach plików QOpenSys, "root", użytkownika i QFileSvr.400.				
[4]	Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.				
[5]	Gdy rodzaj naruszenia to ″T″, nazwa obiektu składa się z portu TCP/IP, do którego użytkownik nie jest uprawniony. Wartość jest wyrównana do lewej strony i pusta. Pola biblioteki obiektu oraz typu obiektu będą puste.				
[6]	Jeśli typem naruszenia jest O, nazwa obiektu nośnika optycznego jest zawarta w polu nazwy obiektu zintegrowanego systemu plików. Pola identyfikatora kraju lub regionu, identyfikatora języka, pliku nadrzędnego oraz pliku obiektu będą puste.				
[7]	Tworzony obiekt klasy języka Java może nie rozszerzać swojej klasy bazowej, ponieważ klasa bazowa ma atrybuty systemowe Java.				
[8]	Gdy indykator bezwzględnej nazwy ścieżki (pozycja 1061) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla nazwy ścieżki. Gdy wskaźnikiem bezwzględnej nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.				
[9]	Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.				
[10]	Jeśli obiekt znajduje się w bibliotece, jest to informacja puli ASP biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja obiektu.				
[11]	Gdy typem naruszenia jest X, a wartością kodu naruszenia operacji jest LIC, wskazuje, że poprawka do Licencjonowanego Kodu Wewnętrznego nie została zastosowana z powodu naruszenia podpisu. To pole zawiera numer poprawki do Licencjonowanego Kodu Wewnętrznego, której zastosowanie nie powiodło się.				

Tabela 158. Pozycje kroniki AP (uprawnienie adoptowane). Zbiór opisów pól QASYAPJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	**S** Uruchomienie **E** Zakończenie **A** Uprawnienia adoptowane użyte podczas aktywowania programu
157	225	611	Nazwa obiektu	Char(10)	Nazwa programu, programu usługowego lub pakietu SQL
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Profil użytkownika właściciela	Char(10)	Nazwa profilu użytkownika, którego uprawnienia są adoptowane.

Tabela 158. Pozycje kroniki AP (uprawnienie adoptowane) (kontynuacja). Zbiór opisów pól QASYAPJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
195	263	649	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	279	665	Nazwa puli ASP[1]	Char(10)	Nazwa urządzenia puli ASP.
	289	675	Numer puli ASP [1]	Char(5)	Numer urządzenia puli ASP.

1 Jeśli obiekt znajduje się w bibliotece, jest to informacja puli ASP biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja obiektu.

Tabela 159. Pozycje kroniki AU (Zmiany atrybutu). Zbiór opisów pól QASYAUJ5

Pozycja (Offset)			
J5	**Pole**	**Format**	**Opis**
610	Typ pozycji	Char(1)	Typ pozycji.
			E Atrybuty konfiguracji EIM
611	Działanie	Char(3)	Działanie
			CHG Zmieniono atrybuty
614	Nazwa	Char(100)	Nazwa atrybutu
714	Długość nowej wartości	Binary(4)	Długość nowej wartości
716	Identyfikator CCSID nowej wartości	Binary(5)	Identyfikator CCSID nowej wartości
720	Identyfikator kraju lub regionu nowej wartości	Char(2)	Identyfikator kraju lub regionu nowej wartości
722	Identyfikator języka nowej wartości	Char(3)	Identyfikator języka nowej wartości
725	Nowa wartość	Char(2002) [1]	Nowa wartość
2727	Długość poprzedniej wartości	Binary(4)	Długość poprzedniej wartości
2729	Identyfikator CCSID poprzedniej wartości	Binary(5)	Identyfikator CCSID poprzedniej wartości
2733	Identyfikator kraju lub regionu poprzedniej wartości	Char(2)	Identyfikator kraju lub regionu poprzedniej wartości
2735	Identyfikator języka poprzedniej wartości	Char(3)	Identyfikator języka poprzedniej wartości
2738	Poprzednia wartość	Char(2002) [1]	Poprzednia wartość

1 Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość pola.

Tabela 160. Pozycje kroniki CA (Zmiany uprawnień). Zbiór opisów pól QASYCAJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.

Tabela 160. Pozycje kroniki CA (Zmiany uprawnień) (kontynuacja). Zbiór opisów pól QASYCAJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Zmiany uprawnień
157	225	611	Nazwa obiektu	Char(10)	Nazwa obiektu.
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki, w której znajduje się obiekt.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Nazwa użytkownika	Char(10)	Nazwa profilu użytkownika, którego uprawnienia są nadawane lub odbierane.
195	263	649	Nazwa listy autoryzacji	Char(10)	Nazwa listy autoryzacji.
					Uprawnienia nadawane lub odbierane:
205	273	659	Istnienie obiektu	Char(1)	**Y** *OBJEXIST
206	274	660	Zarządzanie obiektami	Char(1)	**Y** *OBJMGT
207	275	661	Operacyjne do obiektu	Char(1)	**Y** *OBJOPR
208	276	662	Zarządzanie listą autoryzacji	Char(1)	**Y** *AUTLMGT
209	277	663	Lista autoryzacji	Char(1)	**Y** Uprawnienia publiczne *AUTL
210	278	664	Uprawnienie do odczytu	Char(1)	**Y** *READ
211	279	665	Uprawnienie do dodawania	Char(1)	**Y** *ADD
212	280	666	Uprawnienie do aktualizacji	Char(1)	**Y** *UPD
213	281	667	Uprawnienie do usuwania	Char(1)	**Y** *DLT
214	282	668	Uprawnienie na wyłączność	Char(1)	**Y** *EXCLUDE
215	283	669	Uprawnienie do uruchamiania	Char(1)	**Y** *EXECUTE
216	284	670	Uprawnienie do zmiany obiektu	Char(1)	**Y** *OBJALTER
217	285	671	Uprawnienie odniesienia do obiektu	Char(1)	**Y** *OBJREF
218	286	672	(Obszar zastrzeżony)	Char(4)	
222	290	676	Typ komendy	Char(3)	Typ użytej komendy. **GRT** Nadanie **RPL** Nadanie z zastąpieniem **RVK** Odwołanie **USR** Operacja GRTUSRAUT
225	293	679	Nazwa pola	Char(10)	Nazwa pola.
235	303	689	(Obszar zastrzeżony)	Char(10)	
245	313	699	Użytkownik biurowy	Char(10)	Nazwa użytkownika biurowego.
255	323	709	Nazwa DLO	Char(12)	Nazwa DLO.

Tabela 160. Pozycje kroniki CA (Zmiany uprawnień) (kontynuacja). Zbiór opisów pól QASYCAJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
267	335	721	(Obszar zastrzeżony)	Char(8)	
275	343	729	Ścieżka folderu	Char(63)	Ścieżka do folderu.
338	406	792	Praca w imieniu użytkownika	Char(10)	Użytkownik pracujący w imieniu innego użytkownika.
348	416	802	Status osobisty	Char(1)	**Y** Zmiana statusu osobistego
349	417	803	Kod dostępu	Char(1)	**A** Dodanie kodu dostępu **R** Usunięcie kodu dostępu
350	418	804	Kod dostępu	Char(4)	Kod dostępu.
354			(Obszar zastrzeżony)	Char(20)	
	422	808	(Obszar zastrzeżony)	Char(18)	
	440	826	Długość nazwy obiektu [1]	Binary(4)	Długość nazwy obiektu.
374	442	828	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.
378	446	832	Identyfikator kraju lub regionu nazwy obiektu[1]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
380	448	834	Identyfikator języka nazwy obiektu[1]	Char(3)	Identyfikator języka dla nazwy obiektu.
383	451	837	(Obszar zastrzeżony)	Char(3)	
386	454	840	Identyfikator pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
402	470	856	Identyfikator pliku obiektu[1,2]	Char(16)	Identyfikator pliku obiektu.
418	486	872	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	998	1384	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	1014	1400	Nazwa puli ASP [5]	Char(10)	Nazwa urządzenia puli ASP.
	1024	1410	Numer puli ASP [5]	Char(5)	Numer urządzenia puli ASP.
	1029	1415	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	1033	1419	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	1035	1421	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	1038	1424	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.

Tabela 160. Pozycje kroniki CA (Zmiany uprawnień) (kontynuacja). Zbiór opisów pól QASYCAJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1040	1426	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	1041	1427	Identyfikator pliku o dostępie pośrednim[3]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	1057	1443	Bezwzględna nazwa ścieżki[4]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

1 Te pola używane są tylko dla obiektów w systemach plików QOpenSys, "root", użytkownika i QFileSvr.400.

2 Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

3 Gdy indykator nazwy ścieżki (pozycja 1040) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

4 Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

5 Jeśli obiekt znajduje się w bibliotece, jest to informacja puli ASP biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja obiektu.

Tabela 161. Pozycje kroniki CD (łańcuch komendy). Zbiór opisów pól QASYCDJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **C** Uruchomiono komendę **L** Instrukcja OCL **O** Komenda sterująca operatora **P** Procedura S/36 **S** Uruchomiono komendę po podstawieniu komendy. **U** Instrukcja sterująca programu narzędziowego
157	225	611	Nazwa obiektu	Char(10)	Nazwa obiektu.
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki, w której znajduje się obiekt.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Uruchomienie z programu CL	Char(1)	**Y** Tak **N** Nie
186	254	640	Łańcuch komendy	Char(6000)	Komenda, która została uruchomiona, razem z parametrami.

Tabela 161. Pozycje kroniki CD (łańcuch komendy) (kontynuacja). Zbiór opisów pól QASYCDJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
		6640	Nazwa puli ASP dla biblioteki komendy	Char(10)	Nazwa puli ASP dla biblioteki komendy
		6650	Numer puli ASP dla biblioteki komendy	Char(5)	Numer puli ASP dla biblioteki komendy

Tabela 162. Pozycje kroniki CO (tworzenie obiektu). Zbiór opisów pól QASYCOJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **N** Tworzenie nowego obiektu **R** Zastąpienie istniejącego obiektu
157	225	611	Nazwa obiektu	Char(10)	Nazwa obiektu.
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki, w której znajduje się obiekt.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	(Obszar zastrzeżony)	Char(20)	
205	273	659	Użytkownik biurowy	Char(10)	Nazwa użytkownika biurowego.
215	283	669	Nazwa DLO	Char(12)	Nazwa tworzonego obiektu biblioteki dokumentów.
227	295	681	(Obszar zastrzeżony)	Char(8)	
235	303	689	Ścieżka folderu	Char(63)	Ścieżka do folderu.
298	366	752	Praca w imieniu użytkownika	Char(10)	Użytkownik pracujący w imieniu innego użytkownika.
308			(Obszar zastrzeżony)	Char(20)	
	376	762	(Obszar zastrzeżony)	Char(18)	
	394	780	Długość nazwy obiektu	Binary(4)	Długość nazwy obiektu.
328	396	782	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.
332	400	786	Identyfikator kraju lub regionu nazwy obiektu[1]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
334	402	788	Identyfikator języka nazwy obiektu[1]	Char(3)	Identyfikator języka dla nazwy obiektu.
337	405	791	(Obszar zastrzeżony)	Char(3)	
340	408	794	Identyfikator pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.

Tabela 162. Pozycje kroniki CO (tworzenie obiektu) (kontynuacja). Zbiór opisów pól QASYCOJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
356	424	810	Identyfikator pliku obiektu[1,2]	Char(16)	Identyfikator pliku obiektu.
372	440	826	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	952	1338	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	968	1354	Nazwa puli ASP [5]	Char(10)	Nazwa urządzenia puli ASP.
	978	1364	Numer puli ASP [5]	Char(5)	Numer urządzenia puli ASP.
	983	1369	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	987	1373	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	989	1375	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	992	1378	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.
	994	1380	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	995	1381	Identyfikator pliku o dostępie pośrednim[3]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	1011	1397	Bezwzględna nazwa ścieżki[4]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

1 Te pola używane są tylko dla obiektów w systemach plików QOpenSys, "root" oraz użytkownika.

2 Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

3 Gdy indykator nazwy ścieżki (pozycja 994) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

4 Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

5 Jeśli obiekt znajduje się w bibliotece, jest to informacja puli ASP biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja obiektu.

Tabela 163. Pozycje kroniki CP (zmiany profilu użytkownika). Zbiór opisów pól QASYCPJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Zmiana w profilu użytkownika

Tabela 163. Pozycje kroniki CP (zmiany profilu użytkownika) (kontynuacja). Zbiór opisów pól QASYCPJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
157	225	611	Nazwa profilu użytkownika	Char(10)	Nazwa profilu użytkownika, który został zmieniony.
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	256	639	Nazwa komendy	Char(3)	Typ użytej komendy.
					CRT CRTUSRPRF
					CHG CHGUSRPRF
					RST RSTUSRPRF
					DST Resetowanie hasła użytkownika QSECOFR za pomocą narzędzi DST
					RPA Funkcja API QSYRESPA
188	256	642	Zmiana hasła	Char(1)	**Y** Hasło zmienione
189	257	643	Hasło *NONE	Char(1)	**Y** Hasło ma wartość *NONE.
190	258	644	Utrata ważności hasła	Char(1)	**Y** Wartość pola utraty ważności hasła to *YES **N** Wartość pola utraty ważności hasła to *NO
191	259	645	Uprawnienia specjalne do wszystkich obiektów	Char(1)	**Y** uprawnienia specjalne *ALLOBJ
192	260	646	Uprawnienia specjalne do kontroli zadań	Char(1)	**Y** Uprawnienia specjalne *JOBCTL
193	261	647	Uprawnienia specjalne do składowania systemu	Char(1)	**Y** Uprawnienia specjalne *SAVSYS
194	262	648	Uprawnienia specjalne administratora ochrony	Char(1)	**Y** Uprawnienie specjalne *SECADM.
195	263	649	Uprawnienia specjalne do sterowania buforem	Char(1)	**Y** Uprawnienia specjalne *SPLCTL
196	264	650	Uprawnienia specjalne Service	Char(1)	**Y** Uprawnienia specjalne *SERVICE
197	265	651	Uprawnienia specjalne do kontrolowania	Char(1)	**Y** Uprawnienia specjalne *AUDIT
198	266	652	Uprawnienia specjalne do konfiguracji systemu	Char(1)	**Y** Uprawnienia specjalne *IOSYSCFG
199	267	653	(Obszar zastrzeżony)	Char(13)	
212	280	666	Profil grupowy	Char(10)	Nazwa profilu grupowego.
222	290	676	Właściciel	Char(10)	Właściciel obiektów tworzonych jako podzbiory profilu grupowego.

Tabela 163. Pozycje kroniki CP (zmiany profilu użytkownika) (kontynuacja). Zbiór opisów pól QASYCPJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
232	300	686	Uprawnienie grupowe	Char(10)	Uprawnienie profilu grupowego.
242	310	696	Program początkowy	Char(10)	Nazwa programu początkowego użytkownika.
252	320	706	Biblioteka programu początkowego	Char(10)	Nazwa biblioteki, w której znaleziono program początkowy.
262	330	716	Menu początkowe	Char(10)	Nazwa menu początkowego użytkownika.
272	340	726	Biblioteka menu początkowego	Char(10)	Nazwa biblioteki, w której znaleziono menu początkowe.
282	350	736	Biblioteka bieżąca	Char(10)	Nazwa biblioteki bieżącej użytkownika.
292	360	746	Ograniczone możliwości	Char(10)	Wartość parametru ograniczonych możliwości.
302	370	756	Klasa użytkownika	Char(10)	Klasa użytkownika.
312	380	766	Ograniczenie priorytetu	Char(1)	Wartość parametru ograniczenia priorytetu.
313	381	767	Status profilu	Char(10)	Status profilu użytkownika.
323	391	777	Typ uprawnień grupowych	Char(10)	Wartość parametru GRPAUTTYP.
333	401	787	Dodatkowe profile grupowe	Char(150)	Nazwy do 15 dodatkowych profili grupowych dla użytkownika.
483	551	937	Identyfikator użytkownika	Char(10)	uid dla użytkownika.
493	561	947	Identyfikator grupy	Char(10)	gid dla użytkownika.
503	571	957	Zarządzanie hasłem lokalnym	Char(10)	Wartość parametru LCLPWDMGT.

*Tabela 164. Pozycje kroniki CQ (Zmiany *CRQD).* Zbiór opisów pól QASYCQJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Zmiana obiektu *CRQD
157	225	611	Nazwa obiektu	Char(10)	Nazwa zmienionego obiektu.
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki obiektu.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
		639	Nazwa puli ASP	Char(10)	Nazwa puli ASP dla biblioteki obiektu CRQD
		649	Numer puli ASP	Char(5)	Numer puli ASP dla biblioteki obiektu CRQD

Tabela 165. Pozycje kroniki CU (Operacje klastra). Zbiór opisów pól QASYCUJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505 i Tabela 153 na stronie 507.
	224	610	Typ pozycji	Char(1)	Typ pozycji. **M** Sterowanie klastrem **R** Zarządzanie grupą zasobów klastra (*GRP)
	225	611	Pozycja działania	Char(3)	Typ działania. **ADD** Dodanie **CRT** Tworzenie **DLT** Usunięcie **DST** Dystrybucja **END** Zakończenie **FLO** Przełączanie awaryjne **LST** Informacje o liście **RMV** Usuwanie **STR** Uruchomienie **SWT** Przełączenie **UPC** Aktualizowanie atrybutów
	228	614	Status	Char(3)	Status żądania. **ABN** Żądanie zakończone niepoprawnie **AUT** Błąd uprawnień, wymagane uprawnienia *IOSYSCFG **END** Żądanie zakończone pomyślnie **STR** Żądanie zostało uruchomione
	231	617	Nazwa obiektu CRG	Char(10)	Nazwa obiektu grupy zasobów klastra. **Uwaga:** Ta wartość jest podana, gdy typem pozycji jest R.
	241	627	Nazwa biblioteki CRG	Char(10)	Biblioteka obiektu grupy zasobów klastra. **Uwaga:** Ta wartość jest podana, gdy typem pozycji jest R.
	251	637	Nazwa klastra	Char(10)	Nazwa klastra.
	261	647	Identyfikator węzła	Char(8)	Identyfikator węzła.
	269	655	Identyfikator węzła źródłowego	Char(8)	Identyfikator węzła źródłowego.
	277	663	Nazwa użytkownika źródłowego	Char(10)	Nazwa użytkownika systemu źródłowego, który zainicjował żądanie.
	287	673	Nazwa kolejki użytkownika	Char(10)	Nazwa kolejki użytkownika, do której mają być wysyłane odpowiedzi.
	297	683	Biblioteka kolejki użytkownika	Char(10)	Biblioteka kolejki użytkownika.

Tabela 165. Pozycje kroniki CU (Operacje klastra) (kontynuacja). Zbiór opisów pól QASYCUJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
		693	Nazwa puli ASP	Char(10)	Nazwa puli ASP dla biblioteki kolejki użytkownika
		703	Numer puli ASP	Char(5)	Numer puli ASP dla biblioteki kolejki użytkownika

Tabela 166. Pozycje kroniki CV (Sprawdzanie przełączenia). Zbiór opisów pól QASYCVJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505 i Tabela 153 na stronie 507.
	224	610	Typ pozycji	Char(1)	Typ pozycji. **C** Ustanowiono połączenie **E** Zakończono połączenie **R** Połączenie odrzucone
	225	611	Działanie	Char(1)	Działania podjęte dla typu połączenia. ″ ″ Połączenie ustanowiono lub zakończono normalnie. Używane dla typu pozycji C lub E. **A** Węzeł sieci nie został uwierzytelniony. Używane dla typu pozycji E lub R. **C** Brak odpowiedzi z serwera uwierzytelniania. Używane dla typu pozycji R. **L** Błąd konfiguracji LCP. Używane dla typu pozycji R. **N** Błąd konfiguracji NCP. Używane dla typu pozycji R. **P** Hasło nie jest poprawne. Używane dla typu pozycji E lub R. **R** Uwierzytelnianie zostało odrzucone przez węzeł sieci. Używane dla typu pozycji R. **T** Błąd konfiguracji L2TP. Używane dla typu pozycji E lub R. **U** Użytkownik nie jest poprawny. Używane dla typu pozycji E lub R.
	226	612	Nazwa profilu punkt z punktem	Char(10)	Nazwa profilu punkt z punktem.
	236	622	Protokół	Char(10)	Typ pozycji. **L2TP** Protokół tunelowania Layer 2 (L2T) **PPP** Protokół punkt z punktem. **SLIP** Protokół Serial Line Internet Protocol.

Tabela 166. Pozycje kroniki CV (Sprawdzanie przełączenia) (kontynuacja). Zbiór opisów pól QASYCVJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	246	632	Metoda uwierzytelniania lokalnego	Char(10)	Typ pozycji. **CHAP** Protokół Challenge Handshake Authentication. **PAP** Protokół Password Authentication Protocol. **SCRIPT** Metoda skryptu.
	256	642	Metoda uwierzytelniania zdalnego	Char(10)	Typ pozycji. **CHAP** Protokół Challenge Handshake Authentication. **PAP** Protokół Password Authentication Protocol. **RADIUS** Metoda serwera Radius. **SCRIPT** Metoda skryptu.
	266	652	Nazwa obiektu	Char(10)	Nazwa obiektu *VLDL.
	276	662	Nazwa biblioteki	Char(10)	Nazwa biblioteki obiektu *VLDL.
	286	672	Nazwa użytkownika *VLDL	Char(100)	Nazwa użytkownika *VLDL.
	386	772	Lokalny adres IP	Char(40)	Lokalny adres IP.
	426	812	Zdalny adres IP	Char(40)	Zdalny adres IP.
	466	852	Przekazywanie IP	Char(1)	Typ pozycji. **Y** Przekazywanie IP jest włączone. **N** Przekazywanie IP jest wyłączone.

Tabela 166. Pozycje kroniki CV (Sprawdzanie przełączenia) (kontynuacja). Zbiór opisów pól QASYCVJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	467	853	Proxy ARP	Char(1)	Typ pozycji. **Y** Proxy ARP jest włączony. **N** Proxy ARP nie jest włączony.
	468	854	Nazwa serwera Radius	Char(10)	Nazwa profilu AAA.
	478	864	Adres IP uwierzytelniania	Char(40)	Adres IP uwierzytelniania.
	518	904	Identyfikator sesji konta	Char(14)	Identyfikator sesji konta.
	532	918	Identyfikator wielu sesji konta	Char(14)	Identyfikator wielu sesji konta.
	546	932	Liczba dowiązań konta	Binary(4)	Liczba dowiązań konta.
	548	934	Typ tunelu	Char(1)	Typ tunelu: **0** Brak tunelowania **3** L2TP **6** AH **9** ESP
	549	935	Punkt końcowy klienta tunelu	Char(40)	Punkt końcowy klienta tunelu.
	589	975	Punkt końcowy serwera tunelu	Char(40)	Punkt końcowy serwera tunelu.
	629	1015	Czas sesji konta	Char(8)	Czas sesji konta. Używany dla typu pozycji E lub R.
	637	1023	Przyczyna zakończenia konta	Binary(4)	Przyczyna zakończenia konta. Używana dla typu pozycji E lub R.
		1025	Nazwa puli ASP	Char(10)	Nazwa puli ASP dla biblioteki listy weryfikacji
		1035	Numer puli ASP	Char(5)	Numer puli ASP dla biblioteki listy weryfikacji

Tabela 167. Pozycje kroniki CY (Konfigurowanie szyfrowania). Zbiór opisów pól QASYCYJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Funkcja kontroli dostępu **F** Funkcja kontroli narzędzia **M** Funkcja klucza głównego

Tabela 167. Pozycje kroniki CY (Konfigurowanie szyfrowania) (kontynuacja). Zbiór opisów pól QASYCYJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	225	611	Działanie	Char(3)	Wykonywana funkcja konfigurowania szyfrowania: **CCP** Definiowanie profilu karty. **CCR** Definiowanie roli karty. **CLK** Ustawianie zegara. **CLR** Usuwanie zawartości kluczy głównych. **CRT** Tworzenie kluczy głównych. **DCP** Usunięcie profilu karty. **DCR** Usunięcie roli karty. **DST** Dystrybucja kluczy głównych. **EID** Ustawienie identyfikatora środowiska. **FCV** Ładowanie/czyszczenie zawartości FCV. **INI** Reinicjowanie karty. **QRY** Rola zapytania lub informacje profilu. **RCP** Zastąpienie profilu karty. **RCR** Zastąpienie roli karty. **RCV** Odebranie kluczy głównych. **SET** Ustawienie kluczy głównych. **SHR** Klonowanie zasobów współużytkowanych.
	228	614	Profil karty	Char(8)	Nazwa profilu karty.
	236	622	Rola karty	Char(8)	Rola profilu karty.
	244	630	Nazwa urządzenia	Char(10)	Nazwa urządzenia szyfrującego.

Tabela 168. DI (serwer katalogów), pozycje kroniki. Zbiór opisów pól QASYDIJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
	224	610	Typ pozycji	Char(1)	Typ pozycji. **L** Operacja LDAP

Tabela 168. DI (serwer katalogów), pozycje kroniki (kontynuacja). Zbiór opisów pól QASYDIJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	225	611	Typ operacji	Char(2)	Typ operacji LDAP: **AD** Zmiana atrybutu kontroli. **AF** Błąd uprawnień. **BN** Łączenie powiodło się. **CA** Zmiana uprawnień do obiektu. **CF** Zmiana konfiguracji. **CO** Tworzenie obiektu. **CP** Zmiana hasła. **DO** Usunięcie obiektu. **EX** Eksportowanie katalogu LDAP. **IM** Importowanie katalogu LDAP. **OM** Zarządzanie obiektem (zmiana nazwy). **OW** Zmiana prawa własności. **PW** Awaria hasła. **UB** Odłączanie powiodło się. **ZC** Zmiana obiektu. **ZR** Odczytanie obiektu.
	227	613	Kod błędu uprawnień	Char(1)	Kod dla błędów uprawnień. To pole używane jest tylko wtedy, gdy typ operacji (pozycja 225) to AF. **A** Nieuprawniona próba zmiany wartości kontroli. **B** Nieuprawniona próba łączenia. **C** Nieuprawniona próba utworzenia obiektu. **D** Nieuprawniona próba usunięcia obiektu. **E** Nieuprawniona próba eksportu. **F** Nieuprawniona zmiana konfiguracji (administrator, protokół zmian, biblioteka postprocesora, repliki, publikowanie replik) **I** Nieuprawniona próba importu. **M** Nieuprawniona próba zmiany. **R** Nieuprawniona próba odczytu (wyszukiwania).
	228	614	Zmiana konfiguracji	Char(1)	Zmiany konfiguracji. To pole jest używane, gdy typ operacji (pozycja 225) to CF. **A** Zmiana nazwy administratora **C** Zmiana logowania/wylogowywania **L** Zmiana nazwy biblioteki postprocesora **P** Zmiana agenta publikowania **R** Zmiana serwera replik

Tabela 168. DI (serwer katalogów), pozycje kroniki (kontynuacja). Zbiór opisów pól QASYDIJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	229	615	Kod zmiany konfiguracji	Char(1)	Kod zmian konfiguracji. To pole jest używane tylko wtedy, gdy typ operacji (pozycja 225) to CF. **A** Dodanie elementu do konfiguracji **D** Usunięcie elementu z konfiguracji **M** Modyfikacja elementu
	230	616	Flaga propagacji	Char(1)	Wskazuje nowe ustawienie właściciela lub wartość propagacji ACL. To pole jest używane tylko wtedy gdy typ operacji (pozycja 225) to CA. **T** Prawda **F** Fałsz
	231	617	Wybór uwierzytelniania połączenia	Char(20)	Wybór uwierzytelniania połączenia. To pole jest używane tylko wtedy, gdy typ operacji (pozycja 225) to BN.
	251	637	Wersja LDAP	Char(4)	Wersja klienta żądającego. To pole jest używane tylko wtedy, gdy operacja przeprowadzana jest za pośrednictwem serwera LDAP. **2** LDAP wersja 2 **3** LDAP wersja 3
	255	641	Indykator SSL	Char(1)	Wskazuje, czy w żądaniu użyto protokołu SSL. To pole jest używane tylko wtedy, gdy operacja przeprowadzana jest za pośrednictwem serwera LDAP. **0** Nie **1** Tak
	256	642	Rodzaj żądania	Char(1)	Rodzaj żądania. To pole używane jest tylko gdy operacja przeprowadzana jest za pośrednictwem serwera LDAP. **A** Uwierzytelnione **N** Anonimowe **U** Nieuwierzytelnione
	257	643	Identyfikator połączenia	Char(20)	Identyfikator połączenia żądania. To pole używane jest tylko gdy operacja przeprowadzana jest za pośrednictwem serwera LDAP.
	277	663	Adres IP klienta	Char(50)	Adres IP i numer portu klienta. To pole używane jest tylko gdy operacja przeprowadzana jest za pośrednictwem serwera LDAP.
	327	713	Identyfikator CCSID nazwy użytkownika	Bin(5)	Identyfikator kodowanego zestawu znaków (CCSID) nazwy użytkownika.
	331	717	Długość nazwy użytkownika	Bin(4)	Długość nazwy użytkownika.
	333	719	Nazwa użytkownika[1]	Char(2002)	Nazwa użytkownika LDAP.
	2335	2721	Identyfikator CCSID nazwy obiektu	Bin(5)	Identyfikator kodowanego zestawu znaków (CCSID) nazwy obiektu.
	2339	2725	Długość nazwy obiektu	Bin(4)	Długość nazwy obiektu.
	2341	2727	Nazwa obiektu[1]	Char(2002)	Nazwa obiektu LDAP.

Tabela 168. DI (serwer katalogów), pozycje kroniki (kontynuacja). Zbiór opisów pól QASYDIJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	4343	4729	Identyfikator CCSID nazwy właściciela	Bin(5)	Identyfikator kodowanego zestawu znaków (CCSID) nazwy właściciela. To pole jest używane tylko wtedy, gdy typ operacji (pozycja 225) to OW.
	4347	4733	Długość nazwy właściciela	Bin(4)	Długość nazwy właściciela. To pole jest używane tylko wtedy, gdy typ operacji to OW.
	4349	4735	Nazwa właściciela[1]	Char(2002)	Nazwa właściciela. To pole używane jest tylko gdy typ operacji (pozycja 225) to OW.
	6351	6737	Identyfikator CCSID nowej nazwy	Bin(5)	Identyfikator kodowanego zestawu znaków (CCSID) nowej nazwy. To pole jest używane tylko wtedy, gdy typ operacji (pozycja 225) to OM, OW, ZC lub AF+M. • Dla typu operacji OM, to pole będzie zawierało identyfikator CCSID nowej nazwy obiektu. • Dla typu operacji OW, to pole będzie zawierało identyfikator CCSID nowej nazwy właściciela. • Dla typu operacji ZC lub AF+M, to pole będzie zawierało identyfikator CCSID listy typów zmienionych atrybutów z pola Nowa nazwa.
	6355	6741	Długość nowej nazwy	Bin(4)	Długość nowej nazwy. To pole używane jest tylko gdy typ operacji (pozycja 225) to OM, OW, ZC lub AF+M. • Dla typu operacji OM, to pole będzie zawierało długość nowej nazwy obiektu. • Dla typu operacji OW, to pole będzie zawierało długość nowej nazwy właściciela. • Dla typu operacji ZC lub AF+M, to pole będzie zawierało długość listy typów zmienionych atrybutów z pola Nowa nazwa.
	6357	6743	Nowa nazwa[1]	Char(2002)	Nowa nazwa. To pole używane jest tylko gdy typ operacji (pozycja 225) to OM, OW, ZC lub AF+M. • Dla typu operacji OM, to pole będzie zawierało nową nazwę obiektu. • Dla typu operacji OW, to pole będzie zawierało nową nazwę właściciela. • Dla typu operacji ZC lub AF+M, to pole będzie zawierało listę typów zmienionych atrybutów.
	8359	8745	Identyfikator pliku obiektu[2]	Char(16)	Identyfikator pliku obiektu do eksportowania.
	8375	8761	Nazwa puli ASP [2]	Char(10)	Nazwa urządzenia puli ASP.
	8385	8771	Numer puli ASP [2]	Char(5)	Numer urządzenia puli ASP.
	8390	8776	Identyfikator CCSID nazwy ścieżki[2]	Bin(5)	Identyfikator kodowanego zestawu znaków bezwzględnej nazwy ścieżki.
	8394	8780	Identyfikator kraju lub regionu nazwy ścieżki[2]	Char(2)	Identyfikator kraju lub regionu bezwzględnej nazwy ścieżki.
	8396	8782	Identyfikator języka nazwy ścieżki[2]	Char(3)	Identyfikator języka bezwzględnej nazwy ścieżki.
	8399	8785	Długość nazwy ścieżki[2]	Bin(4)	Długość nazwy bezwzględnej nazwy ścieżki.

Tabela 168. DI (serwer katalogów), pozycje kroniki (kontynuacja). Zbiór opisów pól QASYDIJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	8401	8787	Indykator pełnej nazwy ścieżki[2]	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki. **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	8402	8788	Identyfikator pliku o dostępie pośrednim[2,3]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	8418	8804	Bezwzględna nazwa ścieżki[1,2]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.
		13806	Profil użytkownika lokalnego	Char(10)	Nazwa profilu użytkownika lokalnego, która jest odwzorowywana na nazwę użytkownika LDAP (J5 pozycja 719). Puste miejsce oznacza brak odwzorowania profilu użytkownika.
		13816	Indykator administratora	Char(1)	Indykator administratora dla nazwy użytkownika LDAP (J5 pozycja 719). **Y** Użytkownik LDAP jest administratorem. **N** Użytkownik LDAP nie jest administratorem. **U** W tym momencie nie wiadomo, czy użytkownik LDAP jest administratorem.

[1] Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość wartości tego pola.

[2] Te pola używane są tylko wtedy, gdy typ operacji (pozycja 225) to EX lub IM.

[3] Gdy indykator nazwy ścieżki (pozycja 8401) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

Tabela 169. Pozycje kroniki DO (Operacja usunięcia). Zbiór opisów pól QASYDOJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Obiektu nie usunięto za pomocą kontroli transakcji **C** Oczekujące usunięcie obiektu zostało zatwierdzone **D** Oczekujące tworzenie obiektu zostało wycofane **P** Oczekiwanie na usunięcie obiektu (usuwanie zostało przeprowadzone za pomocą kontroli transakcji) **R** Oczekujące usuwanie obiektu zostało wycofane

Tabela 169. Pozycje kroniki DO (Operacja usunięcia) (kontynuacja). Zbiór opisów pól QASYDOJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
157	225	611	Nazwa obiektu	Char(10)	Nazwa obiektu.
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki, w której znajduje się obiekt.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	(Obszar zastrzeżony)	Char(20)	
205	273	659	Użytkownik biurowy	Char(10)	Nazwa użytkownika biurowego.
215	283	669	Nazwa DLO	Char(12)	Nazwa obiektu biblioteki dokumentów.
227	295	681	(Obszar zastrzeżony)	Char(8)	
235	303	689	Ścieżka folderu	Char(63)	Ścieżka do folderu.
298	366	752	Praca w imieniu użytkownika	Char(10)	Użytkownik pracujący w imieniu innego użytkownika.
308			(Obszar zastrzeżony)	Char(20)	
	376	762	(Obszar zastrzeżony)	Char(18)	
	394	780	Długość nazwy obiektu [1]	Binary(4)	Długość nazwy obiektu.
328	396	782	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.
332	400	786	Identyfikator kraju lub regionu nazwy obiektu[1]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
334	402	788	Identyfikator języka nazwy obiektu[1]	Char(3)	Identyfikator języka dla nazwy obiektu.
337	405	791	(Obszar zastrzeżony)	Char(3)	
340	408	794	Identyfikator pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
356	424	810	Identyfikator pliku obiektu[1,2]	Char(16)	Identyfikator pliku obiektu.
372	440	826	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	952	1338	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	968	1354	Nazwa puli ASP [5]	Char(10)	Nazwa urządzenia puli ASP.
	978	1364	Numer puli ASP [5]	Char(5)	Numer urządzenia puli ASP.
	983	1369	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	987	1373	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	989	1375	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	992	1378	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.

Tabela 169. Pozycje kroniki DO (Operacja usunięcia) (kontynuacja). Zbiór opisów pól QASYDOJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	994	1380	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	995	1381	Identyfikator pliku o dostępie pośrednim[3]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	1011	1397	Bezwzględna nazwa ścieżki[4]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

[1] Te pola używane są tylko dla obiektów w systemach plików QOpenSys, "root" oraz użytkownika.

[2] Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

[3] Gdy indykator nazwy ścieżki (pozycja 994) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

[4] Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

[5] Jeśli obiekt znajduje się w bibliotece, jest to informacja puli ASP biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja obiektu.

Tabela 170. Pozycje kroniki DS (Resetowanie identyfikatora użytkownika IBM narzędzi serwisowych). Zbiór opisów pól QASYDSJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Resetowanie hasła identyfikatora użytkownika narzędzi seriwsowych. **C** Zmiana identyfikatora użytkownika narzędzi serwisowych. **P** Hasło identyfikatora użytkownika narzędzi serwisowych został zmienione.
157	225	611	Resetowanie identyfikatora użytkownika IBM narzędzi SST	Char(1)	**Y** Żądanie zresetowania identyfikatora użytkownika IBM narzędzi serwisowych.
158	226	612	Typ identyfikatora użytkownika narzędzi serwisowych	Char(10)	Typ identyfikatora użytkownika narzędzi serwisowych ***SECURITY** ***FULL** ***BASIC**

Tabela 170. Pozycje kroniki DS (Resetowanie identyfikatora użytkownika IBM narzędzi serwisowych) (kontynuacja). Zbiór opisów pól QASYDSJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
168	236	622	Nowa nazwa identyfikatora użytkownika narzędzi serwisowych	Char(8)	Nazwa identyfikatora użytkownika narzędzi serwisowych.
176	244	630	Zmiana hasła identyfikatora użytkownika narzędzi serwisowych	Char(1)	Żądanie zmiany hasła identyfikatora użytkownika narzędzi seriwsowych. **Y** Żądanie zmiany hasła identyfikatora użytkownika narzędzi seriwsowych.
	245	631	Nowa nazwa identyfikatora użytkownika narzędzi serwisowych	Char(10)	Nazwa identyfikatora użytkownika narzędzi serwisowych.
	255	641	Profil żądający identyfikatora użytkownika narzędzi serwisowych	Char(10)	Nazwa identyfikatora użytkownika narzędzi serwisowych, który żąda zmiany.

Tabela 171. Pozycje kroniki EV (Zmienna środowiskowa). Zbiór opisów pól QASYEVJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Dodanie **C** Zmiana **D** Usunięcie
	225	611	Obcięta nazwa	Char(1)	Wskazuje, czy nazwa zmiennej środowiskowej (pozycja 232), jest obcięta. **Y** Nazwa zmiennej środowiskowej jest obcięta. **N** Nazwa zmiennej środowiskowej nie jest obcięta.
	226	612	Identyfikator CCSID	Binary(5)	Identyfikator CCSID nazwy zmiennej środowiskowej.
	230	616	Długość	Binary(4)	Długość nazwy zmiennej środowiskowej.
	232	618	Nazwa zmiennej środowiskowej[2]	Char(1002)	Nazwa zmiennej środowiskowej.

Tabela 171. Pozycje kroniki EV (Zmienna środowiskowa) (kontynuacja). Zbiór opisów pól QASYEVJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1234	1620	Nowa obcięta nazwa[1]	Char(1)	Wskazuje, czy nowa nazwa zmiennej środowiskowej (pozycja 1241), jest obcięta. **Y** Wartość zmiennej środowiskowej jest obcięta. **N** Wartość zmiennej środowiskowej nie jest obcięta.
	1235	1621	Identyfikator CCSID nowej nazwy[1]	Binary(5)	Identyfikator CCSID nowej nazwy zmiennej środowiskowej.
	1239	1625	Długość nowej nazwy[1]	Binary(4)	Długość nowej nazwy zmiennej środowiskowej.
	1241	1627	Nowa nazwa zmiennej środowiskowej[1,2]	Char (1002)	Nowa nazwa zmiennej środowiskowej.

1 Te pola są używane, gdy typ pozycji to C.

2 Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy zmiennej środowiskowej.

Tabela 172. Pozycje kroniki GR (Rekord ogólny). Zbiór opisów pól QASYGRJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505 i Tabela 153 na stronie 507.
	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Dodano program obsługi wyjścia **C** Monitorowanie zasobów operacji i operacje sterowania **D** Usunięto program obsługi wyjścia **F** Operacje rejestrowania funkcji. **R** Zastąpiono program obsługi wyjścia
	225	611	Działanie	Char(2)	Wykonywane działanie. **ZC** Zmiana **ZR** Odczyt
	227	613	Nazwa użytkownika	Char(10)	Nazwa profilu użytkownika Dla typu pozycji F, to pole zawiera nazwę użytkownika, dla którego wykonywana była operacja rejestrowania funkcji.
	237	623	Identyfikator CCSID pola 1	Binary(5)	Wartość identyfikatora CCSID dla pola 1.
	241	627	Długość pola 1	Binary (4)	Długość danych w polu 1.

Tabela 172. Pozycje kroniki GR (Rekord ogólny) (kontynuacja). Zbiór opisów pól QASYGRJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	243	629	Pole 1	Char(102)[1]	Dane pola 1 Dla typu pozycji F, to pole zawiera opis wykonanej operacji rejestrowania funkcji. Możliwe wartości to: ***REGISTER:** Funkcja została zarejestrowana ***REREGISTER:** Funkcja została zaktualizowana ***DEREGISTER:** Funkcja została wyrejestrowana ***CHGUSAGE:** Informacje o używaniu funkcji zostały zmienione ***CHKUSAGE:** Dla użytkownika sprawdzono użycie funkcji i sprawdzenie zostało zatwierdzone ***USAGEFAILURE:** Dla użytkownika sprawdzono użycie funkcji i sprawdzenie nie powiodło się Dla typów pozycji A, D i R, to pole będzie zawierało informacje o programie obsługi wyjścia dla danej funkcji, która była wykonywana. Dla typu pozycji C, to pole zawiera nazwę funkcji RMC, którą próbowano uruchomić. Możliwe wartości to: • **mc_reg_event_select** Rejestrowanie zdarzenia za pomocą wyboru atrybutu • **mc_reg_event_handle** Rejestrowanie zdarzenia za pomocą uchwytu zasobu • **mc_reg_class_event** Rejestrowanie zdarzenia dla klasy zasobu • **mc_unreg_event** Wyrejestrowanie zdarzenia • **mc_define_resource** Definiowanie nowego zasobu • **mc_undefine_resource** Usunięcie definicji zasobu • **mc_set_select** Ustawienie wartości atrybutu zasobu za pomocą wyboru atrybutu • **mc_set_handle** Ustawienie wartości atrybutu zasobu za pomocą uchwytu zasobu • **mc_class_set** Ustawienie wartości atrybutu klasy zasobu • **mc_query_p_select** Zapytanie o stałe atrybuty zasobu za pomocą wyboru atrybutu • **mc_query_d_select** Zapytanie o zmienne atrybuty zasobu za pomocą wyboru atrybutu

Tabela 172. Pozycje kroniki GR (Rekord ogólny) (kontynuacja). Zbiór opisów pól QASYGRJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
243 (cont)					• **mc_query_p_handle** Zapytanie o stałe atrybuty zasobu za pomocą uchwytu zasobu **mc_query_d_handle** Zapytanie o zmienne atrybuty zasobu za pomocą uchwytu zasobu **mc_class_query_p** Zapytanie o stałe atrybuty klasy zasobu **mc_class_query_d** Zapytanie o zmienne atrybuty klasy zasobu **mc_qdef_resource_class** Zapytanie o definicję klasy zasobu **mc_qdef_p_attribute** Zapytanie o definicję stałego atrybutu **mc_qdef_d_attribute** Zapytanie o definicję zmiennego atrybutu **mc_qdef_sd** Zapytanie o definicję danych strukturalnych **mc_qdef_valid_values** Zapytanie o definicję poprawnych wartości stałego atrybutu **mc_qdef_actions** Zapytanie o definicję działań zasobu **mc_invoke_action** Wywołanie działania na zasobie **mc_invoke_class_action** Wywołanie działania na klasie zasobu
	345	731	Identyfikator CCSID pola 2	Binary(5)	Wartość identyfikatora CCSID dla pola 2.
	349	735	Długość pola 2	Binary (4)	Długość danych w polu 2.
	351	737	Pole 2	Char (102)[1]	Dane pola 2 Dla typu pozycji F, to pole zawiera nazwę funkcji, na której wykonywano działanie. Dla typu pozycji C, to pole zawiera nazwę zasobu lub klasy zasobu, dla której próbowano wykonać operację.
	453	839	Identyfikator CCSID pola 3	Binary(5)	Wartość identyfikatora CCSID dla pola 3.
	457	843	Długość pola 3	Binary (4)	Długość danych w polu 3.

Tabela 172. Pozycje kroniki GR (Rekord ogólny) (kontynuacja). Zbiór opisów pól QASYGRJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	459	845	Pole 3	Char(102)[1]	Dane pola 3. Dla typu pozycji F, to pole zawiera ustawienia użycia dla użytkownika. Jeśli operacja rejestrowanie funkcji jest jedną z wymienionych poniżej, wartość będzie podana tylko dla tego pola: ***REGISTER:** Gdy jest to operacja *REGISTER, pole zawiera domyślną wartość użycia. Nazwą użytkownika będzie *DEFAULT. ***REREGISTER:** Gdy jest to operacja *REREGISTER, pole zawiera domyślną wartość użycia. Nazwą użytkownika będzie *DEFAULT. ***CHGUSAGE:** Gdy jest to operacja *CHGUSAGE, pole zawiera wartość użycia dla użytkownika podanego w polu nazwa użytkownika. Dla typu pozycji C to pole zawiera wynik sprawdzania uprawnień, które zostało przeprowadzone dla operacji wskazanej w polu 1. Możliwe są następujące wartości: • *NOAUTHORITYCHECKED: gdy operacja wskazana w polu 1 nie wymaga sprawdzania uprawnień lub z jakiegoś innego powodu sprawdzanie uprawnień nie doszło do skutku. • *AUTHORITYPASSED: gdy odwzorowany identyfikator użytkownika wskazany w polu Nazwa profilu użytkownika pomyślnie przeszedł sprawdzanie uprawnień do operacji wskazanej w polu 1 dla zasobu lub klasy zasobu wskazanego w polu 2. • *AUTHORITYFAILED: gdy odwzorowany identyfikator użytkownika wskazany w polu Nazwa profilu użytkownika niepomyślnie przeszedł sprawdzanie uprawnień do operacji wskazanej w polu 1 dla zasobu lub klasy zasobu wskazanego w polu 2.
	561	947	Identyfikator CCSID pola 4	Binary(5)	Wartość identyfikatora CCSID dla pola 4.
	565	951	Długość pola 4	Binary (4)	Długość danych w polu 4.
	567	953	Pole 4	Char(102)[1]	Dane pola 4. Dla typu pozycji F, to pole zawiera ustawienie *ALLOBJ dla funkcji. Jeśli operacja rejestrowanie funkcji jest jedną z wymienionych poniżej, wartość będzie podana tylko dla tego pola: ***REGISTER** ***REREGISTER**

[1] Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość pola.

Tabela 173. Pozycje kroniki GS (Nadanie deskryptora). Zbiór opisów pól QASYGSJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **G** Nadanie deskryptora **R** Otrzymano deskryptor **U** Nie można użyć deskryptora
157	225	611	Nazwa zadania	Char(10)	Nazwa zadania.
167	235	621	Nazwa użytkownika	Char(10)	Nazwa użytkownika.
177	245	631	Numer zadania	Zoned(6,0)	Numer zadania.
183	251	637	Nazwa profilu użytkownika	Char(10)	Nazwa profilu użytkownika.
	261	647	JUID	Char(10)	Tożsamość użytkownika zadania dla zadania docelowego. (Ta wartość stosowana jest tylko dla podtypu G rekordów kontroli.)

Tabela 174. Pozycje kroniki IP (Komunikacja międzyprocesorowa). Zbiór opisów pól QASYIPJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 na stronie 507 na stronie 507 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Zmiany prawa własności i/lub uprawnień **C** Tworzenie **D** Usunięcie **F** Błąd uprawnień **G** Pobranie **M** Podłączenie pamięci współużytkowanej **Z** Zwykłe zamknięcie semafora lub odłączenie pamięci współużytkowanej
157	225	611	Typ IPC	Char(1)	Typ IPC **M** Pamięć współużytkowana **N** Zwykły semafor **Q** Kolejka komunikatów **S** Semafor
158	226	612	Uchwyt IPC	Binary(5)	Identyfikator uchwytu IPC
162	230	616	Nowy właściciel	Char(10)	Nowy właściciel jednostki IPC
172	240	626	Poprzedni właściciel	Char(10)	Poprzedni właściciel jednostki IPC

Tabela 174. Pozycje kroniki IP (Komunikacja międzyprocesorowa) (kontynuacja). Zbiór opisów pól QASYIPJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
182	250	636	Uprawnienie właściciela	Char(3)	Uprawnienia właściciela do jednostki IPC ***R** odczyt ***W** zapis ***RW** odczyt i zapis
185	253	639	Nowa grupa	Char(10)	Grupa związana z jednostką IPC
195	263	649	Poprzednia grupa	Char(10)	Poprzednia grupa związana z jednostką IPC
205	273	659	Uprawnienie grupowe	Char(3)	Uprawnienia grupowe do jednostki IPC ***R** odczyt ***W** zapis ***RW** odczyt i zapis
208	276	662	Uprawnienia publiczne	Char(3)	Uprawnienia publiczne do jednostki IPC ***R** odczyt ***W** zapis ***RW** odczyt i zapis
211	279	665	Identyfikator CCSID nazwy semafora	Binary(5)	Identyfikator CCSID nazwy semafora.
216	283	669	Długość nazwy semafora	Binary(4)	Długość nazwy semafora.
218	285	671	Nazwa semafora	Char(2050)	Nazwa semafora. **Uwaga:** Jest to pole o zmiennej długości. Dwa pierwsze znaki zawierają długość nazwy semafora.

Tabela 175. Pozycje kroniki IR (Działania reguł IP). Zbiór opisów pól QASYIRJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505 i Tabela 153 na stronie 507.
	224	610	Typ pozycji	Char(1)	Typ pozycji. **L** Reguły IP zostały załadowane z pliku. **N** Reguły IP zostały rozładowane dla połączenia ochrony IP **P** Reguły IP zostały załadowane dla połączenia ochrony IP **R** Reguły IP zostały odczytane i skopiowane do pliku. **U** Reguły IP zostały rozładowane (usunięte).
	225	611	Nazwa zbioru	Char(10)	Nazwa zbioru QSYS użytego do załadowania lub pobrania reguł IP. Jeśli użyty plik nie był plikiem systemu plików QSYS, to pole będzie puste.
	235	621	Biblioteka zbioru	Char(10)	Nazwa biblioteki zbiorów QSYS.

Tabela 175. Pozycje kroniki IR (Działania reguł IP) (kontynuacja). Zbiór opisów pól QASYIRJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	245	631	Zastrzeżone	Char(18)	
	263	649	Długość nazwy zbioru	Binary (4)	Długość nazwy zbioru.
	265	651	Identyfikator CCSID nazwy zbioru[1]	Binary(5)	Identyfikator kodowanego zestawu znaków dla nazwy zbioru.
	269	655	Identyfikator kraju lub regionu zbioru[1]	Char(2)	Identyfikator kraju lub regionu dla nazwy zbioru.
	271	657	Identyfikator języka zbioru[1]	Char(3)	Identyfikator języka dla nazwy zbioru.
	274	660	Zastrzeżone	Char(3)	
	277	663	Identyfikator pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
	293	679	Identyfikator pliku obiektu[1,2]	Char(16)	Identyfikator pliku zbioru.
	309	695	Nazwa zbioru[1]	Char(512)	Nazwa zbioru.
	821	1207	Sekwencja połączenia	Char(40)	Nazwa połączenia.
	861	1247	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	877	1263	Nazwa puli ASP	Char(10)	Nazwa urządzenia puli ASP.
	887	1273	Numer puli ASP [5]	Char(5)	Numer urządzenia puli ASP.
	892	1278	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	896	1282	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	898	1284	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	901	1287	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.
	903	1289	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	904	1290	Identyfikator pliku o dostępie pośrednim[3]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	920	1306	Bezwzględna nazwa ścieżki[4]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

Tabela 175. Pozycje kroniki IR (Działania reguł IP) (kontynuacja). Zbiór opisów pól QASYIRJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
[1]	Te pola używane są tylko dla obiektów w systemach plików QOpenSys i 'root'.				
[2]	Jeśli identyfikator ma ustawiony ostatni lewy bit i resztę bitów zerowych oznacza to, że identyfikator **nie** jest ustawiony.				
[3]	Gdy indykator nazwy ścieżki (pozycja 903) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.				
[4]	Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość pola.				
[5]	Jeśli obiekt znajduje się w bibliotece, jest to informacja puli ASP biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja obiektu.				

Tabela 176. Pozycje kroniki IS (Zarządzanie ochroną internetową). Zbiór opisów pól QASYISJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505 i Tabela 153 na stronie 507.
	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Niepowodzenie (ten typ nie jest już używany) **C** Zwykły (ten typ nie jest już używany) **U** Użytkownik mobilny (ten typ nie jest już używany) **1** Faza 1 IKE uzgodnienia SA **2** Faza 2 IKE uzgodnienia SA
	225	611	Lokalny adres IP	Char(15)	Lokalny adres IP.
	240	626	Port identyfikatora klienta lokalnego	Char(5)	Port identyfikatora klienta lokalnego.
	245	631	Zdalny adres IP	Char(15)	Zdalny adres IP.
	260	646	Port identyfikatora klienta zdalnego	Char(5)	Port identyfikatora klienta zdalnego (poprawny dla fazy 2).
	265	651	Identyfikator urządzenia mobilnego	Char(256)	Identyfikator urządzenia mobilnego. To pole nie jest już używane.
	521	907	Kod wyniku	Char(4)	Wynik uzgadniania: **0** Pomyślne **1–30** Błędy protokołu (dokumentacja w artykule ISAKMP RFC2408, dostępnym pod adresem http://www.ietf.org) **82xx** Błędy programu iSeries VPN Key Manager

Tabela 176. Pozycje kroniki IS (Zarządzanie ochroną internetową) (kontynuacja). Zbiór opisów pól QASYISJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	525	911	Identyfikator CCSID	Bin(5)	Identyfikator kodowanego zestawu znaków dla następujących pól: • Identyfikator lokalny • Wartość identyfikatora klienta lokalnego, • Identyfikator zdalny • Wartość identyfikatora klienta zdalnego.
	529	915	Identyfikator lokalny	Char(256)	Lokalny identyfikator IKE
	785	1171	Typ identyfikatora klienta lokalnego,	Char(2)	Typ identyfikatora klienta (poprawny dla fazy 2): **1** adres IP w wersji 4 **2** pełna nazwa domeny **3** Pełna nazwa domeny użytkownika **4** podsieć IP w wersji 4 **7** zakres adresów IP w wersji 4 **9** nazwa wyróżniająca **11** identyfikator klucza
	787	1173	Wartość identyfikatora klienta lokalnego,	Char(256)	Identyfikator klienta lokalnego (poprawny dla fazy 2)
	1043	1429	Protokół identyfikatora klienta lokalnego	Char(4)	Protokół identyfikatora klienta lokalnego (poprawny dla fazy 2)
	1047	1433	Identyfikator zdalny	Char(256)	Zdalny identyfikator IKE
	1303	1689	Typ identyfikatora klienta zdalnego	Char(2)	Typ identyfikatora klienta (poprawny dla fazy 2) **1** adres IP w wersji 4 **2** pełna nazwa domeny **3** Pełna nazwa domeny użytkownika **4** podsieć IP w wersji 4 **7** zakres adresów IP w wersji 4 **9** nazwa wyróżniająca **11** identyfikator klucza
	1305	1691	Wartość identyfikatora klienta zdalnego.	Char(256)	Identyfikator klienta zdalnego (poprawny dla fazy 2)
	1561	1947	Protokół identyfikatora klienta zdalnego	Char(4)	Protokół identyfikatora klienta zdalnego (poprawny dla fazy 2)

Tabela 177. Pozycje kroniki JD (Zmiana opisu zadania). Zbiór opisów pól QASYJDJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Profil użytkownika podany dla parametru USER opisu zadania
157	225	611	Opis zadania	Char(10)	Nazwa opisu zadania, w którym został zmieniony parametr USER.
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki, w której znajduje się obiekt.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Typ komendy	Char(3)	Typ użytej komendy. **CHG** Komenda Zmiana opisu zadania (Change Job Description - CHGJOBD). **CRT** Komenda Tworzenie opisu zadania (Create Job Description - CRTJOBD).
188	256	642	Poprzedni użytkownik	Char(10)	Nazwa profilu użytkownika podanego dla parametru USER, zanim opis zadania został zmieniony.
198	266	652	Nowy użytkownik	Char(10)	Nazwa profilu podanego dla parametru USER, gdy opis zadania został zmieniony.
		662	Nazwa puli ASP	Char(10)	Nazwa puli ASP dla biblioteki JOBD
		672	Numer puli ASP	Char(5)	Numer puli ASP dla biblioteki JOBD

Tabela 178. Pozycje kroniki JS (Zmiana zadania). Zbiór opisów pól QASYJSJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.

Tabela 178. Pozycje kroniki JS (Zmiana zadania) (kontynuacja). Zbiór opisów pól QASYJSJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Komenda ENDJOBABN **B** Wprowadzenie **C** Zmiana **E** Zakończenie **H** Wstrzymanie **I** Odłączenie **M** Zmiana profilu lub profilu grupowego **N** Komenda ENDJOB **P** Podłączenie zadania prestartu lub natychmiastowego zadania wsadowego **Q** Zmiana atrybutów zapytania **R** Zwalnianie **S** Uruchomienie **T** Zmiana profilu lub profilu grupowego przy użyciu tokenu profilu. **U** Komenda CHGUSRTRC **V** Urządzenie wirtualne zmienione za pomocą funkcji API QWSACCDS.
157	225	611	Typ zadania	Char(1)	Typ zadania. **A** Autostartu **B** Wsadowe **I** Interaktywne **M** Monitorowania podsystemu **R** Program czytający **S** Systemowe **W** Program piszący **X** SCPF
158	226	612	Podtyp zadania	Char(1)	Podtyp zadania. **' '** Brak podtypu **D** Natychmiastowe wsadowe **E** Żądanie uruchomienia procedury **J** Prestartu **P** Sterownik drukarki **Q** Zapytanie **T** MRT **U** Alternatywny użytkownik buforu
159	227	613	Nazwa zadania	Char(10)	Pierwsza część pełnej nazwy zadania

Tabela 178. Pozycje kroniki JS (Zmiana zadania) (kontynuacja). Zbiór opisów pól QASYJSJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
169	237	623	Nazwa użytkownika zadania	Char(10)	Druga część pełnej nazwy zadania
179	247	633	Numer zadania	Char(6)	Trzecia część pełnej nazwy zadania
185	253	639	Nazwa urządzenia	Char(10)	Nazwa urządzenia.
195	263	649	Efektywny profil użytkownika[2]	Char(10)	Nazwa efektywnego profilu użytkownika dla wątku
205	273	659	Nazwa opisu zadania	Char(10)	Nazwa opisu zadania dla zadania
215	283	669	Biblioteka opisu zadania	Char(10)	Nazwa biblioteki dla opisu zadania
225	293	679	Nazwa kolejki zadań	Char(10)	Nazwa kolejki zadań dla zadania
235	303	689	Biblioteka kolejki zadań	Char(10)	Nazwa biblioteki dla kolejki zadań
245	313	699	Nazwa kolejki wyjściowej	Char(10)	Nazwa kolejki wyjściowej dla zadania
255	323	709	Biblioteka kolejki wyjściowej	Char(10)	Nazwa biblioteki dla kolejki wyjściowej
265	333	719	Drukarka	Char(10)	Nazwa drukarki dla zadania
275	343	729	Lista bibliotek[2]	Char(430)	Lista bibliotek dla zadania
705	773	1159	Nazwa efektywnego profilu grupowego[2]	Char(10)	Nazwa efektywnego profilu grupowego dla wątku
715	783	1169	Dodatkowe profile grupowe[2]	Char(150)	Nazwy dodatkowych profili grupowych dla wątku.
	933	1319	Opis JUID	Char(1)	Opisuje znaczenie pola JUID: **' '** Pole JUID zawiera wartość dla zadania. **C** Wywołano funkcję API usuwania zawartości JUID. Pole JUID zawiera nową wartość. **S** Wywołano funkcję API ustawienia zawartości JUID. Pole JUID zawiera nową wartość.
	934	1320	Pole JUID	Char(10)	Zawiera wartość JUID
	944	1330	Rzeczywisty profil użytkownika	Char(10)	Nazwa rzeczywistego profilu użytkownika dla wątku.
	954	1340	Zeskładowany profil użytkownika	Char(10)	Nazwa zeskładowanego profilu użytkownika dla wątku.
	964	1350	Rzeczywisty profil grupowy	Char(10)	Nazwa rzeczywistego profilu grupowego dla wątku.
	974	1360	Zeskładowany profil grupowy	Char(10)	Nazwa zeskładowanego profilu grupowego dla wątku.
	984	1370	Zmiana rzeczywistego użytkownika[3]	Char(1)	Rzeczywisty profil użytkownika został zmieniony. **Y** Tak **N** Nie
	985	1371	Zmiana użytkownika efektywnego[3]	Char(1)	Efektywny profil użytkownika został zmieniony. **Y** Tak **N** Nie

Tabela 178. Pozycje kroniki JS (Zmiana zadania) (kontynuacja). Zbiór opisów pól QASYJSJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	986	1372	Zmiana zeskładowanego użytkownika[3]	Char(1)	Zeskładowany profil użytkownika został zmieniony **Y** Tak **N** Nie
	987	1373	Zmiana rzeczywistej grupy[3]	Char(1)	Rzeczywisty profil grupowy został zmieniony. **Y** Tak **N** Nie
	988	1374	Zmiana grupy efektywnej[3]	Char(1)	Efektywny profil grupowy został zmieniony **Y** Tak **N** Nie
	989	1375	Zmiana zeskładowanej grupy[3]	Char(1)	Zeskładowy profil grupowy został zmieniony. **Y** Tak **N** Nie
	990	1376	Zmiana grup dodatkowych[3]	Char(1)	Dodatkowe profile grupowe zostały zmienione. **Y** Tak **N** Nie
	991	1377	Numer listy bibliotek[4]	Bin(4)	Liczba bibliotek w polu rozszerzenia listy bibliotek (pozycja 993).
	993	1379	Rozszerzenie listy bibliotek[4,5]	Char(2252)	Rozszerzenie listy bibliotek dla zadania.
		3631	Grupa bibliotecznych ASP	Char(10)	Grupa bibliotecznych ASP
		3641	Nazwa puli ASP	Char(10)	Nazwa puli ASP dla biblioteki JOBD
		3651	Numer puli ASP	Char(5)	Numer puli ASP dla biblioteki JOBD

1 To pole jest puste jeśli zadanie znajduje się w kolejce zadań i nie zostało uruchomione.

2 Gdy jedno z zadań wykonuje operację na innym zadaniu i generowany jest rekord kontroli JS, to pole będzie zawierało dane z wątku początkowego zadania, na którym wykonywana jest operacja. We wszystkich pozostałych przypadkach, pole będzie zawierało dane z wątku, który wykonał operację.

3 To pole jest używane tylko wtedy, gdy typ pozycji (pozycja 224) to M lub T.

4 To pole jest używane tylko wtedy, gdy liczba bibliotek na liście bibliotek przekracza liczbę podaną w polu na pozycji 343.

5 Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość danych w tym polu.

Tabela 179. Pozycje kroniki KF (Plik bazy kluczy). Zbiór opisów pól QASYKFJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505 i Tabela 153 na stronie 507.

Tabela 179. Pozycje kroniki KF (Plik bazy kluczy) (kontynuacja). Zbiór opisów pól QASYKFJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	224	610	Typ pozycji	Char(1)	Typ pozycji. **C** Operacja certyfikatu **K** Operacja pliku bazy kluczy **P** Niepoprawne hasło **T** Operacja użytkownika zaufanego
	225	611	Operacja certyfikatu	Char(3)	Rodzaj działania[4]. **ADK** Dodano certyfikat z kluczem prywatnym **ADD** Dodano certyfikat **REQ** Żądanie certyfikatu **SGN** Podpisanie certyfikatu
	228	614	Operacja pliku bazy kluczy	Char(3)	Rodzaj działania[5]. **ADD** Dodanie pary kluczy **DFT** Wyznaczenie pary kluczy jako domyślnej **EXP** Wyeksportowanie pary kluczy **IMP** Zaimportowanie pary kluczy **LST** Drukowanie etykiet pary kluczy do pliku **PWD** Zmiana hasła pliku bazy kluczy **RMV** Usunięcie pary kluczy **INF** Odtwarzanie informacji o parze kluczy **2DB** Przekształcenie pliku bazy kluczy do formatu bazy danych kluczy **2YR** Przekształcenie pliku bazy danych kluczy do pliku bazy kluczy
	231	617	Operacja użytkownika zaufanego	Char(3)	Rodzaj działania[6]. **TRS** Wyznaczenie pary kluczy jako użytkownika zaufanego **RMV** Usuwanie wyznaczenia użytkownika zaufanego **LST** Lista użytkowników zaufanych
	234	620	Zastrzeżone	Char(18)	
	252	638	Długość nazwy obiektu	Binary(4)	Długość nazwy pliku bazy kluczy
	254	640	Identyfikator CCSID nazwy obiektu	Binary(5)	Identyfikator CCSID nazwy pliku kluczy.
	258	644	Identyfikator kraju lub regionu nazwy obiektu	Char(2)	Identyfikator kraju lub regionu nazwy pliku kluczy.
	260	646	Identyfikator języka nazwy obiektu	Char(3)	Identyfikator języka nazwy pliku kluczy
	263	649	Zastrzeżone	Char(3)	

Tabela 179. Pozycje kroniki KF (Plik bazy kluczy) (kontynuacja). Zbiór opisów pól QASYKFJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	266	652	Identyfikator pliku nadrzędnego	Char(16)	Identyfikator pliku katalogu nadrzędnego kluczy.
	282	668	Identyfikator pliku obiektu	Char(16)	Nazwa pliku katalogu bazy kluczy.
	298	684	Nazwa obiektu	Char(512)	Nazwa pliku bazy kluczy.
	810	1196	Zastrzeżone	Char(18)	
	828	1214	Długość nazwy obiektu	Binary(4)	Długość nazwy zbioru źródłowego lub docelowego.
	830	1216	Identyfikator CCSID nazwy obiektu	Binary(5)	Identyfikator CCSID nazwy zbioru źródłowego lub docelowego.
	834	1220	Identyfikator kraju lub regionu nazwy obiektu	Char(2)	Identyfikator kraju lub regionu nazwy zbioru źródłowego lub docelowego.
	836	1222	Identyfikator języka nazwy obiektu	Char(3)	Identyfikator języka nazwy zbioru źródłowego lub docelowego.
	839	1225	Zastrzeżone	Char(3)	
	842	1228	Identyfikator pliku nadrzędnego	Char(16)	Identyfikator pliku katalogu nadrzędnego źródłowego lub docelowego.
	858	1244	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku katalogu źródłowego lub docelowego.
	874	1260	Nazwa obiektu	Char(512)	Nazwa zbioru źródłowego lub docelowego.
	1386	1772	Długość etykiety certyfikatu	Binary(4)	Długość etykiety certyfikatu.
	1388	1774	Etykieta certyfikatu[1]	Char(1026)	Etykieta certyfikatu.
	2414	2800	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku bazy kluczy.
	2430	2816	Nazwa puli ASP	Char(10)	Nazwa urządzenia puli ASP.
	2440	2826	Numer puli ASP	Char(5)	Numer urządzenia puli ASP.
	2445	2831	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	2449	2835	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	2451	2837	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	2454	2840	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.

Tabela 179. Pozycje kroniki KF (Plik bazy kluczy) (kontynuacja). Zbiór opisów pól QASYKFJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	2456	2842	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do pliku bazy kluczy. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełnej bezwzględnej nazwy ścieżki do pliku bazy kluczy.
	2457	2843	Identyfikator pliku o dostępie pośrednim[2]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	2473	2859	Bezwzględna nazwa ścieżki[1]	Char(5002)	Bezwzględna nazwa ścieżki do pliku bazy kluczy.
	7475	7861	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku zbioru docelowego lub źródłowego.
	7491	7877	Nazwa puli ASP	Char(10)	Nazwa puli ASP zbioru źródłowego lub docelowego
	7501	7887	Numer puli ASP	Char(5)	Numer puli ASP zbioru źródłowego lub docelowego
	7506	7892	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	7510	7896	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	7512	7898	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	7515	7901	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.
	7517	7903	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do zbioru źródłowego lub docelowego. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełnej bezwzględnej nazwy ścieżki do zbioru docelowego lub źródłowego.
	7518	7904	Identyfikator pliku o dostępie pośrednim[3]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	7534	7920	Bezwzględna nazwa ścieżki[1]	Char(5002)	Bezwzględna nazwa ścieżki zbioru źródłowego lub docelowego.

Tabela 179. Pozycje kroniki KF (Plik bazy kluczy) (kontynuacja). Zbiór opisów pól QASYKFJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**

[1] Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

[2] Gdy indykator nazwy ścieżki (pozycja 2456) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla bezwzględnej nazwy ścieżki z pozycji 2473. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

[3] Gdy indykator nazwy ścieżki (pozycja 7517) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla bezwzględnej nazwy ścieżki z pozycji 7534. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

[4] Jeśli nie jest to operacja certyfikatu, pole będzie puste.

[5] Jeśli nie jest to operacja pliku bazy kluczy, pole będzie puste.

[6] Jeśli nie jest to operacja użytkownika zaufanego, pole będzie puste.

Tabela 180. Pozycje kroniki LD (Dowiązanie, usunięcie dowiązania, wyszukiwanie katalogu). Zbiór opisów pól QASYLDJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **L** Dowiązanie katalogu **U** Usunięcie dowiązania katalogu **K** Wyszukiwanie katalogu
157			(Obszar zastrzeżony)	Char(20)	
	225	611	(Obszar zastrzeżony)	Char(18)	
	243	629	Długość nazwy obiektu [1]	Binary (4)	Długość nazwy obiektu.
177	245	631	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.
181	249	635	Identyfikator kraju lub regionu nazwy obiektu[1]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
183	251	637	Identyfikator języka nazwy obiektu[1]	Char(3)	Identyfikator języka dla nazwy obiektu.
186	254	640	(Obszar zastrzeżony)	Char(3)	
189	257	643	Identyfikator pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
205	273	659	Identyfikator pliku obiektu[1,2]	Char(16)	Identyfikator pliku obiektu.
221	289	675	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.

Tabela 180. Pozycje kroniki LD (Dowiązanie, usunięcie dowiązania, wyszukiwanie katalogu) (kontynuacja). Zbiór opisów pól QASYLDJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	801	1187	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	817	1203	Nazwa puli ASP	Char(10)	Nazwa urządzenia puli ASP.
	827	1213	Numer puli ASP	Char(5)	Numer urządzenia puli ASP.
	832	1218	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	836	1222	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	838	1224	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	841	1227	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.
	843	1229	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	844	1230	Identyfikator pliku o dostępie pośrednim[1]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	860	1246	Bezwzględna nazwa ścieżki[2]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

1 Gdy indykator nazwy ścieżki (pozycja 843) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla bezwzględnej nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

2 Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

Tabela 181. Pozycje kroniki ML (Działanie poczty). Zbiór opisów pól QASYMLJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **O** Otwarto protokół poczty
157	225	611	Profil użytkownika	Char(10)	Nazwa profilu użytkownika.
167	235	621	ID użytkownika	Char(8)	Identyfikator użytkownika
175	243	629	Adres	Char(8)	Adres użytkownika

Pozycje kroniki kontroli

Tabela 182. Pozycje kroniki NA (Zmiana atrybutu). Zbiór opisów pól QASYNAJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Zmiana atrybutu sieciowego. **T** Zmiana atrybutu TCP/IP.
157	225	611	Atrybut	Char(10)	Nazwa atrybutu.
167	235	621	Nowa wartość atrybutu	Char(250)	Wartość atrybutu po zmianie.
417	485	871	Poprzednia wartość atrybutu	Char(250)	Wartość atrybutu przed zmianą.

Tabela 183. ND (filtr przeszukiwania katalogów APPN), pozycje kroniki. Zbiór opisów pól QASYNDJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Naruszenie filtru przeszukiwania katalogów
157	225	611	Nazwa filtrowania punktu kontrolnego.	Char(8)	Nazwa filtrowania punktu kontrolnego.
165	233	619	NETID filtrowanego punktu kontrolnego.	Char(8)	NETID filtrowanego punktu kontrolnego.
173	241	627	Nazwa miejsca filtrowania CP	Char(8)	Nazwa miejsca filtrowania CP
181	249	635	NETID miejsca filtrowania CP	Char(8)	NETID miejsca filtrowania CP
189	257	643	Nazwa miejsca partnera	Char(8)	Nazwa miejsca partnera.
197	265	651	NETID miejsca partnera	Char(8)	NETID miejsca partnera.
205	273	659	Sesja przychodząca	Char(1)	Sesja przychodząca. **Y** To jest sesja przychodząca **N** To nie jest sesja przychodząca
206	274	660	Sesja wychodząca	Char(1)	Sesja wychodząca. **Y** To jest sesja wychodząca **N** To nie jest sesja wychodząca

Więcej informacji dotyczących filtru przeszukiwania katalogów APPN i punktów końcowych APPN znajduje się w temacie Centrum informacyjne (patrz “Informacje wstępne i pokrewne” na stronie xvi, aby uzyskać szczegółowe informacje).

Tabela 184. NE (filtr punktów końcowych APPN), pozycje kroniki. Zbiór opisów pól QASYNEJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Naruszenie filtru punktu końcowego
157	225	611	Nazwa lokalnego miejsca	Char(8)	Nazwa lokalnego miejsca.
165	233	619	Nazwa zdalnego miejsca	Char(8)	Nazwa zdalnego miejsca.
173	241	627	Zdalny NETID	Char(8)	Zdalny NETID.
181	249	635	Sesja przychodząca	Char(1)	Sesja przychodząca. **Y** To jest sesja przychodząca **N** To nie jest sesja przychodząca
182	250	636	Sesja wychodząca	Char(1)	Sesja wychodząca. **Y** To jest sesja wychodząca **N** To nie jest sesja wychodząca

Więcej informacji dotyczących filtru przeszukiwania katalogów APPN i punktów końcowych APPN znajduje się w temacie Centrum informacyjne (patrz “Informacje wstępne i pokrewne” na stronie xvi, aby uzyskać szczegółowe informacje).

Tabela 185. Pozycje kroniki OM (Zmiana zarządzania obiektami). Zbiór opisów pól QASYOMJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **M** Obiekt przeniesiono do innej biblioteki. **R** Zmieniono nazwę obiektu.
157	225	611	Poprzednia nazwa obiektu	Char(10)	Poprzednia nazwa obiektu.
167	235	621	Poprzednia nazwa biblioteki	Char(10)	Nazwa biblioteki, w której znajduje się obiekt z poprzednią nazwą.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Nowa nazwa obiektu	Char(10)	Nowa nazwa obiektu.
195	263	649	Nowa nazwa biblioteki	Char(10)	Nazwa biblioteki, do której obiekt został przeniesiony.
205	273	659	(Obszar zastrzeżony)	Char(20)	

Tabela 185. Pozycje kroniki OM (Zmiana zarządzania obiektami) (kontynuacja). Zbiór opisów pól QASYOMJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
225	293	679	Użytkownik biurowy	Char(10)	Nazwa użytkownika biurowego.
235	303	689	Poprzednia nazwa folderu lub dokumentu	Char(12)	Poprzednia nazwa folderu lub dokumentu
247	315	701	(Obszar zastrzeżony)	Char(8)	
255	323	709	Poprzednia ścieżka folderu	Char(63)	Poprzednia ścieżka folderu.
318	386	772	Nowa nazwa folderu lub dokumentu	Char(12)	Nowa nazwa folderu lub dokumentu.
330	398	784	(Obszar zastrzeżony)	Char(8)	
338	406	792	Nowa ścieżka folderu	Char(63)	Nowa ścieżka folderu.
401	469	855	Praca w imieniu użytkownika	Char(10)	Użytkownik pracujący w imieniu innego użytkownika.
411			(Obszar zastrzeżony)	Char(20)	
	479	865	(Obszar zastrzeżony)	Char(18)	
	497	883	Długość nazwy obiektu	Binary (4)	Długość pola poprzedniej nazwy obiektu.
431	499	885	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.
435	503	889	Identyfikator kraju lub regionu nazwy obiektu[1]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
437	505	891	Identyfikator języka nazwy obiektu[1]	Char(3)	Identyfikator języka dla nazwy obiektu.
440	508	894	(Obszar zastrzeżony)	Char(3)	
443	511	897	Identyfikator poprzedniego pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku poprzedniego katalogu nadrzędnego.
459	527	913	Identyfikator pliku poprzedniego obiektu[1,2]	Char(16)	Identyfikator pliku poprzedniego obiektu.
475	543	929	Nazwa poprzedniego obiektu[1]	Char(512)	Nazwa poprzedniego obiektu.
987	1055	1441	Identyfikator nowego pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku nowego katalogu nadrzędnego.
1003	1071	1457	Nowa nazwa obiektu[1,2,6]	Char(512)	Nowa nazwa obiektu.
	1583	1969	Identyfikator pliku obiektu[1,2]	Char(16)	Identyfikator pliku obiektu.
	1599	1985	Nazwa puli ASP[7]	Char(10)	Nazwa urządzenia puli ASP.

Tabela 185. Pozycje kroniki OM (Zmiana zarządzania obiektami) (kontynuacja). Zbiór opisów pól QASYOMJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1609	1995	Numer puli ASP [7]	Char(5)	Numer urządzenia puli ASP.
	1614	2000	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	1618	2004	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	1620	2006	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	1623	2009	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.
	1625	2011	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	1626	2012	Identyfikator pliku o dostępie pośrednim[3]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	1642	2028	Bezwzględna nazwa ścieżki[5]	Char(5002)	Poprzednia bezwzględna nazwa ścieżki do obiektu.
	6644	7030	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	6660	7046	Nazwa puli ASP [8]	Char(10)	Nazwa urządzenia puli ASP.
	6670	7056	Numer puli ASP [8]	Char(5)	Numer urządzenia puli ASP.
	6675	7061	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	6679	7065	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	6681	7067	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	6684	7070	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.
	6686	7072	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	6687	7073	Identyfikator pliku o dostępie pośrednim[4]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	6703	7089	Bezwzględna nazwa ścieżki[5]	Char(5002)	Nowa bezwzględna nazwa ścieżki do obiektu.

Tabela 185. Pozycje kroniki OM (Zmiana zarządzania obiektami) (kontynuacja). Zbiór opisów pól QASYOMJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**

[1] Te pola używane są tylko dla obiektów w systemach plików QOpenSys, "root" oraz użytkownika.

[2] Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

[3] Gdy indykator nazwy ścieżki (pozycja 1625) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla bezwzględnej nazwy ścieżki z pozycji 1642. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

[4] Gdy indykator nazwy ścieżki (pozycja 6686) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla bezwzględnej nazwy ścieżki z pozycji 6703. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

[5] Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

[6] Dla tej wartości nie istnieje pole długości. Łańcuch uzupełniany jest zerami (null) aż osiągnie długość 512 znaków.

[7] Jeśli poprzedni obiekt znajduje się w bibliotece, jest to informacja o puli ASP biblioteki obiektu. Jeśli poprzedni obiekt nie znajduje się w bibliotece, jest to informacja o puli ASP obiektu.

[8] Jeśli nowy obiekt znajduje się w bibliotece, jest to informacja o puli ASP biblioteki obiektu. Jeśli nowy obiekt nie znajduje się w bibliotece, jest to informacja o puli obiektu.

Tabela 186. Pozycje kroniki OR (Odtwarzanie obiektu). Zbiór opisów pól QASYORJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **N** W systemie został odtworzony nowy obiekt. **E** W systemie został odtworzony istniejący obiekt.
157	225	611	Nazwa odtworzonego obiektu	Char(10)	Nazwa odtworzonego obiektu.
167	235	621	Nazwa odtworzonej biblioteki	Char(10)	Nazwa biblioteki odtworzonego obiektu.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Nazwa obiektu składowania	Char(10)	Nazwa obiektu składowania.
195	263	649	Nazwa biblioteki składowania	Char(10)	Nazwa biblioteki, z której obiekt był składowany.
205	273	659	Stan programu [1]	Char(1)	**I** Odtworzony został program z atrybutem inherit-state. **Y** Odtworzony został program z atrybutem system-state. **N** Odtworzony został program z atrybutem user-state.

Tabela 186. Pozycje kroniki OR (Odtwarzanie obiektu) (kontynuacja). Zbiór opisów pól QASYORJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
206	274	660	Komenda systemu[2]	Char(1)	**Y** Odtworzona została komenda systemu. **N** Odtworzona została komenda z atrybutem user-state.
207			(Obszar zastrzeżony)	Char(18)	
	275	661	Tryb SETUID	Char(1)	Indykator trybu SETUID. **Y** Bit trybu SETUID dla odtworzonego obiektu jest ustawiony. **N** Bit trybu SETUID dla odtworzonego obiektu nie jest ustawiony.
	276	662	Tryb SETGID	Char(1)	Indykator trybu SETGID. **Y** Bit trybu SETGID dla odtworzonego obiektu jest ustawiony. **N** Bit trybu SETGID dla odtworzonego obiektu nie jest ustawiony.
	277	663	Status podpisu	Char(1)	Status podpisu odtworzonego obiektu. **B** Podpis nie miał formatu OS/400 **E** Podpis istnieje ale nie był sprawdzany **F** Podpis nie jest zgodny z zawartością obiektu **I** Podpis został zignorowany **N** Obiekt niepodpisywalny **S** Podpis jest poprawny **T** Podpis niezaufany **U** Obiekt nie jest podpisany
	278	664	Atrybut skanowania	Char(1)	Jeśli zbiór był obiektem zintegrowanego systemu plików, jest wartość atrybutu skanowania dla tego obiektu, gdzie **Y** *YES **N** *NO **C** *CHGONLY Opisy tych wartości zawiera opis komendy CHGATR.
	279	665	Zastrzeżone	Char(14)	
225	293	679	Użytkownik biurowy	Char(10)	Nazwa użytkownika biurowego.
235	303	689	Nazwa odtwarzanego obiektu DLO	Char(12)	Nazwa obiektu biblioteki dokumentów odtworzonego obiektu.
247	315	701	(Obszar zastrzeżony)	Char(8)	
255	323	709	Ścieżka folderu odtwarzania	Char(63)	Folder do którego odtworzony został obiekt DLO.

Tabela 186. Pozycje kroniki OR (Odtwarzanie obiektu) (kontynuacja). Zbiór opisów pól QASYORJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
318	386	772	Nazwa składowanego obiektu DLO	Char(12)	Nazwa DLO składowanego obiektu.
330	398	784	(Obszar zastrzeżony)	Char(8)	
338	406	792	Ścieżka folderu składowania	Char(63)	Folder z którego obiektu DLO był składowany.
401	469	855	Praca w imieniu użytkownika	Char(10)	Użytkownik pracujący w imieniu innego użytkownika.
411			(Obszar zastrzeżony)	Char(20)	
	479	865	(Obszar zastrzeżony)	Char(18)	
	497	883	Długość nazwy obiektu	Binary (4)	Długość pola poprzedniej nazwy obiektu.
431	499	885	Identyfikator CCSID nazwy obiektu[3]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.
435	503	889	Identyfikator kraju lub regionu nazwy obiektu[3]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
437	505	891	Identyfikator języka nazwy obiektu[3]	Char(3)	Identyfikator języka dla nazwy obiektu.
440	508	894	(Obszar zastrzeżony)	Char(3)	
443	511	897	Identyfikator pliku nadrzędnego[3,4]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
459	527	913	Identyfikator pliku obiektu[3,4]	Char(16)	Identyfikator pliku obiektu.
475	543	929	Nazwa obiektu [3]	Char(512)	Nazwa obiektu.
	1055	1441	Identyfikator poprzedniego pliku	Char(16)	Identyfikator pliku dla poprzedniego obiektu.
	1071	1457	Identyfikator pliku nośnika	Char(16)	Identyfikator składowany w pliku nośnika. **Uwaga:** Identyfikator pliku składowany na nośniku jest identyfikatorem, który obiekt ma w systemie źródłowym.
	1087	1473	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	1103	1489	Nazwa puli ASP[7]	Char(10)	Nazwa urządzenia puli ASP.
	1113	1499	Numer puli ASP [7]	Char(5)	Numer urządzenia puli ASP.
	1118	1504	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	1122	1508	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.

Tabela 186. Pozycje kroniki OR (Odtwarzanie obiektu) (kontynuacja). Zbiór opisów pól QASYORJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1124	1510	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	1127	1513	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.
	1129	1515	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	1130	1516	Identyfikator pliku o dostępie pośrednim[5]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	1146	1532	Bezwzględna nazwa ścieżki[6]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

1 To pole ma pozycję tylko wtedy, gdy odtwarzany obiekt to program.

2 To pole ma pozycję tylko wtedy, gdy odtwarzany obiekt to komenda.

3 Te pola używane są tylko dla obiektów w systemach plików QOpenSys i "root".

4 Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

5 Gdy indykator nazwy ścieżki (pozycja 1129) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla bezwzględnej nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

6 Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

7 Jeśli obiekt znajduje się w bibliotece, jest to informacja puli ASP biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja obiektu.

Tabela 187. Pozycje kroniki OW (Zmiana prawa własności). Zbiór opisów pól QASYOWJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Zmiana właściciela obiektu
157	225	611	Nazwa obiektu	Char(10)	Nazwa obiektu.
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki, w której znajduje się obiekt.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Poprzedni właściciel	Char(10)	Poprzedni właściciel obiektu.
195	263	649	Nowy właściciel	Char(10)	Nowy właściciel obiektu.
205	273	659	(Obszar zastrzeżony)	Char(20)	

Tabela 187. Pozycje kroniki OW (Zmiana prawa własności) (kontynuacja). Zbiór opisów pól QASYOWJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
225	293	679	Użytkownik biurowy	Char(10)	Nazwa użytkownika biurowego.
235	303	689	Nazwa DLO	Char(12)	Nazwa obiektu biblioteki dokumentów.
247	315	701	(Obszar zastrzeżony)	Char(8)	
255	323	709	Ścieżka folderu	Char(63)	Ścieżka do folderu.
318	386	772	Praca w imieniu użytkownika	Char(10)	Użytkownik pracujący w imieniu innego użytkownika.
328			(Obszar zastrzeżony)	Char(20)	
	396	782	(Obszar zastrzeżony)	Char(18)	
	414	800	Długość nazwy obiektu	Binary (4)	Długość nowej nazwy obiektu.
348	416	802	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.
352	420	806	Identyfikator kraju lub regionu nazwy obiektu[1]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
354	422	808	Identyfikator języka nazwy obiektu[1]	Char(3)	Identyfikator języka dla nazwy obiektu.
357	425	811	(Obszar zastrzeżony)	Char(3)	
360	428	814	Identyfikator pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
376	444	830	Identyfikator pliku obiektu[1,2]	Char(16)	Identyfikator pliku obiektu.
392	460	846	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	972	1358	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	988	1374	Nazwa puli ASP[5]	Char(10)	Nazwa urządzenia puli ASP.
	998	1384	Numer puli ASP[5]	Char(5)	Numer urządzenia puli ASP.
	1003	1389	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	1007	1393	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	1009	1395	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	1012	1398	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.

Tabela 187. Pozycje kroniki OW (Zmiana prawa własności) (kontynuacja). Zbiór opisów pól QASYOWJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1014	1400	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	1015	1401	Identyfikator pliku o dostępie pośrednim[3]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	1031	1417	Bezwzględna nazwa ścieżki[4]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

1 Te pola używane są tylko dla obiektów w systemach plików QOpenSys i "root".

2 Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

3 Gdy indykator nazwy ścieżki (pozycja 1014) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla bezwzględnej nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

4 Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

5 Jeśli obiekt znajduje się w bibliotece, jest to informacja puli ASP biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja obiektu.

Tabela 188. O1 (dostęp optyczny), pozycje kroniki. zbiór opisu pola QASY01JE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Odczyt (R-Read) Aktualizowanie (U-Update) Usunięcie (D-Delete) Tworzenie katalogu (C-Create Dir) Zwolnienie zawieszonego zbioru (X-Release Held File)
157	225	611	Typ obiektu	Char(1)	Zbiór (F-File) Zakończenie katalogu (D-Directory End) Pamięć (S-Storage)
158	226	612	Typ dostępu	Char(1)	Dane zbioru (D-File Data) Atrybuty katalogu zbioru (A-File Directory Attributes) Odtwarzanie (R-Restore operation) Składowanie (S-Save operation)
159	227	613	Nazwa urządzenia	Char(10)	Nazwa LUD biblioteki
169	237	623	Nazwa CSI	Char(8)	Nazwa obiektu pobocznego
177	245	631	Biblioteka CSI	Char(10)	Biblioteka obiektu pobocznego

Tabela 188. O1 (dostęp optyczny), pozycje kroniki (kontynuacja). zbiór opisu pola QASY01JE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
187	255	641	Nazwa woluminu	Char(32)	Nazwa woluminu optycznego
219	287	673	Nazwa obiektu	Char(256)	Nazwa zbioru/katalogu optycznego
		929	Nazwa puli ASP	Char(10)	Nazwa puli ASP dla biblioteki CSI
		939	Numer puli ASP	Char(5)	Numer puli ASP dla biblioteki CSI

Uwaga: Ta pozycja używana jest do kontrolowania następujących funkcji nośnika optycznego:

otwieranie zbioru lub katalogu,

Tworzenie katalogu (Create Directory)

usunięcie katalogu zbioru,

zmiana lub wczytanie atrybutów,

zwalnianie zawieszonego zbioru optycznego.

Tabela 189. O2 (dostęp optyczny), pozycje kroniki. zbiór opisu pola QASY02JE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Kopiowanie (C-Copy) Zmiana nazwy (R-Rename) Składowanie katalogu lub zbioru (B-Backup Dir or File) Składowanie zawieszonego zbioru (S-Save Held File) Przenoszenie zbioru (M-Move File)
157	225	611	Typ obiektu	Char(1)	Zbiór (F-File) Katalog (D-Directory)
158	226	612	Nazwa urządzenia źródłowego	Char(10)	Nazwa LUD biblioteki źródłowej
168	236	622	Nazwa źródłowego CSI	Char(8)	Nazwa źródłowego obiektu pobocznego
176	244	630	Źródłowa biblioteka CSI	Char(10)	Źródłowa biblioteka obiektu pobocznego
186	254	640	Nazwa woluminu źródłowego	Char(32)	Nazwa źródłowego woluminu optycznego
218	286	672	Nazwa obiektu źródłowego	Char(256)	Nazwa źródłowego zbioru/katalogu optycznego
474	542	928	Nazwa urządzenia docelowego	Char(10)	Nazwa LUD biblioteki docelowej
484	552	938	Nazwa docelowego CSI	Char(8)	Nazwa docelowego obiektu pobocznego
492	560	946	Docelowa biblioteka CSI	Char(10)	Docelowa biblioteka obiektu pobocznego

Tabela 189. O2 (dostęp optyczny), pozycje kroniki (kontynuacja). zbiór opisu pola QASY02JE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
502	570	956	Nazwa woluminu docelowego	Char(32)	Nazwa docelowego woluminu optycznego
534	602	988	Nazwa obiektu docelowego	Char(256)	Nazwa docelowego zbioru/katalogu optycznego
		1244	Nazwa puli ASP	Char(10)	Nazwa puli ASP dla źródłowej biblioteki CSI
		1254	Numer puli ASP	Char(5)	Numer puli ASP dla źródłowej biblioteki CSI
		1259	Nazwa puli ASP dla docelowej biblioteki CSI	Char(10)	Nazwa puli ASP dla docelowej biblioteki CSI
		1269	Numer puli ASP dla docelowej biblioteki CSI	Char(5)	Numer puli ASP dla docelowej biblioteki CSI

Tabela 190. O3 (dostęp optyczny), pozycje kroniki. zbiór opisu pola QASY03JE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Inicjowanie (I-Initialize) Zmiana nazwy (N-Rename) Składowanie woluminu (B-Backup Volume) Konwertowanie woluminu składowania na podstawowy (C-Convert Backup Volume to Primary) Importowanie (M-Import) Eksportowanie (E-Export) Zmiana uprawnień (L-Change Auth.) Sporządzenie listy (List) Zmiana atrybutów woluminu (A-Change Volume Attributes) Odczyt bezwzględny (R-Absolute Read)
157	225	611	Nazwa urządzenia	Char(10)	Nazwa LUD biblioteki
167	235	621	Nazwa CSI	Char(8)	Nazwa obiektu pobocznego
175	243	629	Biblioteka CSI	Char(10)	Biblioteka obiektu pobocznego
185	253	639	Poprzednia nazwa woluminu	Char(32)	Poprzednia nazwa woluminu optycznego
217	285	671	Nowa nazwa woluminu [1]	Char(32)	Nowa nazwa woluminu optycznego
249	317	703	Poprzednia lista autoryzacji [2]	Char(10)	Poprzednia lista autoryzacji

Tabela 190. O3 (dostęp optyczny), pozycje kroniki (kontynuacja). zbiór opisu pola QASY03JE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
259	327	713	Nowa lista autoryzacji [3]	Char(10)	Nowa lista autoryzacji
269	337	723	Adres [4]	Binary(5)	Blok początkowy
273	341	727	Długość [4]	Binary(5)	Odczytana długość
		731	Nazwa puli ASP	Char(10)	Nazwa puli ASP dla biblioteki CSI
		741	Numer puli ASP	Char(5)	Numer puli ASP dla biblioteki CSI

1 To pole zawiera nową nazwę woluminu dla funkcji inicjowania (Initialize), zmiany nazwy (Rename) i konwertowania (Convert); zawiera nazwę woluminu składowania dla funkcji Składowania (Backup). Zawiera nazwę woluminu dla funkcji importowania (Import), eksportowania (Export), zmiany listy autoryzacji (Change Authorization List), zmiany atrybutów woluminu (Change Volume Attributes) i odczytu sektora (Sector Read).

2 Używane tylko dla funkcji importowania (Import), eksportowania (Export) i zmiany listy autoryzacji (Change Authorization List).

3 Używane tylko dla funkcji zmiany listy autoryzacji (Change Authorization List).

4 Używane tylko dla funkcji odczytu sektora (Sector Read).

Tabela 191. Pozycje kroniki PA (adoptowanie programu). Zbiór opisów pól QASYPAJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Zmiana programu do adoptowania uprawnień właściciela. **J** Program w języku Java adoptuje uprawnienia właściciela. **M** Zmiana identyfikatora SETUID, SETGID obiektu albo wskaźnik trybu ograniczenia zmiany nazwy i usuwania dowiązania.
157	225	611	Nazwa programu[3]	Char(10)	Nazwa programu.
167	235	621	Biblioteka programu[3]	Char(10)	Nazwa biblioteki, w której znajduje się program.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Właściciel	Char(10)	Nazwa właściciela.
	263	649	Tryb IXVTX	Char(1)	Indykator trybu zmiany nazwy zastrzeżonej lub usunięcia dowiązania (ISVTX). **Y** Indykator trybu ISVTX jest włączony dla obiektu. **N** Indykator trybu ISVTX nie jest włączony dla obiektu.
	263	649	Zastrzeżone	Char(17)	
	281	667	Długość nazwy obiektu [1]	Binary (4)	Długość nazwy obiektu.

Tabela 191. Pozycje kroniki PA (adoptowanie programu) (kontynuacja). Zbiór opisów pól QASYPAJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	283	669	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.
	287	673	Identyfikator kraju lub regionu nazwy obiektu	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
	289	675	Identyfikator języka nazwy obiektu[1]	Char(3)	Identyfikator języka dla nazwy obiektu.
	292	678	Zastrzeżone	Char(3)	
	295	681	Identyfikator pliku nadrzędnego[1, 2, 3]	Char(16)	Identyfikator pliku nadrzędnego.
	311	697	Identyfikator pliku obiektu[3]	Char(16)	Identyfikator pliku dla obiektu
	327	713	Nazwa obiektu[1]	Char(512)	Nazwa obiektu dla obiektu.
	839	1225	Tryb SETUID	Char(1)	Indykator trybu ustawiania efektywnego identyfikatora użytkownika (Set effective user ID - SETUID). **Y** Bit trybu SETUID jest włączony dla obiektu. **N** Bit trybu SETUID nie jest włączony dla obiektu.
	840	1226	Tryb SETGID	Char(1)	Indykator trybu ustawiania efektywnego identyfikatora grupy (Set effective group ID - SETGID). **Y** Bit trybu SETGID jest włączony dla obiektu. **N** Bit trybu SETGID nie jest włączony dla obiektu.
	841	1227	Właściciel grupy podstawowej	Char(10)	Nazwa właściciela grupy podstawowej.
	851	1237	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	867	1253	Nazwa puli ASP[6]	Char(10)	Nazwa urządzenia puli ASP.
	877	1263	Numer puli ASP [6]	Char(5)	Numer urządzenia puli ASP.
	882	1268	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	886	1272	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	888	1274	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	891	1277	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.
	893	1279	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	894	1280	Identyfikator pliku o dostępie pośrednim[4]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	910	1296	Bezwzględna nazwa ścieżki[5]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

Tabela 191. Pozycje kroniki PA (adoptowanie programu) (kontynuacja). Zbiór opisów pól QASYPAJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**

[1] Te pola używane są tylko dla obiektów w systemach plików QOpenSys i "root".

[2] Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

[3] Gdy typ pozycji to ″J″, pola nazwy programu i nazwy biblioteki będą zawierały wartość ″*N″. Ponadto pola identyfikatora zbioru nadrzędnego oraz identyfikatora zbioru obiektu będą zawierały zera binarne.

[4] Gdy indykator nazwy ścieżki (pozycja 893) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla bezwzględnej nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

[5] Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

[6] Jeśli obiekt znajduje się w bibliotece, jest to informacja puli ASP biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja obiektu.

Tabela 192. Pozycje kroniki PG (Zmiana grupy podstawowej). Zbiór opisów pól QASYPGJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Zmiana grupy podstawowej.
157	225	611	Nazwa obiektu	Char(10)	Nazwa obiektu.
167	235	621	Biblioteka obiektu	Char(10)	Nazwa biblioteki, w której znajduje się obiekt.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Poprzednia grupa podstawowa	Char(10)	Poprzednia grupa podstawowa dla obiektu.[5]
195	263	649	Nowa grupa podstawowa	Char(10)	Nowa grupa podstawowa dla obiektu.
					Uprawnienia dla nowej grupy podstawowej:
205	273	659	Istnienie obiektu	Char(1)	**Y** *OBJEXIST
206	274	660	Zarządzanie obiektami	Char(1)	**Y** *OBJMGT
207	275	661	Operacyjne do obiektu	Char(1)	**Y** *OBJOPR
208	276	662	Zmiana obiektu	Char(1)	**Y** *OBJALTER
209	277	663	Odniesienie do obiektu	Char(1)	**Y** *OBJREF
210	278	664	(Obszar zastrzeżony)	Char(10)	
220	288	674	Zarządzanie listą autoryzacji	Char(1)	**Y** *AUTLMGT
221	289	675	Uprawnienie do odczytu	Char(1)	**Y** *READ
222	290	676	Uprawnienie do dodawania	Char(1)	**Y** *ADD
223	291	677	Uprawnienie do aktualizacji	Char(1)	**Y** *UPD

Tabela 192. Pozycje kroniki PG (Zmiana grupy podstawowej) (kontynuacja). Zbiór opisów pól QASYPGJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
224	292	678	Uprawnienie do usuwania	Char(1)	**Y** *DLT
225	293	679	Uprawnienie do uruchamiania	Char(1)	**Y** *EXECUTE
226	294	680	(Obszar zastrzeżony)	Char(10)	
236	304	690	Uprawnienie na wyłączność	Char(1)	**Y** *EXCLUDE
237	305	691	Odebranie poprzedniej grupy podstawowej	Char(1)	**Y** Odebranie uprawnień dla poprzedniej grupy podstawowej. **' '** Nieodbieranie uprawnień dla poprzedniej grupy podstawowej.
238	306	692	(Obszar zastrzeżony)	Char (20)	
258	326	712	Użytkownik biurowy	Char(10)	Nazwa użytkownika biurowego.
268	336	722	Nazwa DLO	Char(12)	Nazwa obiektu biblioteki dokumentów lub folderu.
280	348	734	(Obszar zastrzeżony)	Char(8)	
288	356	742	Ścieżka folderu	Char(63)	Ścieżka do folderu.
351	419	805	Praca w imieniu użytkownika	Char(10)	Użytkownik pracujący w imieniu innego użytkownika.
361			(Obszar zastrzeżony)	Char(20)	
	429	815	(Obszar zastrzeżony)	Char(18)	
	447	833	Długość nazwy obiektu [1]	Binary (4)	Długość nazwy obiektu.
381	449	835	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.
385	453	839	Identyfikator kraju lub regionu nazwy obiektu[1]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
387	455	841	Identyfikator języka nazwy obiektu[1]	Char(3)	Identyfikator języka dla nazwy obiektu.
390	458	844	(Obszar zastrzeżony)	Char(3)	
393	461	847	Identyfikator pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
409	477	863	Identyfikator pliku obiektu[1,2]	Char(16)	Identyfikator pliku obiektu.
425	493	879	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	1005	1391	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
		1407	Nazwa puli ASP[6]	Char(10)	Nazwa urządzenia puli ASP.
		1417	Numer puli ASP [6]	Char(5)	Numer urządzenia puli ASP.
	1035	1422	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.

Tabela 192. Pozycje kroniki PG (Zmiana grupy podstawowej) (kontynuacja). Zbiór opisów pól QASYPGJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1040	1426	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	1042	1428	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	1045	1431	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.
	1047	1433	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	1048	1434	Identyfikator pliku o dostępie pośrednim[3]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	1064	1450	Bezwzględna nazwa ścieżki[4]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

1 Te pola używane są tylko dla obiektów w systemach plików QOpenSys i "root".

2 Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

3 Gdy indykator nazwy ścieżki (pozycja 1047) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla bezwzględnej nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

4 Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

5 Wartość *N oznacza, że wartość pola Poprzednia grupa podstawowa nie była dostępna.

6 Jeśli obiekt znajduje się w bibliotece, jest to informacja puli ASP biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja obiektu.

Tabela 193. Pozycje kroniki PO (Zbiór wydruku). Zbiór opisów pól QASYPOJE/J4/J5

Pozycja (Offset)					
JE	**`J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ wydruku	Char(1)	Typ wydruku. **D** Drukowanie bezpośrednie **R** Wysłanie do systemu zdalnego do drukowania **S** Drukowanie za pośrednictwem zbioru buforowego
157	225	611	Status po drukowaniu	Char(1)	**D** Usunięto po wydrukowaniu **H** Wstrzymano po wydrukowaniu **S** Zeskładowano po wydrukowaniu **' '** Drukowanie bezpośrednie

Tabela 193. Pozycje kroniki PO (Zbiór wydruku) (kontynuacja). Zbiór opisów pól QASYPOJE/J4/J5

Pozycja (Offset)					
JE	**`J4**	**J5**	**Pole**	**Format**	**Opis**
158	226	612	Nazwa zadania	Char(10)	Pierwsza część pełnej nazwy zadania.
168	236	622	Nazwa użytkownika zadania	Char(10)	Druga część pełnej nazwy zadania.
178	246	632	Numer zadania	Zoned(6,0)	Trzecia część pełnej nazwy zadania.
184	252	638	Profil użytkownika	Char(10)	Profil użytkownika, który utworzył wydruk.
194	262	648	Kolejka wyjściowa	Char(10)	Kolejka wyjściowa zawierająca zbiór buforowy[1].
204	272	658	Nazwa biblioteki kolejki wyjściowej	Char(10)	Nazwa biblioteki zawierającej kolejkę wyjściową.[1]
214	282	668	Nazwa urządzenia	Char(10)	Urządzenie, na którym drukowano[2].
224	292	678	Typ urządzenia	Char(4)	Typ drukarki[2].
228	296	682	Model urządzenia	Char(4)	Model drukarki[2].
232	300	686	Nazwa zbioru urządzenia	Char(10)	Nazwa zbioru urządzenia użytego przy dostępie do drukarki.
242	310	696	Biblioteka zbioru urządzenia	Char(10)	Nazwa biblioteki dla zbioru urządzenia.
252	320	706	Nazwa zbioru buforowego	Char(10)	Nazwa zbioru buforowego[1]
262	330	716	Krótki numer zbioru buforowego	Char(4)	Numer zbioru buforowego[1]. Jeśli jest zbyt długi, pole będzie puste.
266	334	720	Typ formularza	Char(10)	Typ formularza zbioru buforowego.
276	344	730	Dane użytkowników	Char(10)	Dane użytkownika związane ze zbiorem buforowym[1].
286			(Obszar zastrzeżony)	Char(20)	
	354	740	Numer zbioru buforowego	Char(6)	Numer zbioru buforowego.
	360	746	Obszar zastrzeżony	Char(14)	
306	374	760	System zdalny	Char(255)	Nazwa systemu zdalnego, do którego wysłany został wydruk.
561	629	1015	Kolejka wydruków systemu zdalnego	Char(128)	Nazwa kolejki wyjściowej w systemie zdalnym.
	757	1143	Nazwa systemu zadania zbioru buforowego	Char(8)	Nazwa systemu, w którym znajduje się zbiór buforowy.
	765	1151	Data utworzenia zbioru buforowego	Char (7)	Data utworzenia zbioru buforowego (CYYMMDD)
	772	1158	Godzina utworzenia zbioru buforowego	Char(6)	Godzina utworzenia zbioru buforowego (HHMMSS).

Tabela 193. Pozycje kroniki PO (Zbiór wydruku) (kontynuacja). Zbiór opisów pól QASYPOJE/J4/J5

Pozycja (Offset)					
JE	**`J4**	**J5**	**Pole**	**Format**	**Opis**
		1164	Nazwa puli ASP	Char(10)	Nazwa puli ASP dla biblioteki urządzenia
		1174	Numer puli ASP	Char(5)	Numer puli ASP dla biblioteki zbioru urządzenia
		1179	Nazwa puli ASP kolejki wyjściowej	Char(10)	Nazwa puli ASP dla biblioteki kolejki wyjściowej.
		1189	Numer puli ASP kolejki wyjściowej	Char(5)	Numer puli ASP dla biblioteki kolejki wyjściowej.

1 To pole jest puste, jeśli typem wydruku jest drukowanie bezpośrednie.

2 To pole jest puste, jeśli typem wydruku jest drukowanie zdalne.

Tabela 194. Pozycje kroniki PS (Przełączanie profilu). Zbiór opisów pól QASYPSJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Przełączanie profilu podczas tranzytu. **E** Zakończenie pracy w imieniu relacji. **H** Uchwyt profilu wygenerowany przez funkcję API QSYGETPH. **I** Wszystkie znaczniki profilu zostały unieważnione. **M** Wygenerowano maksymalną liczbę znaczników profilu. **P** Wygenerowano znacznik profilu dla użytkownika. **R** Wszystkie znaczniki profilu dla użytkownika zostały usunięte. **S** Rozpoczęcie pracy w imieniu relacji. **V** Profil użytkownika został uwierzytelniony.
157	225	611	Profil użytkownika	Char(10)	Nazwa profilu użytkownika.
167	235	621	Miejsce źródłowe	Char(8)	Miejsce źródłowe tranzytu.
175	243	629	Profil użytkownika początkowego miejsca docelowego	Char(10)	Profil użytkownika początkowego miejsca docelowego tranzytu.
185	253	639	Profil użytkownika nowego miejsca docelowego	Char(10)	Profil użytkownika nowego miejsca docelowego tranzytu.

Tabela 194. Pozycje kroniki PS (Przełączanie profilu) (kontynuacja). Zbiór opisów pól QASYPSJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
195	263	649	Użytkownik biurowy	Char(10)	Użytkownik biurowy uruchamiający lub kończący pracę w imieniu relacji.
205	273	659	W imieniu użytkownika	Char(10)	Użytkownik, w którego imieniu pracuje użytkownik biurowy.
215	283	669	Typ znacznika profilu	Char(1)	Typ znacznika profilu, który został wygenerowany. **M** znacznik profilu do wielokrotnego użycia **R** Regenerowany znacznik profilu do wielokrotnego użycia **S** znacznik profilu do jednokrotnego użycia
216	284	670	Limit czasu znacznika profilu	Binary(4)	Liczba sekund, przez które znacznik profilu jest poprawny.

Tabela 195. Pozycje kroniki PW (Hasło). Zbiór opisów pól QASYPWJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji naruszenia	Char(1)	Typ naruszenia **A** Konsolidacja APPC nie powiodła się. **D** Nazwa identyfikatora użytkownika narzędzi serwisowych nie jest poprawna. **E** Hasło identyfikatora użytkownika narzędzi serwisowych nie jest poprawne. **P** Hasło nie jest poprawne. **S** Hasło szyfrowania SQL nie jest poprawne. **U** Nazwa użytkownika jest niepoprawna **X** Identyfikator użytkownika narzędzi serwisowych jest zablokowany. **Y** Identyfikator użytkownika narzędzi serwisowych nie jest poprawny. **Z** Hasło identyfikatora użytkownika narzędzi serwisowych nie jest poprawne.
157	225	611	Nazwa użytkownika	Char(10)	Nazwa użytkownika zadania lub nazwa identyfikatora użytkownika narzędzi serwisowych.
167	235	621	Nazwa urządzenia	Char(40)	Nazwa urządzenia lub urządzenia komunikacyjnego, na którym wprowadzono hasło lub identyfikator użytkownika. Jeśli typ pozycji to X, Y lub Z, to pole będzie zawierało nazwę narzędzia serwisowego.
207	275	661	Nazwa zdalnego miejsca	Char(8)	Nazwa zdalnego miejsca dla konsolidowania APPC.
215	283	669	Nazwa miejsca lokalnego	Char(8)	Nazwa miejsca lokalnego dla konsolidowania APPC.
223	291	677	ID sieci	Char(8)	ID sieci dla konsolidowania APPC.

Tabela 195. Pozycje kroniki PW (Hasło) (kontynuacja). Zbiór opisów pól QASYPWJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
		685[2]	Nazwa obiektu	Char(10)	Nazwa deszyfrowanego obiektu.
		695	Biblioteka obiektu	Char(10)	Biblioteka dla deszyfrowanego obiektu.
		705	Typ obiektu	Char(8)	Typ deszyfrowanego obiektu.
		713	Nazwa puli ASP[1]	Char(10)	Nazwa urządzenia puli ASP.
		723	Numer puli ASP[1]	Char(5)	Numer urządzenia puli ASP.

1 Jeśli obiekt znajduje się w bibliotece, jest to informacja o puli ASP dla biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja o puli ASP dla obiektu.

2 Jeśli nazwa obiektu ma wartość *N a typ naruszenia to S, użytkownik próbował deszyfrować dane w zmiennej języka bazowego.

Tabela 196. Pozycje kroniki RA (Zmiana uprawnień dla odtworzonego obiektu). Zbiór opisów pól QASYRAJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Zmiany w uprawnieniach dla odtworzonego zbioru
157	225	611	Nazwa obiektu	Char(10)	Nazwa obiektu.
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki, w której znajduje się obiekt.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Nazwa listy autoryzacji	Char(10)	Nazwa listy autoryzacji.
195	263	649	Uprawnienia publiczne	Char(1)	**Y** Uprawnienia publiczne ustawione na *EXCLUDE.
196	264	650	Uprawnienia prywatne	Char(1)	**Y** Usunięto uprawnienia prywatne.
197	265	651	Usunięto AUTL	Char(1)	**Y** Lista autoryzacji została usunięta z obiektu.
198	266	652	(Obszar zastrzeżony)	Char(20)	
218	286	672	Nazwa DLO	Char(12)	Nazwa obiektu biblioteki dokumentów.
230	298	684	(Obszar zastrzeżony)	Char(8)	
238	306	692	Ścieżka folderu	Char(63)	Folder zawierający obiekt biblioteki dokumentów.
301			(Obszar zastrzeżony)	Char(20)	
	369	755	(Obszar zastrzeżony)	Char(18)	
	387	773	Długość nazwy obiektu	Binary(4)	Długość nazwy obiektu.
321	389	775	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.

Tabela 196. Pozycje kroniki RA (Zmiana uprawnień dla odtworzonego obiektu) (kontynuacja). Zbiór opisów pól QASYRAJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
325	393	779	Identyfikator kraju lub regionu nazwy obiektu[1]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
327	395	781	Identyfikator języka nazwy obiektu[1]	Char(3)	Identyfikator języka dla nazwy obiektu.
330	398	784	(Obszar zastrzeżony)	Char(3)	
333	401	787	Identyfikator pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
349	417	803	Identyfikator pliku obiektu[1,2]	Char(16)	Identyfikator pliku obiektu.
365	433	819	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	945	1331	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	961	1347	Nazwa puli ASP[5]	Char(10)	Nazwa urządzenia puli ASP.
	971	1357	Numer puli ASP[5]	Char(5)	Numer urządzenia puli ASP.
	976	1362	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	980	1366	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	982	1368	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	985	1371	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.
	987	1373	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	988	1374	Identyfikator pliku o dostępie pośrednim[3]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	1004	1390	Bezwzględna nazwa ścieżki[4]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

Tabela 196. Pozycje kroniki RA (Zmiana uprawnień dla odtworzonego obiektu) (kontynuacja). Zbiór opisów pól QASYRAJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**

[1] Te pola używane są tylko dla obiektów w systemach plików QOpenSys i "root".

[2] Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

[3] Gdy indykator nazwy ścieżki (pozycja 987) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla bezwzględnej nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

[4] Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

[5] Jeśli obiekt znajduje się w bibliotece, jest to informacja puli ASP biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja obiektu.

Tabela 197. Pozycje kroniki RJ (Odtwarzanie opisu zadania). Zbiór opisów pól QASYRJJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Odtwarzanie opisu zadania, który w parametrze USER miał podany profil użytkownika.
157	225	611	Nazwa opisu zadania	Char(10)	Nazwa odtworzonego opisu zadania.
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki, do której został odtworzony opis zadania.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Nazwa użytkownika	Char(10)	Nazwa profilu użytkownika podana w opisie zadania.
		649	Nazwa puli ASP	Char(10)	Nazwa puli ASP dla biblioteki JOBD
		659	Numer puli ASP	Char(5)	Numer puli ASP dla biblioteki JOBD

Tabela 198. Pozycje kroniki RO (Zmiana prawa własności do odtworzonego obiektu). Zbiór opisów pól QASYROJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Odtwarzanie obiektów, które podczas odtwarzania miały zmienione prawa własności
157	225	611	Nazwa obiektu	Char(10)	Nazwa obiektu.
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki, w której znajduje się obiekt.

Tabela 198. Pozycje kroniki RO (Zmiana prawa własności do odtworzonego obiektu) (kontynuacja). Zbiór opisów pól QASYROJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Poprzedni właściciel	Char(10)	Nazwa właściciela przed zmianą prawa własności.
195	263	649	Nowy właściciel	Char(10)	Nazwa właściciela po zmianie prawa własności.
205	273	659	(Obszar zastrzeżony)	Char(20)	
225	293	679	Nazwa DLO	Char(12)	Nazwa obiektu biblioteki dokumentów.
237	305	691	(Obszar zastrzeżony)	Char(8)	
245	313	699	Ścieżka folderu	Char(63)	Folder, do którego został odtworzony obiekt.
308			(Obszar zastrzeżony)	Char(20)	
	376	762	(Obszar zastrzeżony)	Char(18)	
	394	780	Długość nazwy obiektu [1]	Binary(4)	Długość nazwy obiektu.
328	396	782	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.
332	400	786	Identyfikator kraju lub regionu nazwy obiektu[1]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
334	402	788	Identyfikator języka nazwy obiektu[1]	Char(3)	Identyfikator języka dla nazwy obiektu.
337	405	791	(Obszar zastrzeżony)	Char(3)	
340	408	794	Identyfikator pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
356	424	810	Identyfikator pliku obiektu[1,2]	Char(16)	Identyfikator pliku obiektu.
372	440	826	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	952	1338	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	968	1354	Nazwa puli ASP [5]	Char(10)	Nazwa urządzenia puli ASP.
	978	1364	Numer puli ASP [5]	Char(5)	Numer urządzenia puli ASP.
	983	1369	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	987	1373	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	989	1375	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	992	1378	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.

Tabela 198. Pozycje kroniki RO (Zmiana prawa własności do odtworzonego obiektu) (kontynuacja). Zbiór opisów pól QASYROJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	994	1380	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	995	1381	Identyfikator pliku o dostępie pośrednim[3]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	1011	1397	Bezwzględna nazwa ścieżki[4]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

1 Te pola używane są tylko dla obiektów w systemach plików QOpenSys i "root".

2 Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

3 Gdy indykator nazwy ścieżki (pozycja 994) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla bezwzględnej nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

4 Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

5 Jeśli obiekt znajduje się w bibliotece, jest to informacja puli ASP biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja obiektu.

Tabela 199. Pozycje kroniki RP (Odtwarzanie programów adoptujących uprawnienia). Zbiór opisów pól QASYRPJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Odtwarzanie programów adoptujących uprawnienia właściciela
157	225	611	Nazwa programu	Char(10)	Nazwa programu.
167	235	621	Biblioteka programu	Char(10)	Nazwa biblioteki, w której znajduje się program.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Nazwa właściciela	Char(10)	Nazwa właściciela.
	263	649	(Obszar zastrzeżony)	Char(18)	
	281	667	Długość nazwy obiektu [1]	Binary (4)	Długość nazwy obiektu.
	283	669	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	Identyfikator kodowanego zestawu znaków dla nazwy obiektu.
	287	673	Identyfikator kraju lub regionu nazwy obiektu[1]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.

Tabela 199. Pozycje kroniki RP (Odtwarzanie programów adoptujących uprawnienia) (kontynuacja). Zbiór opisów pól QASYRPJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	289	675	Identyfikator języka nazwy obiektu[1]	Char(3)	Identyfikator języka dla nazwy obiektu.
	292	678	(Obszar zastrzeżony)	Char(3)	
	295	681	Identyfikator pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
	311	697	Identyfikator pliku obiektu[1,2]	Char(16)	Identyfikator pliku obiektu.
	327	713	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	839	1225	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	855	1241	Nazwa puli ASP [5]	Char(10)	Nazwa urządzenia puli ASP.
	865	1251	Numer puli ASP [5]	Char(5)	Numer urządzenia puli ASP.
	870	1256	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	874	1260	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	876	1262	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	879	1265	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.
	881	1267	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	882	1268	Identyfikator pliku o dostępie pośrednim[3]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	898	1284	Bezwzględna nazwa ścieżki[4]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

1 Te pola używane są tylko dla obiektów w systemach plików QOpenSys i 'root'.

2 Jeśli identyfikator ma ustawiony ostatni lewy bit i resztę bitów zerowych oznacza to, że identyfikator **nie** jest ustawiony.

3 Gdy indykator nazwy ścieżki (pozycja 994) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla bezwzględnej nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

4 Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

5 Jeśli obiekt znajduje się w bibliotece, jest to informacja puli ASP biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja obiektu.

Pozycje kroniki kontroli

Tabela 200. Pozycje kroniki RQ (Odtwarzanie obiektu deskryptora żądania zmiany). Zbiór opisów pól QASYRQJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Odtworzenie obiektu *CRQD adoptującego uprawnienia.
157	225	611	Nazwa obiektu	Char(10)	Nazwa deskryptora żądania zmiany.
167	235	621	Biblioteka obiektu	Char(10)	Nazwa biblioteki, w której znajduje się deskryptor żądania zmiany.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
		639	Nazwa puli ASP	Char(10)	Nazwa puli ASP dla biblioteki obiektu CRQD
		649	Numer puli ASP	Char(5)	Numer puli ASP dla biblioteki obiektu CRQD

Tabela 201. Pozycje kroniki RU (Odtwarzanie uprawnień dla profilu użytkownika). Zbiór opisów pól QASYRUJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Odtwarzanie uprawnień dla profilu użytkownika
157	225	611	Nazwa użytkownika	Char(10)	Nazwa profilu użytkownika, którego uprawnienia zostały odtworzone.
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
	253	639	Odtworzone uprawnienia	Char(1)	Wskazuje, czy dla użytkownika zostały odtworzone wszystkie uprawnienia. **A** Wszystkie uprawnienia zostały odtworzone **S** Niektóre uprawnienia nie zostały odtworzone

Tabela 202. Pozycje kroniki RZ (Zmiana grupy podstawowej dla odtworzonego obiektu). Zbiór opisów pól QASYRZJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Grupa podstawowa została zmieniona.
157	225	611	Nazwa obiektu	Char(10)	Nazwa obiektu.
167	235	621	Biblioteka obiektu	Char(10)	Nazwa biblioteki, w której znajduje się obiekt.

Tabela 202. Pozycje kroniki RZ (Zmiana grupy podstawowej dla odtworzonego obiektu) (kontynuacja). Zbiór opisów pól QASYRZJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Poprzednia grupa podstawowa	Char(10)	Poprzednia grupa podstawowa dla obiektu.
195	263	649	Nowa grupa podstawowa	Char(10)	Nowa grupa podstawowa dla obiektu.
205	273	659	(Obszar zastrzeżony)	Char(20)	
225	293	679	Nazwa DLO	Char(12)	Nazwa obiektu biblioteki dokumentów.
237	305	691	(Obszar zastrzeżony)	Char(8)	
245	313	699	Ścieżka folderu	Char(63)	Folder, do którego został odtworzony obiekt.
308			(Obszar zastrzeżony)	Char(20)	
	376	762	(Obszar zastrzeżony)	Char(18)	
	394	780	Długość nazwy obiektu [1]	Binary(4)	Długość nazwy obiektu.
328	396	782	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.
332	400	786	Identyfikator kraju lub regionu nazwy obiektu[1]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
334	402	788	Identyfikator języka nazwy obiektu[1]	Char(3)	Identyfikator języka dla nazwy obiektu.
337	405	791	(Obszar zastrzeżony)	Char(3)	
340	408	794	Identyfikator pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
356	424	810	Identyfikator pliku obiektu[1,2]	Char(16)	Identyfikator pliku obiektu.
372	440	826	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	952	1338	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	968	1354	Nazwa puli ASP	Char(10)	Nazwa urządzenia puli ASP.
	978	1364	Numer puli ASP	Char(5)	Numer urządzenia puli ASP.
	983	1369	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	987	1373	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	989	1375	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	992	1378	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.

Tabela 202. Pozycje kroniki RZ (Zmiana grupy podstawowej dla odtworzonego obiektu) (kontynuacja). Zbiór opisów pól QASYRZJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	994	1380	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	995	1381	Identyfikator pliku o dostępie pośrednim[3]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	1011	1397	Bezwzględna nazwa ścieżki[4]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

1 Te pola używane są tylko dla obiektów w systemach plików QOpenSys i "root".

2 Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

3 Gdy indykator nazwy ścieżki (pozycja 1014) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla bezwzględnej nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

4 Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

Tabela 203. Pozycje kroniki SD (Zmiana katalogu dystrybucyjnego systemu). Zbiór opisów pól QASYSDJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **S** Zmiana katalogu systemu
157	225	611	Rodzaj zmiany	Char(3)	**ADD** Dodanie pozycji katalogu **CHG** Zmiana pozycji katalogu **COL** Pozycja kolektora **DSP** Wyświetlenie pozycji katalogu **OUT** Żądanie zbioru wyjściowego **PRT** Drukowanie pozycji katalogu **RMV** Usuwanie pozycji katalogu **RNM** Zmiana nazwy pozycji katalogu **RTV** Odtworzenie szczegółów **SUP** Pozycja dostawcy

Tabela 203. Pozycje kroniki SD (Zmiana katalogu dystrybucyjnego systemu) (kontynuacja). Zbiór opisów pól QASYSDJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
160	228	614	Typ rekordu	Char(4)	**DIRE** Katalog **DPTD** Szczegóły wydziału **SHDW** Cień katalogu **SRCH** Wyszukiwanie katalogu
164	232	618	System początkowy	Char(8)	System, który inicjuje zmianę
172	240	626	Profil użytkownika	Char(10)	Profil użytkownika wprowadzającego zmianę
182	250	636	System żądający	Char(8)	System żądający zmiany
190	258	644	Żądana funkcja	Char(6)	**INIT** Inicjowanie **OFFLIN** Inicjowanie offline **REINIT** Ponowne inicjowanie **SHADOW** Zwykłe tworzenie cienia **STPSHD** Zatrzymanie tworzenia cienia
196	264	650	ID użytkownika	Char(8)	Zmieniony identyfikator użytkownika
204	272	658	Adres	Char(8)	Zmieniony adres
212	280	666	Identyfikator użytkownika sieci	Char(47)	Zmieniony identyfikator użytkownika sieci

Tabela 204. Pozycje kroniki SE (Zmiana pozycji routingu podsystemu). Zbiór opisów pól QASYSEJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Zmieniono pozycje routingu podsystemu
157	225	611	Nazwa podsystemu	Char(10)	Nazwa obiektu
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki, w której znajduje się obiekt
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Nazwa programu	Char(10)	Nazwa programu, który zmienił pozycję routingu
195	263	649	Nazwa biblioteki	Char(10)	Nazwa biblioteki dla programu
205	273	659	Numer kolejny	Char(4)	Numer kolejny
209	277	663	Nazwa komendy	Char(3)	Typ użytej komendy **ADD** ADDRTGE **CHG** CHGRTGE **RMV** RMVRTGE

Tabela 204. Pozycje kroniki SE (Zmiana pozycji routingu podsystemu) (kontynuacja). Zbiór opisów pól QASYSEJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
		666	Nazwa puli ASP dla biblioteki SBSD	Char(10)	Nazwa puli ASP dla biblioteki SBSD
		676	Numer puli ASP dla biblioteki SBSD	Char(5)	Numer puli ASP dla biblioteki SBSD
		681	Nazwa puli ASP dla biblioteki programu	Char(10)	Nazwa puli ASP dla biblioteki programu
		691	Numer puli ASP dla biblioteki programu	Char(5)	Numer puli ASP dla biblioteki programu

Tabela 205. Pozycje kroniki SF (Działanie na zbiorze buforowym). Zbiór opisów pól QASYSFJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ dostępu	Char(1)	Typ pozycji **A** Odczytanie zbioru buforowego. **C** Utworzenie zbioru buforowego. **D** Usunięcie zbioru buforowego. **H** Wstrzymanie zbioru buforowego. **I** Tworzenie zbioru wstawianego. **R** Zwolnienie zbioru buforowego. **U** Zmiana zbioru buforowego związanego z ochroną. **V** Zmiana atrybutów tylko zbioru buforowego niezwiązanego z ochroną.
157	225	611	Nazwa zbioru bazy danych	Char(10)	Nazwa zbioru bazy danych zawierającego zbiór buforowy
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki dla zbioru bazy danych
177	245	631	Typ obiektu	Char(8)	Typ obiektu zbioru bazy danych
185	253	639	Obszar zastrzeżony	Char(10)	
195	263	649	Nazwa podzbioru	Char(10)	Nazwa podzbioru.
205	273	659	Nazwa zbioru buforowego	Char(10)	Nazwa zbioru buforowego[1].
215	283	669	Krótki numer zbioru buforowego	Char(4)	Numer zbioru buforowego[1]. Jeśli numer zbioru buforowego jest większy niż 4 bajty, to pole będzie puste i zostanie użyte pole Numer zbioru buforowego (J5 pozycja 693).
219	287	673	Nazwa kolejki wyjściowej	Char(10)	Nazwa kolejki wyjściowej zawierającej zbiór buforowy.

Tabela 205. Pozycje kroniki SF (Działanie na zbiorze buforowym) (kontynuacja). Zbiór opisów pól QASYSFJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
229	297	683	Biblioteka kolejki wyjściowej	Char(10)	Nazwa biblioteki dla kolejki wyjściowej.
239			Obszar zastrzeżony	Char(20)	
	307	693	Numer zbioru buforowego	Char(6)	Numer zbioru buforowego.
	313	699	Obszar zastrzeżony	Char(14)	
259	327	713	Poprzednie kopie	Char(3)	Liczba poprzednich kopii zbioru buforowego
262	330	716	Nowe kopie	Char(3)	Liczba nowych kopii zbioru buforowego
265	333	719	Poprzednia drukarka	Char(10)	Poprzednia drukarka dla zbioru buforowego
275	343	729	Nowa drukarka	Char(10)	Nowa drukarka dla zbioru buforowego
285	353	739	Nowa kolejka wyjściowa	Char(10)	Nowa kolejka wyjściowa dla zbioru buforowego
295	363	749	Biblioteka nowej kolejki wyjściowej	Char(10)	Biblioteka dla nowej kolejki wyjściowej
305	373	759	Poprzedni typ formularza	Char(10)	Poprzedni typ formularza zbioru buforowego
315	383	769	Nowy typ formularza	Char(10)	Nowy typ formularza zbioru buforowego
325	393	779	Poprzednia strona restartu	Char(8)	Poprzednia strona restartu dla zbioru buforowego
333	401	787	Nowa strona restartu	Char(8)	Nowa strona restartu dla zbioru buforowego
341	409	795	Początek poprzedniego zakresu stron	Char(8)	Początek poprzedniego zakresu stron dla zbioru buforowego
349	417	803	Początek nowego zakresu stron	Char(8)	Początek nowego zakresu stron dla zbioru buforowego
357	425	811	Koniec poprzedniego zakresu stron	Char(8)	Koniec poprzedniego zakresu stron dla zbioru buforowego
365	433	819	Koniec nowego zakresu stron	Char(8)	Koniec nowego zakresu stron dla zbioru buforowego
	441	827	Nazwa zadania zbioru buforowego	Char(10)	Nazwa zadania zbioru buforowego.
	451	837	Użytkownik zadania zbioru buforowego	Char(10)	Użytkownik dla zadania zbioru buforowego.
	461	847	Numer zadania zbioru buforowego	Char(6)	Numer dla zadania zbioru buforowego.
	467	853	Poprzedni pojemnik	Char(8)	Poprzedni pojemnik źródłowy.
	475	861	Nowy pojemnik	Char(8)	Nowy pojemnik źródłowy.
	483	869	Nazwa poprzedniej definicji strony	Char(10)	Nazwa poprzedniej definicji strony.
	493	879	Biblioteka poprzedniej definicji strony	Char(10)	Nazwa biblioteki poprzedniej definicji strony.
	503	889	Nazwa nowej definicji strony	Char(10)	Nazwa nowej definicji strony.
	513	899	Biblioteka nowej definicji strony	Char(10)	Biblioteka nowej definicji strony.

Tabela 205. Pozycje kroniki SF (Działanie na zbiorze buforowym) (kontynuacja). Zbiór opisów pól QASYSFJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	523	909	Nazwa poprzedniej definicji formularza	Char(10)	Nazwa poprzedniej definicji formularza.
	533	919	Biblioteka poprzedniej definicji formularza	Char(10)	Nazwa biblioteki poprzedniej definicji formularza.
	543	929	Nazwa nowej definicji formularza	Char(10)	Nazwa nowej definicji formularza
	553	939	Biblioteka nowej definicji formularza	Char(10)	Nazwa biblioteki nowej definicji formularza.
	563	949	Poprzednia opcja 1 użytkownika	Char(10)	Poprzednia opcja 1 użytkownika.
	573	959	Poprzednia opcja 2 użytkownika	Char(10)	Poprzednia opcja 2 użytkownika.
	583	969	Poprzednia opcja 3 użytkownika	Char(10)	Poprzednia opcja 3 użytkownika.
	593	979	Poprzednia opcja 4 użytkownika	Char(10)	Poprzednia opcja 4 użytkownika.
	603	989	Nowa opcja 1 użytkownika	Char(10)	Nowa opcja 1 użytkownika.
	613	999	Nowa opcja 2 użytkownika	Char(10)	Nowa opcja 2 użytkownika.
	623	1009	Nowa opcja 3 użytkownika	Char(10)	Nowa opcja 3 użytkownika.
	633	1019	Nowa opcja 4 użytkownika	Char(10)	Nowa opcja 4 użytkownika.
	643	1029	Poprzedni obiekt użytkownika	Char(10)	Nazwa poprzedniego obiektu użytkownika.
	653	1039	Biblioteka poprzedniego obiektu użytkownika	Char(10)	Nazwa biblioteki poprzedniego obiektu użytkownika.
	663	1049	Typ poprzedniego obiektu użytkownika	Char(10)	Typ poprzedniego obiektu użytkownika.
	673	1059	Nowy obiekt użytkownika	Char(10)	Nowy obiekt użytkownika.
	683	1069	Biblioteka nowego obiektu użytkownika	Char(10)	Nazwa biblioteki nowego obiektu użytkownika.
	693	1079	Typ nowego obiektu użytkownika	Char(10)	Typ nowego obiektu użytkownika.
	703	1089	Nazwa systemu zadania zbioru buforowego	Char(8)	Nazwa systemu, w którym znajduje się zbiór buforowy.
	711	1097	Data utworzenia zbioru buforowego	Char (7)	Data utworzenia zbioru buforowego (CYYMMDD).

Tabela 205. Pozycje kroniki SF (Działanie na zbiorze buforowym) (kontynuacja). Zbiór opisów pól QASYSFJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	718	1104	Godzina utworzenia zbioru buforowego	Char(6)	Godzina utworzenia zbioru buforowego (HHMMSS).
		1110	Nazwa poprzednich danych użytkownika	Char(255)	Nazwa poprzednich danych użytkownika
		1365	Nazwa nowych danych użytkownika	Char(255)	Nazwa nowych danych użytkownika
		1620	Nazwa puli ASP zbioru	Char(10)	Nazwa puli ASP dla biblioteki zbioru bazy danych.
		1630	Numer puli ASP zbioru	Char(5)	Numer puli ASP dla biblioteki zbioru bazy danych.
		1635	Nazwa puli ASP kolejki wyjściowej	Char(10)	Nazwa puli ASP dla biblioteki kolejki wyjściowej.
		1645	Numer puli ASP kolejki wyjściowej	Char(5)	Numer puli ASP dla biblioteki kolejki wyjściowej.
		1650	Nazwa puli ASP nowej kolejki wyjściowej	Char(10)	Nazwa puli ASP dla biblioteki nowej kolejki wyjściowej.
		1660	Numer puli ASP nowej kolejki wyjściowej	Char(5)	Numer puli ASP dla biblioteki nowej kolejki wyjściowej.

[1] Gdy typ pozycji to I (drukowanie wstawiane), wtedy to pole jest puste.

Tabela 206. Pozycje kroniki SG (Sygnały asynchroniczne). Zbiór opisów pól QASYSGJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505 i Tabela 153 na stronie 507.
	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Przetworzono asynchroniczny sygnał iSeries **P** Przetworzono asynchroniczny sygnał środowiska PASE
	225	611	Numer sygnału	Char(4)	Numer przetworzonego sygnału.
	229	615	Działanie uchwytu	Char(1)	Działanie podjęte dla tego sygnału. **C** Kontynuowanie procesu **E** Wyjątek sygnału **H** Obsługa przez wywołanie funkcji przechwytywania sygnału **S** Zatrzymanie przetwarzania **T** Koniec prztewarzania **U** Koniec żądania

Tabela 206. Pozycje kroniki SG (Sygnały asynchroniczne) (kontynuacja). Zbiór opisów pól QASYSGJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	230	616	Źródło sygnału	Char(1)	Źródło sygnału. **M** Komputer **P** Proces **Uwaga:** Jeśli wartością źródła sygnału jest komputer, wartości zadania źródłowego są puste.
	231	617	Nazwa zadania źródłowego	Char(10)	Pierwsza część pełnej nazwy zadania źródłowego.
	241	627	Nazwa użytkownika zadania źródłowego	Char(10)	Druga część pełnej nazwy zadania źródłowego.
	251	637	Numer zadania źródłowego	Char(6)	Trzecia część pełnej nazwy zadania źródłowego.
	257	643	Bieżący użytkownik zadania źródłowego	Char(10)	Bieżący profil użytkownika dla zadania źródłowego.
	267	653	Datownik generacji	Char(8)	Format *DTS godziny, o której został wygenerowany sygnał. **Uwaga:** Funkcji API QWCCVTDT można użyć do przekształcenia datownika *DTS na inne formaty.

Tabela 207. Pozycje kroniki SK (Połączenia SSL). Zbiór opisów pól QASYSKJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505 i Tabela 153 na stronie 507.
	224	610	Typ pozycji	Char(1)	**A** Akceptowanie **C** Połączenie **D** Przypisano adres DHCP **F** Przefiltrowano pocztę **P** Port jest niedostępny **R** Odrzucenie poczty **U** Nie przypisano adresu DHCP
	225	611	Lokalny adres IP[3]	Char(15)	Lokalny adres IP.
	240	626	Port lokalny	Char(5)	Port lokalny.
	245	631	Zdalny adres IP[3]	Char(15)	Zdalny adres IP.
	260	646	Port zdalny	Char(5)	Port zdalny.
	265	651	Deskryptor gniazda	Bin(5)	Deskryptor gniazda.
	269	655	Opis filtru	Char(10)	Podany filtr poczty.
	279	665	Długość danych filtru	Bin(4)	Długość danych filtru.
	281	667	Dane filtru[1]	Char(514)	Dane filtru.

Tabela 207. Pozycje kroniki SK (Połączenia SSL) (kontynuacja). Zbiór opisów pól QASYSKJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	795	1181	Rodzina adresów	Char(10)	Rodzina adresów. ***IPV4** Protokół Internet Protocol wersja 4 ***IPV6** Protokół Internet Protocol wersja 6
	805	1191	Lokalny adres IP	Char(46)	Lokalny adres IP.
	851	1237	Zdalny adres IP[2]	Char(46)	Zdalny adres IP.
	897	1283	Adres MAC	Char(32)	Adres MAC klienta żądającego.
	929	1315	Nazwa hosta	Char(255)	Nazwa hosta klienta żądającego.

[1] Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość pola.

[2] Gdy typ pozycji to D, pole zawiera adres IP serwera DHCP przypisanego do klienta żądającego.

[3] Te pola obsługują jedynie adresy IPv4.

Tabela 208. SM (zmiana zarządzania systemami), pozycje kroniki. Zbiór opisów pól QASYSMJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Zwracana funkcja **B** Listę składowania została zmieniona **C** Opcje automatycznego czyszczenia **D** DRDA **F** System plików HFS **N** Operacja pliku sieciowego **O** Opcje składowania zostały zmienione **P** Harmonogram włączania/wyłączania zasilania **S** Lista odpowiedzi systemowych **T** Czasy odtworzania ścieżek dostępu zostały zmienione
157	225	611	Typ dostępu	Char(1)	**A** Dodanie **C** Zmiana **D** Usunięcie **R** Usuwanie **S** Wyświetlanie **T** Odtworzenie lub pobranie
158	226	612	Numer kolejny	Char(4)	Numer kolejny działania
162	230	616	ID komunikatu	Char (7)	ID komunikatu związanego z działaniem
169	237	623	Nazwa relacyjnej bazy danych	Char(18)	Nazwa relacyjnej bazy danych

Tabela 208. SM (zmiana zarządzania systemami), pozycje kroniki (kontynuacja). Zbiór opisów pól QASYSMJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
187	255	641	Nazwa systemu plików	Char(10)	Nazwa systemu plików
197	265	651	Opcja składowania została zmieniona	Char(10)	Opcja składowania została zmieniona
207	275	661	Lista składowania została zmieniona	Char(10)	Nazwa listy składowania, która została zmieniona
217	285	671	Nazwa zbioru sieciowego	Char(10)	Nazwa zbioru sieciowego, który został użyty
227	295	681	Podzbiór zbioru sieciowego	Char(10)	Nazwa podzbioru zbioru sieciowego
237	305	691	Numer zbioru sieciowego	Zoned(6,0)	Numer zbioru sieciowego
243	311	697	Właściciel zbioru sieciowego	Char(10)	Nazwa profilu użytkownika, który jest właścicielem zbioru sieciowego
253	321	707	Początkowy użytkownik zbioru sieciowego	Char(8)	Nazwa profilu użytkownika będącego źródłowym dla zbioru sieciowego
261	329	715	Źródłowy adres zbioru sieciowego	Char(8)	Adres będący źródłowym dla zbioru sieciowego

Tabela 209. Pozycje kroniki SO (Działania na informacjach o użytkowniku dotyczących ochrony serwera). Zbiór opisów pól QASYSOJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji **A** Dodanie pozycji **C** Zmiana pozycji **R** Usuwanie pozycji **T** Odtwarzanie pozycji
157	225	611	Profil użytkownika	Char(10)	Nazwa profilu użytkownika.
	235	621	Typ pozycji informacji o użytkowniku	Char(1)	**N** Typu pozycji nie podano. **U** Pozycja jest pozycją informacji o aplikacji użytkownika. **Y** Pozycja jest pozycją uwierzytelniania serwera.

Tabela 209. Pozycje kroniki SO (Działania na informacjach o użytkowniku dotyczących ochrony serwera) (kontynuacja). Zbiór opisów pól QASYSOJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	236	622	Przechowywanie hasła	Char(1)	**N** Hasło nie jest przechowywane **S** Brak zmiany **Y** Hasło jest przechowywane.
	237	623	Nazwa serwera	Char(200)	Nazwa serwera.
	437	823	(Obszar zastrzeżony)	Char(3)	
	440	826	Długość identyfikatora użytkownika	Binary (4)	Długość identyfikatora użytkownika.
	442	828	(Obszar zastrzeżony)	Char(20)	
	462	848	ID użytkownika	Char(1002)[1]	Identyfikator użytkownika.

[1] Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość pola.

Tabela 210. Pozycje kroniki ST (Działanie narzędzi serwisowych). Zbiór opisów pól QASYSTJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji **A** Rekord usługi

Tabela 210. Pozycje kroniki ST (Działanie narzędzi serwisowych) (kontynuacja). Zbiór opisów pól QASYSTJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
157	225	611	Narzędzie serwisowe	Char(2)	Typ pozycji. **AN** ANZJVM **CS** STRCPYSCN **CD** QTACTLDV **CE** QWTCTLTR **CT** DMPCLUTRC **DC** DLTCMNTRC **DD** DMPDLO **DJ** DMPJVM **DO** DMPOBJ **DS** DMPSYSOBJ, QTADMPTS **EC** ENDCMNTRC **ER** ENDRMTSPT **HD** QYHCHCOP (DASD) **HL** QYHCHCOP (LPAR) **JW** QPYRTJWA **PC** PRTCMNTRC **PE** PRTERRLOG **PI** PRTINTDTA **PS** QP0FPTOS **SE** QWTSETTR **SC** STRCMNTRC **SJ** STRSRVJOB **SR** STRRMTSPT **ST** STRSST **TA** TRCTCPAPP **TC** TRCCNN (podano *FORMAT) **TE** ENDTRC, ENDPEX **TI** TRCINT lub TRCCNN (podano *ON, *OFF lub *END) **TS** STRTRC, STRPEX
159	227	613	Nazwa obiektu	Char(10)	Nazwa obiektu, do którego uzyskano dostęp
169	237	623	Nazwa biblioteki	Char(10)	Nazwa biblioteki dla obiektu
179	247	633	Typ obiektu	Char(8)	Typ obiektu
187	255	641	Nazwa zadania	Char(10)	Pierwsza część pełnej nazwy zadania
197	265	651	Nazwa użytkownika zadania	Char(10)	Druga część pełnej nazwy zadania
207	275	661	Numer zadania	Zoned(6,0)	Trzecia część pełnej nazwy zadania

Tabela 210. Pozycje kroniki ST (Działanie narzędzi serwisowych) (kontynuacja). Zbiór opisów pól QASYSTJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
213	281	667	Nazwa obiektu	Char(30)	Nazwa obiektu dla komendy DMPSYSOBJ
243	311	697	Nazwa biblioteki	Char(30)	Nazwa biblioteki dla obiektu dla komendy DMPSYSOBJ
273	341	727	Typ obiektu	Char(8)	Typ obiektu
281	349	735	Nazwa DLO	Char(12)	Nazwa obiektu biblioteki dokumentów.
293	361	747	(Obszar zastrzeżony)	Char(8)	
301	369	755	Ścieżka folderu	Char(63)	Folder zawierający obiekt biblioteki dokumentów
	432	818	Pole JUID	Char(10)	JUID zadania docelowego.
	442	828	Działanie wczesnego śledzenia[1]	Char(10)	Działanie żądane dla wczesnego śledzenia zadania ***ON** Wczesne śledzenie zostało włączone ***OFF** Wczesne śledzenie zostało wyłączone ***RESET** Wczesne śledzenie zostało wyłączone a informacje o śledzeniu usunięte
	452	838	Opcja śledzenia aplikacji[2]	Char(1)	Opcja śledzenia podana w komendzie TRCTCPAPP. **Y** Zbieranie danych śledzenia zostało uruchomione **N** Zbieranie danych śledzenia zostało zatrzymane, a informacje śledzenia zostały zapisane do zbioru buforowego **E** Zbieranie danych śledzenia zostało zakończone, a wszystkie informacje śledzenia usunięte (nie utworzono danych wyjściowych)
	453	839	Śledzona aplikacja[2]	Char(10)	Nazwa śledzonej aplikacji.
	463	849	Profil narzędzi serwisowych[3]	Char(10)	Nazwa profilu narzędzi serwisowych użytego dla komendy STRSST.
		859	Identyfikator węzła źródłowego	Char(8)	Identyfikator węzła źródłowego
		867	Użytkownik źródłowy	Char(10)	Użytkownik źródłowy
		877	Nazwa puli ASP dla biblioteki obiektu	Char(10)	Nazwa puli ASP dla biblioteki obiektu
		887	Numer puli ASP dla biblioteki obiektu	Char(5)	Numer puli ASP dla biblioteki obiektu
		892	Nazwa puli ASP dla biblioteki obiektu komendy DMPSYSOBJ	Char(10)	Nazwa puli ASP dla biblioteki obiektu komendy DMPSYSOBJ
		902	Numer puli ASP dla biblioteki obiektu komendy DMPSYSOBJ	Char(5)	Numer puli ASP dla biblioteki obiektu komendy DMPSYSOBJ

[1] To pole jest używane tylko wtedy, gdy typem pozycji (pozycja 225) jest CE.

[2] To pole jest używane tylko wtedy, gdy typem pozycji (pozycja 225) jest TA.

[3] To pole używane jest tylko gdy typ pozycji (pozycja 225) to ST.

Tabela 211. Pozycje kroniki SV (Działanie dla wartości systemowej). Zbiór opisów pól QASYSVJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Zmiana wartości systemowych **B** Zmiana atrybutów usługi **C** Zmiana zegara systemowego
157	225	611	Wartość systemowa lub atrybut usługi	Char(10)	Nazwa wartości systemowej lub atrybut usługi
167	235	621	Nowa wartość	Char(250)	Wartość na jaką zmieniono wartość systemową lub atrybut usługi
417	485	871	Poprzednia wartość	Char(250)	Wartość atrybutu usługi lub wartości systemowej przed zmianą
667	735	1121	Nowa wartość kontynuowana	Char(250)	Kontynuacja wartości, na jaką zmieniono wartość systemową lub atrybut usługi.
917	985	1371	Poprzednia wartość kontynuowana	Char(250)	Kontynuacja zmienionej wartości dla wartości systemowej lub atrybutu usługi.

Tabela 212. Pozycje kroniki VA (Zmiana listy kontroli dostępu). Zbiór opisów pól QASYVAJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Status	Char(1)	Status żądania. **S** Pomyślne **F** Niepomyślne
157	225	611	Nazwa serwera	Char(10)	Nazwa opisu serwera sieciowego, który zarejestrował zdarzenie.
167	235	621	Data serwera	Char(6)	Data zaprotokołowania zdarzenia na serwerze sieciowym.
173	241	627	Godzina serwera	Zoned(6,0)	Godzina zaprotokołowania zdarzenia na serwerze sieciowym.
179	247	633	Nazwa komputera	Char(8)	Nazwa komputera wywołującego żądanie zmiany listy kontroli dostępu.
187	255	641	Nazwa requestera	Char(10)	Nazwa użytkownika wywołującego żądanie.
197	265	651	Wykonywane działanie	Char(1)	Działanie wykonywane na profilu kontroli dostępu: **A** Dodanie **C** Modyfikowanie **D** Usuwanie
198	266	652	Nazwa zasobu	Char(260)	Nazwa zasobu, który ma być zmieniony.

Tabela 213. Pozycje kroniki VC (Uruchomienie i zakończenie połączenia). Zbiór opisów pól QASYVCJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Działanie połączenia	Char(1)	Działanie połączenia, które nastąpiło. **S** Uruchomienie **E** Zakończenie **R** Odrzucenie
157	225	611	Nazwa serwera	Char(10)	Nazwa opisu serwera sieciowego, który zarejestrował zdarzenie.
167	235	621	Data serwera	Char(6)	Data zaprotokołowania zdarzenia na serwerze sieciowym.
173	241	627	Godzina serwera	Zoned(6,0)	Godzina zaprotokołowania zdarzenia na serwerze sieciowym.
179	247	633	Nazwa komputera	Char(8)	Nazwa komputera związanego z żądaniem połączenia.
187	255	641	Użytkownik połączenia	Char(10)	Nazwa użytkownika związanego z żądaniem połączenia.
197	265	651	Identyfikator połączenia	Char(5)	Identyfikator uruchomienia lub zakończenia połączenia.
202	270	656	Przyczyna odrzucenia	Char(1)	Przyczyna, dla której połączenie zostało odrzucone: **A** Odłączenie automatyczne (przekroczenie limitu czasu), zasób współużytkowany został usunięty lub brak uprawnień administracyjnych **E** Błąd, odłączenie sesji lub niepoprawne hasło **N** Zwykłe odłączenie lub limit użytkowników **P** Brak uprawnienia do zasobów współużytkowanych
203	271	657	Nazwa sieci	Char(12)	Nazwa sieci związana z połączeniem.

Tabela 214. Pozycje kroniki VF (Zamknięcie plików serwera). Zbiór opisów pól QASYVFJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Przyczyna zamknięcia	Char(1)	Przyczyna zamknięcia zbioru. **A** Odłączenie administracyjne **N** Zwykłe odłączenie klienta **S** Odłączenie sesji
157	225	611	Nazwa serwera	Char(10)	Nazwa opisu serwera sieciowego, który zarejestrował zdarzenie.
167	235	621	Data serwera	Char(6)	Data zaprotokołowania zdarzenia na serwerze sieciowym.

Tabela 214. Pozycje kroniki VF (Zamknięcie plików serwera) (kontynuacja). Zbiór opisów pól QASYVFJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
173	241	627	Godzina serwera	Zoned(6,0)	Godzina zaprotokołowania zdarzenia na serwerze sieciowym.
179	247	633	Nazwa komputera	Char(8)	Nazwa komputera żądającego zamknięcia.
187	255	641	Użytkownik połączenia	Char(10)	Nazwa użytkownika żądającego zamknięcia.
197	265	651	Identyfikator zbioru	Char(5)	Identyfikator zamykanego zbioru.
202	270	656	Przedział czasu	Char(6)	Liczba sekund, przez które zbiór był otwarty.
208	276	662	Nazwa zasobu	Char(260)	Nazwa zasobu, który jest właścicielem danego zbioru.

Tabela 215. Pozycje kroniki VL (Przekroczenie limitu konta). Zbiór opisów pól QASYVLJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Przyczyna	Char(1)	Przyczyna przekroczenia limitu. **A** Utrata ważności konta **D** Wyłączenie konta **L** Przekroczenie godziny logowania **U** Nieznana lub niedostępna **W** Niepoprawna stacja robocza
157	225	611	Nazwa serwera	Char(10)	Nazwa opisu serwera sieciowego, który zarejestrował zdarzenie.
167	235	621	Data serwera	Char(6)	Data zaprotokołowania zdarzenia na serwerze sieciowym.
173	241	627	Godzina serwera	Zoned(6,0)	Godzina zaprotokołowania zdarzenia na serwerze sieciowym.
179	247	633	Nazwa komputera	Char(8)	Nazwa komputera z naruszeniem limitu konta.
187	255	641	Użytkownik	Char(10)	Nazwa użytkownika z naruszeniem limitu konta.
197	265	651	Nazwa zasobu	Char(260)	Nazwa użytego zasobu.

Tabela 216. Pozycje kroniki VN (Logowanie i wylogowanie z sieci). Zbiór opisów pól QASYVNJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ logowania	Char(1)	Typ zdarzenia, które wystąpiło: **F** Żądanie wylogowania **O** Żądanie logowania **R** Logowanie odrzucono

Tabela 216. Pozycje kroniki VN (Logowanie i wylogowanie z sieci) (kontynuacja). Zbiór opisów pól QASYVNJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
157	225	611	Nazwa serwera	Char(10)	Nazwa opisu serwera sieciowego, który zarejestrował zdarzenie.
167	235	621	Data serwera	Char(6)	Data zaprotokołowania zdarzenia na serwerze sieciowym.
173	241	627	Godzina serwera	Zoned(6,0)	Godzina zaprotokołowania zdarzenia na serwerze sieciowym.
179	247	633	Nazwa komputera	Char(8)	Nazwa komputera dla zdarzenia.
187	255	641	Użytkownik	Char(10)	Użytkownik, który się zalogował lub wylogował.
197	265	651	Uprawnienia użytkownika	Char(1)	Uprawnienia logującego się użytkownika: **A** Administrator **G** Gość **U** Użytkownik
198	266	652	Przyczyna odrzucenia	Char(1)	Przyczyna, dla której logowanie zostało odrzucone: **A** Odmowa dostępu **F** Odłączenie wymuszone z powodu limitu logowania **P** Niepoprawne hasło
199	267	653	Dodatkowa przyczyna	Char(1)	Szczegóły odmowy dostępu: **A** Utrata ważności konta **D** Wyłączenie konta **L** Niepoprawne godziny logowania **R** Niepoprawny identyfikator requestera **U** Nieznana lub niedostępna

Tabela 217. Pozycje kroniki VO (Lista weryfikacji). Zbiór opisów pól QASYVOJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505 i Tabela 153 na stronie 507.
	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Dodanie pozycji listy weryfikacji **C** Zmiana pozycji listy weryfikacji **F** Szukanie pozycji listy weryfikacji **R** Usunięcie pozycji listy weryfikacji **U** Sprawdzanie pozycji listy weryfikacji nie powiodło się **V** Pomyślne sprawdzenie pozycji listy weryfikacji

Tabela 217. Pozycje kroniki VO (Lista weryfikacji) (kontynuacja). Zbiór opisów pól QASYVOJ4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	225	611	Rodzaj niepowodzenia	Char(1)	Rodzaj niepowodzenia sprawdzania. **E** Zaszyfrowane dane są niepoprawne **I** Nie odnaleziono identyfikatora pozycji **V** Nie odnaleziono listy weryfikacji
	226	612	Lista weryfikacji	Char(10)	Nazwa listy weryfikacji.
	236	622	Nazwa biblioteki	Char(10)	Nazwa biblioteki, w której znajduje się lista weryfikacji.
	246	632	Zaszyfrowane dane	Char(1)	Wartość danych do zaszyfrowania. **Y** Dane do zaszyfrowania zostały podane w żądaniu. **N** Dane do zaszyfrowania nie zostały podane w żądaniu.
	247	633	Dane pozycji	Char(1)	Wartość danych pozycji. **Y** Dane pozycji zostały podane w żądaniu. **N** Dane pozycji nie zostały podane w żądaniu.
	248	634	Długość identyfikatora pozycji	Binary(4)	Długość identyfikatora pozycji.
	250	636	Długość danych	Binary(4)	Długość danych pozycji.
	252	638	Atrybut zaszyfrowanych danych	Char(1)	Zaszyfrowane dane. **' '** Atrybut zaszyfrowanych danych nie został podany. **0** Dane do zaszyfrowania mogą być użyte jedynie do sprawdzenia pozycji. Jest to działanie domyślne. **1** Dane do zaszyfrowania mogą być użyte do sprawdzenia pozycji oraz zwrócone za pomocą operacji wyszukiwania.
	253	639	Atrybut certyfikatu X.509	Char(1)	Certyfikat X.509.
	254	640	(Obszar zastrzeżony)	Char (28)	
	282	668	Identyfikator pozycji	Byte(100)	Identyfikator pozycji.
	382	768	Dane pozycji	Byte(1000)	Dane pozycji.
		1768	Nazwa puli ASP dla biblioteki listy weryfikacji	Char(10)	Nazwa puli ASP dla biblioteki listy weryfikacji
		1778	Numer puli ASP dla biblioteki listy weryfikacji	Char(5)	Numer puli ASP dla biblioteki listy weryfikacji

Tabela 218. Pozycje kroniki VP (Błąd hasła sieciowego). Zbiór opisów pól QASYVPJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.

Tabela 218. Pozycje kroniki VP (Błąd hasła sieciowego) (kontynuacja). Zbiór opisów pól QASYVPJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
156	224	610	Rodzaj błędu	Char(1)	Rodzaj błędu, który wystąpił. **P** Błąd hasła
157	225	611	Nazwa serwera	Char(10)	Nazwa opisu serwera sieciowego, który zarejestrował zdarzenie.
167	235	621	Data serwera	Char(6)	Data zaprotokołowania zdarzenia na serwerze sieciowym.
173	241	627	Godzina serwera	Zoned(6,0)	Godzina zaprotokołowania zdarzenia na serwerze sieciowym.
179	247	633	Nazwa komputera	Char(8)	Nazwa komputera inicjującego żądanie.
187	255	641	Użytkownik	Char(10)	Użytkownik, który próbował zalogować się.

Tabela 219. Pozycje kroniki VR (Dostęp do zasobu sieciowego). Zbiór opisów pól QASYVRJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Status	Char(1)	Status dostępu. **F** Dostęp do zasobu nie powiódł się **S** Dostęp do zasobu powiódł się
157	225	611	Nazwa serwera	Char(10)	Nazwa opisu serwera sieciowego, który zarejestrował zdarzenie.
167	235	621	Data serwera	Char(6)	Data zaprotokołowania zdarzenia na serwerze sieciowym.
173	241	627	Godzina serwera	Zoned(6,0)	Godzina zaprotokołowania zdarzenia na serwerze sieciowym.
179	247	633	Nazwa komputera	Char(8)	Nazwa komputera żądającego zasobu.
187	255	641	Użytkownik	Char(10)	Nazwa użytkownika żądającego zasobu.
197	265	651	Typ operacji	Char(1)	Typ wykonywanej operacji: **A** Zmodyfikowanie atrybutów zasobu **C** Utworzenie instancji zasobu **D** Usunięcie zasobu **P** Zmodyfikowanie uprawnień zasobu **R** Odczyt danych lub uruchomienie z zasobu **W** Zapisanie danych do zasobu **X** Uruchomienie zasobu
198	266	652	Kod powrotu	Char(4)	Kod powrotu otrzymany, jeśli został nadany dostęp do zasobu.
202	270	656	Komunikat serwera	Char(4)	Komunikat wysłany po nadaniu dostępu.
206	274	660	Identyfikator zbioru	Char(5)	Identyfikator zbioru, do którego uzyskano dostęp.
211	279	665	Nazwa zasobu	Char(260)	Nazwa użytego zasobu.

Tabela 220. Pozycje kroniki VS (Sesja serwera). Zbiór opisów pól QASYVSJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Działanie sesji	Char(1)	Działanie sesji, które wystąpiło. **E** Zakończenie sesji **S** Uruchomienie sesji
157	225	611	Nazwa serwera	Char(10)	Nazwa opisu serwera sieciowego, który zarejestrował zdarzenie.
167	235	621	Data serwera	Char(6)	Data zaprotokołowania zdarzenia na serwerze sieciowym.
173	241	627	Godzina serwera	Zoned(6,0)	Godzina zaprotokołowania zdarzenia na serwerze sieciowym.
179	247	633	Nazwa komputera	Char(8)	Nazwa komputera żądającego sesji.
187	255	641	Użytkownik	Char(10)	Nazwa użytkownika żądającego sesji.
197	265	651	Uprawnienia użytkownika	Char(1)	Poziom uprawnień użytkownika dla uruchomienia sesji: **A** Administrator **G** Gość **U** Użytkownik
198	266	652	Kod przyczyny	Char(1)	Kod przyczyny zakończenia sesji. **A** Odłączenie przez administratora **D** Odłączenie automatyczne (przekroczenie limitu czasu), zasób współużytkowany został usunięty lub brak uprawnień administracyjnych **E** Błąd, odłączenie sesji lub niepoprawne hasło **N** Zwykłe odłączenie lub limit użytkowników **R** Ograniczenie konta

Tabela 221. Pozycje kroniki VU (Zmiana profilu sieciowego). Zbiór opisów pól QASYVUJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ	Char(1)	Typ rekordu, który został zmieniony. **G** Rekord grupy **U** Rekord użytkownika **M** Informacje globalne profilu użytkownika
157	225	611	Nazwa serwera	Char(10)	Nazwa opisu serwera sieciowego, który zarejestrował zdarzenie.
167	235	621	Data serwera	Char(6)	Data zaprotokołowania zdarzenia na serwerze sieciowym.
173	241	627	Godzina serwera	Zoned(6,0)	Godzina zaprotokołowania zdarzenia na serwerze sieciowym.

Tabela 221. Pozycje kroniki VU (Zmiana profilu sieciowego) (kontynuacja). Zbiór opisów pól QASYVUJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
179	247	633	Nazwa komputera	Char(8)	Nazwa komputera żądającego zmiany profilu użytkownika.
187	255	641	Użytkownik	Char(10)	Nazwa użytkownika żądającego zmiany profilu użytkownika.
197	265	651	Działanie	Char(1)	Żądane działanie: **A** Dodanie **C** Zmiana **D** Usuwanie **P** Niepoprawne hasło
198	266	652	Nazwa zasobu	Char(260)	Nazwa zasobu.

Tabela 222. Pozycje kroniki VV (Zmiana statusu usługi). Zbiór opisów pól QASYVVJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji: **C** Status usługi został zmieniony **E** Serwer został zatrzymany **P** Serwer został wstrzymany **R** Serwer został zrestartowany **S** Serwer został uruchomiony
157	225	611	Nazwa serwera	Char(10)	Nazwa opisu serwera sieciowego, który zarejestrował zdarzenie.
167	235	621	Data serwera	Char(6)	Data zaprotokołowania zdarzenia na serwerze sieciowym.
173	241	627	Godzina serwera	Zoned(6,0)	Godzina zaprotokołowania zdarzenia na serwerze sieciowym.
179	247	633	Nazwa komputera	Char(8)	Nazwa komputera żądającego zmiany.
187	255	641	Użytkownik	Char(10)	Nazwa użytkownika żądającego zmiany.
197	265	651	Status	Char(1)	Status żądania usługi: **A** Aktywowanie usługi **B** Oczekiwanie na uruchomienie usługi **C** Kontynuowanie wstrzymanej usługi **E** Zatrzymanie oczekiwania na usługę **H** Wstrzymywanie usługi **I** Wstrzymanie usługi **S** Zatrzymanie usługi
198	266	652	Kod usługi	Char(8)	Kod żądanej usługi.
206	274	660	Ustawienie tekstu	Char(80)	Tekst ustawiany przez żądanie usługi.
286	354	740	Zwracana wartość	Char(4)	Zwracana wartość z operacji zmiany.

Tabela 222. Pozycje kroniki VV (Zmiana statusu usługi) (kontynuacja). Zbiór opisów pól QASYVVJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
290	358	744	Usługa	Char(20)	Usługa, która została zmieniona.

Tabela 223. Pozycje kroniki X0 (Uwierzytelnianie sieciowe). Zbiór opisów pól QASYX0JE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.

Tabela 223. Pozycje kroniki X0 (Uwierzytelnianie sieciowe) (kontynuacja). Zbiór opisów pól QASYX0JE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
156	224	610	Typ pozycji	Char(1)	Typ pozycji: **1** Poprawny bilet usług **2** Niezgodne jednostki główne usługi **3** Niezgodne jednostki główne klienta **4** Niezgodność adresu IP biletu **5** Deszyfrowanie biletu nie powiodło się **6** Deszyfrowanie elementu uwierzytelniającego nie powiodło się **7** Dziedzina nie znajduje się w dziedzinach lokalnych klienta **8** Bilet jest próbą utworzenia odpowiedzi **9** Bilet nie jest jeszcze ważny **A** Błąd sumy kontrolnej deszyfrowania KRB_AP_PRIV lub KRB_AP_SAFE **B** Niezgodność zdalnego adresu IP **C** Niezgodność lokalnego adresu IP **D** Błąd datownika KRB_AP_PRIV lub KRB_AP_SAFE **E** Błąd odpowiedzi KRB_AP_PRIV lub KRB_AP_SAFE **F** Błąd kolejności sekwencji KRB_AP_PRIV lub KRB_AP_SAFE **K** Akceptacja GSS — wygasłe uprawnienia **L** Akceptacja GSS — błąd sumy kontrolnej **M** Akceptacja GSS — powiązania kanału **N** Odpakowanie lub weryfikacja GSS - wygasły kontekst **O** Odpakowanie lub weryfikacja GSS - odszyfrowanie/dekodowanie **P** Odpakowanie lub weryfikacja GSS - błąd sumy kontrolnej **Q** Odpakowanie lub weryfikacja GSS - błąd kolejności
	225	611	Kod statusu	Char(8)	Status żądania
	233	619	Wartość statusu GSS	Char(8)	Wartość statusu GSS
	241	627	Zdalny adres IP	Char(21)	Zdalny adres IP
	262	648	Lokalny adres IP	Char(21)	Lokalny adres IP
	283	669	Zaszyfrowane adresy	Char(256)	Zaszyfrowane adresy IP

Tabela 223. Pozycje kroniki X0 (Uwierzytelnianie sieciowe) (kontynuacja). Zbiór opisów pól QASYX0JE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	539	925	Indykator zaszyfrowanych adresów	Char(1)	Indykator zaszyfrowanych adresów IP **Y** wszystkie adresy zostały dołączone **N** nie wszystkie adresy zostały dołączone **X** nie udostępniono
	540	926	Flagi biletu	Char(8)	Flagi biletu
	548	934	Czas uwierzytelnienia biletu	Char(8)	Czas uwierzytelnienia biletu
	556	942	Czas uruchomienia biletu	Char(8)	Czas uruchomienia biletu
	564	950	Czas zakończenia biletu	Char(8)	Czas zakończenia biletu
	572	958	Czas odnowienia biletu	Char(8)	Czas odnowienia biletu
	580	966	Datownik komunikatu	Char(8)	Datownik X0E
	588	974	Datownik wygaśnięcia GSS	Char(8)	Datownik wygaśnięcia wiarygodności GSS lub datownik wygaśnięcia kontekstu
	596	982	CCSID użytkownika serwera	Binary(5)	CCSID użytkownika serwera (z biletu)
	600	986	Długość użytkownika serwera	Binary(4)	Długość użytkownika serwera (z biletu)
	602	988	Indykator użytkownika serwera	Char(1)	Indykator użytkownika serwera (z biletu) **Y** użytkownik serwera zakończony **N** użytkownik serwera nie zakończony **X** nie udostępniono
	603	989	Użytkownik serwera	Char(512)	Użytkownik serwera (z biletu)
	1115	1501	CCSID parametru użytkownika serwera	Binary(5)	CCSID parametru użytkownika serwera (z biletu)
	1119	1505	Długość parametru użytkownika serwera	Binary(4)	Długość parametru użytkownika serwera (z biletu)
	1121	1507	Indykator parametru użytkownika serwera	Char(1)	Indykator parametru użytkownika serwera (z biletu) **Y** użytkownik serwera zakończony **N** użytkownik serwera nie zakończony **X** nie udostępniono
	1122	1508	Parametr użytkownika serwera	Char(512)	Parametr użytkownika serwera, z którym musi zgadzać się bilet
	1634	2020	CCSID użytkownika klienta	Binary(5)	CCSID użytkownika klienta (z elementu uwierzytelniającego)

Tabela 223. Pozycje kroniki X0 (Uwierzytelnianie sieciowe) (kontynuacja). Zbiór opisów pól QASYX0JE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	1638	2024	Długość użytkownika klienta	Binary(4)	Długość użytkownika klienta (z elementu uwierzytelniającego)
	1640	2026	Indykator użytkownika klienta	Char(1)	Indykator użytkownika klienta (z elementu uwierzytelniającego) **Y** użytkownik klienta zakończony **N** użytkownik klienta nie zakończony **X** nie udostępniono
	1641	2027	Użytkownik klienta	Char(512)	Użytkownik klienta z elementu uwierzytelniającego
	2153	2539	CCSID użytkownika klienta	Binary(5)	CCSID użytkownika klienta (z biletu)
	2157	2543	Długość użytkownika klienta	Binary(4)	Długość użytkownika klienta (z biletu)
	2159	2545	Indykator użytkownika klienta	Char(1)	Indykator użytkownika klienta (z biletu) **Y** użytkownik klienta zakończony **N** użytkownik klienta nie zakończony **X** nie udostępniono
	2160	2546	Użytkownik klienta	Char(512)	Użytkownik klienta z biletu
	2672	3058	CCSID użytkownika serwera GSS	Binary(5)	CCSID użytkownika serwera (z referencji GSS)
	2676	3062	Długość użytkownika serwera GSS	Binary(4)	Długość użytkownika serwera (z referencji GSS)
	2678	3064	Indykator użytkownika serwera GSS	Char(1)	Indykator użytkownika serwera (z referencji GSS) **Y** użytkownik serwera zakończony **N** użytkownik serwera nie zakończony **X** nie udostępniono
	2679	3065	Użytkownik serwera GSS	Char(512)	Użytkownik serwera z referencji GSS
	3191	3577	CCSID użytkownika lokalnego GSS	Binary(5)	CCSID nazwy użytkownika lokalnego GSS
	3195	3581	Długość użytkownika lokalnego GSS	Binary(4)	Długość nazwy użytkownika lokalnego GSS
	3197	3583	Indykator użytkownika lokalnego GSS	Char(1)	Indykator nazwy użytkownika lokalnego GSS **Y** użytkownik lokalny zakończony **N** użytkownik lokalny nie zakończony **X** nie udostępniono
	3198	3584	Użytkownik lokalny GSS	Char(512)	Użytkownik lokalny GSS

Tabela 223. Pozycje kroniki X0 (Uwierzytelnianie sieciowe) (kontynuacja). Zbiór opisów pól QASYX0JE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
	3710	4096	CCSID użytkownika zdalnego GSS	Binary(5)	CCSID nazwy użytkownika zdalnego GSS
	3714	4100	Długość użytkownika zdalnego GSS	Binary(4)	Długość nazwy użytkownika zdalnego GSS
	3716	4102	Indykator użytkownika zdalnego GSS	Char(1)	Indykator nazwy użytkownika zdalnego GSS **Y** użytkownik zdalny zakończony **N** użytkownik zdalny nie zakończony **X** nie udostępniono
	3717	4103	Użytkownik zdalny GSS	Char(512)	Użytkownik zdalny GSS

Tabela 224. Pozycje kroniki X1 (Znacznik tożsamości). Zbiór opisów pól QASYX1JE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Typ pozycji: **D** Delegowanie znacznika tożsamości powiodło się **F** Delegowanie znacznika tożsamości nie powiodło się **G** Pobranie użytkownika ze znacznika tożsamości powiodło się **U** Pobranie użytkownika ze znacznika tożsamości nie powiodło się
	225	611	Kod przyczyny	Binary(5)	Kod przyczyny dla żądania, które nie powiodło się: **9** Niezgodność długości znacznika **10** Niezgodność identyfikatora EIM **11** Niezgodność identyfikatora instancji aplikacji **12** Podpis znacznika nie jest poprawny **13** Znacznik tożsamości nie jest poprawny **14** Nie odnaleziono użytkownika docelowego **16** Uchwyt klucza nie jest poprawny **17** Wersja znacznika nie jest obsługiwana **18** Nie odnaleziono klucza publicznego **Uwaga:** W przypadku niepowodzenia, w polach tekstowych pojawią się tylko te informacje, których poprawność została sprawdzona do momentu niepowodzenia.

Tabela 224. Pozycje kroniki X1 (Znacznik tożsamości) (kontynuacja). Zbiór opisów pól QASYX1JE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
		615	Zastrzeżone	Char (7)	Zastrzeżone
		622	Identyfikator CCSID danych	Binary(5)	Identyfikator CCSID danych w polach tekstowych
		626	Długość odbiorcy	Binary(5)	Długość danych w polu odbiorcy.
		630	Dziennik	Char(508)	Odbiorca znacznika tożsamości, dla którego żądanie nie powiodło się lub powiodło się. Dane w tym polu będą miały następujący format: <EIMID>ID_EIM_odbiorcy </EIMID> <APPID>ID_aplikacji_odbiorcy </APPID> <TIMESTAMP>datownik_odbiorcy </TIMESTAMP>. Datownik będzie dołączony tylko do żądań delegowania.
		1138	Długość nadawcy	Binary(5)	Długość danych w polu nadawcy.
		1142		Char(508)	Ostatni nadawca znacznika tożsamości, dla którego żądanie nie powiodło się lub powiodło się. Dane w tym polu będą miały następujący format: <EIMID>ID_EIM_nadawcy </EIMID> <APPID>ID_aplikacji_nadawcy </APPID> <TIMESTAMP>datownik_nadawcy </TIMESTAMP>.
		1650	Długość inicjatora	Binary(5)	Długość danych w polu inicjatora.
		1654	Inicjator	Char(508)	Inicjator żądania znacznika tożsamości. Jeśli pola nadawcy i inicjatora są takie same, wtedy pole długość inicjatora będzie miało wartość 0. Dane w tym polu będą miały następujący format: <EIMID>ID_EIM_inicjatora </EIMID> <APPID>ID_aplikacji_inicjatora </APPID> <TIMESTAMP>datownik_inicjatora </TIMESTAMP>.
		2162	Długość łańcucha	Binary(5)	Długość danych w polu łańcucha.
		2166	Łańcuch	Char(2036)	Łańcuch nadawców między inicjatorem a ostatnim nadawcą. Łańcuch będzie ułożony w kolejności od ostatniego do najwcześniejszego. Jeśli nie ma innych nadawców, pole długości łańcucha będzie miało wartość 0. Jeśli zmiana jest dłuższa niż długość tego pola, pole zostanie obcięte. Dane w tym polu będą miały format: <SNDRz><EIMID>ID_EIM_nadawcy</EIMID> <APPID>ID_aplikacji_nadawcy</APPID> <TIMESTAMP>datownik_nadawcy </TIMESTAMP> </SNDRz> <SNDRy>...</SNDRy>...
		4202	Pozycje łańcucha	Binary(5)	Liczba pozycji w polu łańcucha.
		4206	Dostępne pozycje łańcucha	Binary(5)	Liczba dostępnych pozycji dla łańcucha nadawców. Jeśli pole łańcucha zostało obcięte, ta liczba może być większa niż liczba pozycji w polu.
		4210	Długość rejestru źródłowego	Binary(5)	Długość danych w polu rejestru źródłowego.
		4214	Rejestr źródłowy	Char(508)	Rejestr źródłowy podany w znaczniku tożsamości.
		4722	Długość użytkownika rejestru źródłowego	Binary(5)	Długość danych w polu użytkownika rejestru źródłowego.

Tabela 224. Pozycje kroniki X1 (Znacznik tożsamości) (kontynuacja). Zbiór opisów pól QASYX1JE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
		4726	Użytkownik rejestru źródłowego	Char(508)	Użytkownik rejestru źródłowego podany w znaczniku tożsamości.
		5234	Długość rejestru docelowego	Binary(5)	Długość danych w polu rejestru docelowego.
		5238	Rejestr docelowy	Char(508)	Podany rejestr docelowy.
		5746	Długość użytkownika rejestru docelowego	Binary(5)	Długość danych w polu użytkownika rejestru docelowego.
		5750	Użytkownik rejestru docelowego	Char(508)	Użytkownik rejestru docelowego, na który odwzorowuje znacznik tożsamości. To pole jest wypełniane po pomyślnym pobraniu użytkownika z żądania znacznika tożsamości.

Tabela 225. Pozycje kroniki YC (Zmiana obiektu DLO). Zbiór opisów pól QASYYCJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Dostęp do obiektu **C** Zmiana obiektu DLO
157	225	611	Nazwa obiektu	Char(10)	Nazwa obiektu
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki
177	245	631	Typ obiektu	Char(8)	Typ obiektu
185	253	639	Użytkownik biurowy	Char(10)	Profil użytkownika biurowego
195	263	649	Nazwa folderu lub dokumentu	Char(12)	Nazwa dokumentu lub folderu
207	275	661	(Obszar zastrzeżony)	Char(8)	
215	283	669	Ścieżka folderu	Char(63)	Folder zawierający obiekt biblioteki dokumentów
278	346	732	W imieniu użytkownika	Char(10)	Użytkownik pracujący w imieniu innego użytkownika.
288	356	742	Typ dostępu	Packed(5,0)	Typ dostępu [1]

1 Listę kodów dla typów dostępu zawiera Tabela 230 na stronie 617.

Tabela 226. Pozycje kroniki YR (Odczyt obiektu DLO). Zbiór opisów pól QASYYRJE/J4/J5

Pozycje (Offsets)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Dostęp do obiektu **R** Odczyt obiektu DLO
157	225	611	Nazwa obiektu	Char(10)	Nazwa obiektu
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki
177	245	631	Typ obiektu	Char(8)	Typ obiektu
185	253	639	Użytkownik biurowy	Char(10)	Profil użytkownika biurowego
195	263	649	Nazwa folderu lub dokumentu	Char(12)	Nazwa obiektu biblioteki dokumentów.
207	275	661	(Obszar zastrzeżony)	Char(8)	
215	283	669	Ścieżka folderu	Char(63)	Folder zawierający obiekt biblioteki dokumentów
278	346	732	W imieniu użytkownika	Char(10)	Użytkownik pracujący w imieniu innego użytkownika.
288	356	742	Typ dostępu	Packed(5,0)	Typ dostępu [1]

1 Listę kodów dla typów dostępu zawiera Tabela 230 na stronie 617.

Tabela 227. Pozycje kroniki ZC (Zmiana obiektu). Zbiór opisów pól QASYZCJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Dostęp do obiektu **C** Zmiana obiektu **U** Aktualizowanie dostępu otwartego do obiektu
157	225	611	Nazwa obiektu	Char(10)	Nazwa obiektu
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki, w której znajduje się obiekt.
177	245	631	Typ obiektu	Char(8)	Typ obiektu
185	253	639	Typ dostępu	Packed(5,0)	Typ dostępu [1]

Tabela 227. Pozycje kroniki ZC (Zmiana obiektu) (kontynuacja). Zbiór opisów pól QASYZCJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
188	256	642	Dane dotyczące dostępu	Char(50)	Określone dane dotyczące dostępu Gdy typ obiektu to *IMGCLG, pole zawiera następujące formaty: **Char 3** Numer indeksu pozycji katalogu obrazów. **puste** Wskazuje, że operacja była wykonana na katalogu obrazów. **Char 32** Identyfikator woluminu pozycji katalogu obrazów. **puste** Wskazuje, że operacja była wykonana na katalogu obrazów. **Char 1** Typ dostępu dla pozycji. Możliwe wartości wymienione zostały poniżej. **puste** Wskazuje, że operacja była wykonana na katalogu obrazów. **R** Zbiór zawierający pozycję katalogu obrazu jest tylko do odczytu. **W** Zbiór zawierający pozycję katalogu obrazów można odczytać/zapisać. **Char 1** Zabezpieczenie przed zapisem dla pozycji. **puste** Wskazuje, że operacja była wykonana na katalogu obrazów. **Y** Zbiór zawierający pozycję katalogu obrazów jest zabezpieczony przed zapisem. **N** Zbiór zawierający pozycję katalogu obrazów nie jest zabezpieczony przed zapisem. **Char 10** Nazwa urządzenia wirtualnego. **puste** Wskazuje, że operacja była wykonana na katalogu obrazów lub katalog obrazów nie ma statusu Ready (gotowy). **Char 3** Nieużywane.
238			(Obszar zastrzeżony)	Char(20)	
	306	692	(Obszar zastrzeżony)	Char(18)	
	324	710	Długość nazwy obiektu [2]	Binary (4)	Długość nazwy obiektu.
258	326	712	Identyfikator CCSID nazwy obiektu[2]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.

Tabela 227. Pozycje kroniki ZC (Zmiana obiektu) (kontynuacja). Zbiór opisów pól QASYZCJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
262	330	716	Identyfikator kraju lub regionu nazwy obiektu[2]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
264	332	718	Identyfikator języka nazwy obiektu[2]	Char(3)	Identyfikator języka dla nazwy obiektu.
267	335	721	(Obszar zastrzeżony)	Char(3)	
270	338	724	Identyfikator pliku nadrzędnego[2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
286	354	740	Identyfikator pliku obiektu[2, 4]	Char(16)	Identyfikator pliku obiektu.
302	370	756	Nazwa obiektu[2]	Char(512)	Nazwa obiektu.
	882	1268	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	898	1284	Nazwa puli ASP[6]	Char(10)	Nazwa urządzenia puli ASP.
	908	1294	Numer puli ASP [6]	Char(5)	Numer urządzenia puli ASP.
	913	1299	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	917	1303	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	919	1305	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	922	1308	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.
	924	1310	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	925	1311	Identyfikator pliku o dostępie pośrednim[4]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	941	1327	Bezwzględna nazwa ścieżki[5]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

1 Listę kodów dla typów dostępu zawiera Tabela 230 na stronie 617.

2 Te pola używane są tylko dla obiektów w systemach plików QOpenSys, "root" oraz użytkownika.

3 Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

4 Gdy indykator nazwy ścieżki (pozycja 924) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla bezwzględnej nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

5 Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

6 Jeśli obiekt znajduje się w bibliotece, jest to informacja puli ASP biblioteki obiektu. Jeśli obiekt nie znajduje się w bibliotece, jest to informacja obiektu.

Pozycje kroniki kontroli

Tabela 228. ZM (dostęp do metody SOM), pozycje kroniki. Zbiór opisów pól QASYZMJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1				Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224		Typ dostępu	Char(1)	Typ dostępu
157	225		Istnienie obiektu	Char(1)	Istnienie obiektu Y
158	226		Zarządzanie obiektami	Char(1)	Zarządzanie obiektem Y
159	227		Operacyjne do obiektu	Char(1)	Operacje na obiekcie Y
160	228		Zmiana obiektu	Char(1)	Zmiana obiektu Y
161	229		Odniesienie do obiektu	Char(1)	Odniesienie do obiektu Y
162	230		Zastrzeżone	Char(10)	Pole zastrzeżone
172	240		Zarządzanie listą	Char(1)	Zarządzanie listą autoryzacji Y
173	241		Odczyt	Char(1)	Odczyt Y
174	242		Dodanie	Char(1)	Dodanie Y
175	243		Aktualizacja	Char(1)	Aktualizowanie Y
176	244		Usunięcie	Char(1)	Usunięcie Y
177	245		Wykonywanie	Char(1)	Wykonanie Y
178	246		Zastrzeżone	Char(10)	Pole zastrzeżone
188	256		Identyfikator pliku klasy	Char(16)	Identyfikator pliku klasy
204	272		Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu
220	288		Nazwa metody	Char(4096)	Nazwa metody

Tabela 229. Pozycje kroniki ZR (Odczyt obiektu). Zbiór opisów pól QASYZRJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówkowe wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja Tabela 152 na stronie 505,Tabela 153 na stronie 507 i Tabela 154 na stronie 508.
156	224	610	Typ pozycji	Char(1)	Dostęp do obiektu **R** Odczyt obiektu
157	225	611	Nazwa obiektu	Char(10)	Nazwa obiektu
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki, w której znajduje się obiekt.
177	245	631	Typ obiektu	Char(8)	Typ obiektu
185	253	639	Typ dostępu	Packed(5,0)	Typ dostępu [1]

Tabela 229. Pozycje kroniki ZR (Odczyt obiektu) (kontynuacja). Zbiór opisów pól QASYZRJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
188	256	642	Dane dotyczące dostępu	Char(50)	Określone dane dotyczące dostępu. Gdy typ obiektu to *IMGCLG, pole zawiera następujące formaty: **Char 3** Numer indeksu pozycji katalogu obrazów. **puste** Wskazuje, że operacja była wykonana na katalogu obrazów. **Char 32** Identyfikator woluminu pozycji katalogu obrazów. **puste** Wskazuje, że operacja była wykonana na katalogu obrazów. **Char 1** Typ dostępu dla pozycji. Możliwe wartości wymienione zostały poniżej. **puste** Wskazuje, że operacja była wykonana na katalogu obrazów. **R** Zbiór zawierający pozycję katalogu obrazu jest tylko do odczytu. **W** Zbiór zawierający pozycję katalogu obrazów można odczytać/zapisać. **Char 1** Zabezpieczenie przed zapisem dla pozycji. **puste** Wskazuje, że operacja była wykonana na katalogu obrazów. **Y** Zbiór zawierający pozycję katalogu obrazów jest zabezpieczony przed zapisem. **N** Zbiór zawierający pozycję katalogu obrazów nie jest zabezpieczony przed zapisem. **Char 10** Nazwa urządzenia wirtualnego. **puste** Wskazuje, że operacja była wykonana na katalogu obrazów lub katalog obrazów nie ma statusu Ready (gotowy). **Char 3** Nieużywane.
238			(Obszar zastrzeżony)	Char(20)	
	306	692	(Obszar zastrzeżony)	Char(18)	
	324	710	Długość nazwy obiektu [2]	Binary(4)	Długość nazwy obiektu.
258	326	712	Identyfikator CCSID nazwy obiektu[2]	Binary(5)	Identyfikator identyfikator kodowanego zestawu znaków dla nazwy obiektu.

Tabela 229. Pozycje kroniki ZR (Odczyt obiektu) (kontynuacja). Zbiór opisów pól QASYZRJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
262	330	716	Identyfikator kraju lub regionu nazwy obiektu[2]	Char(2)	Identyfikator kraju lub regionu dla nazwy obiektu.
264	332	718	Identyfikator języka nazwy obiektu[2]	Char(3)	Identyfikator języka dla nazwy obiektu.
267	335	721	(Obszar zastrzeżony)	Char(3)	
270	338	724	Identyfikator pliku nadrzędnego[2,3]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
286	354	740	Identyfikator pliku obiektu[2,3]	Char(16)	Identyfikator pliku obiektu.
302	370	756	Nazwa obiektu[2]	Char(512)	Nazwa obiektu.
	882	1268	Identyfikator pliku obiektu	Char(16)	Identyfikator pliku obiektu.
	898	1284	Nazwa puli ASP	Char(10)	Nazwa urządzenia puli ASP.
	908	1294	Numer puli ASP	Char(5)	Numer urządzenia puli ASP.
	913	1299	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla bezwzględnej nazwy ścieżki.
	917	1303	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla bezwzględnej nazwy ścieżki.
	919	1305	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla bezwzględnej nazwy ścieżki.
	922	1308	Długość nazwy ścieżki	Binary(4)	Długość nazwy bezwzględnej nazwy ścieżki.
	924	1310	Indykator pełnej nazwy ścieżki	Char(1)	Indykator pełnej bezwzględnej nazwy ścieżki: **Y** Pole Bezwzględna nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do obiektu. **N** Pole Bezwzględna nazwa ścieżki nie zawiera pełną bezwzględną nazwę ścieżki do obiektu.
	925	1311	Identyfikator pliku o dostępie pośrednim[4]	Char(16)	Identyfikator pliku o dostępie pośrednim bezwzględnej nazwy ścieżki.
	941	1327	Bezwzględna nazwa ścieżki[5]	Char(5002)	Bezwzględna nazwa ścieżki do obiektu.

1 Listę kodów dla typów dostępu zawiera Tabela 230 na stronie 617.

2 Te pola używane są tylko dla obiektów w systemach plików QOpenSys, "root" oraz użytkownika.

3 Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

4 Gdy indykator nazwy ścieżki (pozycja 924) ma wartość ″N″, to pole będzie zawierało identyfikator pliku o dostępie pośrednim dla bezwzględnej nazwy ścieżki. Gdy wskaźnikiem nazwy ścieżki jest ″Y″, to pole będzie zawierało 16 bajtów zer szesnastkowych.

5 Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

Tabela 230 zawiera kody dostępu używane dla pozycji kroniki kontroli obiektu w zbiorach QASYYCJE/J4/J5, QASYYRJE/J4/J5, QASYZCJE/J4/J5 i QASYZRJE/J4/J5.

Tabela 230. Kody liczbowe dla typów dostępu

Kod	Typ dostępu	Kod	Typ dostępu	Kod	Typ dostępu
1	Dodanie (Add)	26	Załadowanie (Load)	51	Wysłanie (Send)
2	Aktywowanie programu (Activate Program)	27	Sporządzenie listy (List)	52	Uruchomienie (Start)
3	Analizowanie (Analyze)	28	Przeniesienie (Move)	53	Przesłanie (Transfer)
4	Zastosowanie (Apply)	29	Scalanie (Merge)	54	Śledzenie (Trace)
5	Wywołanie lub TFRCTL (Call or TFRCTL)	30	Otwarcie (Open)	55	Weryfikowanie (Verify)
6	Konfigurowanie (Configure)	31	Drukowanie (Print)	56	Aktywowanie (Vary)
7	Zmiana (Change)	32	Zapytanie (Query)	57	Praca (Work)
8	Sprawdzanie (Check)	33	Odzyskiwanie (Reclaim)	58	Odczyt/zmiana atrybutu DLO (Read/Change DLO Attribute)
9	Zamykanie (Close)	34	Odbieranie (Receive)	59	Odczyt/zmiana ochrony DLO (Read/Change DLO Security)
10	Usuwanie zawartości (Clear)	35	Odczyt (Read)	60	Odczyt/zmiana zawartości DLO (Read/Change DLO Content)
11	Porównywanie (Compare)	36	Reorganizowanie (Reorganize)	61	Odczyt/zmiana wszystkich części DLO (Read/Change DLO all parts)
12	Anulowanie (Cancel)	37	Zwalnianie (Release)	62	Dodawanie ograniczenia (Add Constraint)
13	Kopiowanie (Copy)	38	Usuwanie (Remove)	63	Zmiana ograniczenia (Change Constraint)
14	Tworzenie (Create)	39	Zmiana nazwy (Rename)	64	Usunięcie ograniczenia (Remove Constraint)
15	Konwertowanie (Convert)	40	Zastąpienie (Replace)	65	Uruchomienie procedury (Start procedure)
16	Debugowanie (Debug)	41	Wznawianie (Resume)	66	Uzyskiwanie dostępu do **OOPOOL (Get Access on **OOPOOL)
17	Usunięcie (Delete)	42	Odtwarzanie (Restore)	67	Podpisywanie obiektu (Sign object)
18	Zrzut (Dump)	43	Odtwarzanie (Retrieve)	68	Usuwanie wszystkich podpisów (Remove all signatures)

Tabela 230. Kody liczbowe dla typów dostępu (kontynuacja)

Kod	Typ dostępu	Kod	Typ dostępu	Kod	Typ dostępu
19	Wyświetlanie (Display)	44	Uruchamianie (Run)	69	Usuwanie zawartości podpisanego obiektu (Clear a signed object)
20	Edytowanie (Edit)	45	Odwołanie (Revoke)	70	Podłączanie (Mount)
21	Zakończenie (End)	46	Składowanie (Save)	71	Rozładowanie (Unload)
22	Zbiór (File)	47	Składowanie w wolnej pamięci (Save with Storage Free)	72	Zakończenie wycofania (End Rollback)
23	Nadanie (Grant)	48	Składowanie i usunięcie (Save and Delete)		
24	Wstrzymanie (Hold)	49	Wprowadzenie (Submit)		
25	Inicjowanie (Initialize)	50	Ustawianie (Set)		

Dodatek G. Komendy i menu dla komend ochrony

Ten dodatek opisuje komendy i menu narzędzi ochrony. Przykłady użycia komend znajdują się w wielu miejscach w tym podręczniku.

Narzędzia ochrony są dostępne z dwóch menu:

- Menu SECTOOLS (Security tools - Narzędzia ochrony) służy do interaktywnego uruchamiania komend.
- Menu SECBATCH (Submit or Schedule Security Reports to Batch - Wprowadzenie raportów ochrony do zadania wsadowego lub zaplanowanie ich) służy do uruchamiania komend raportów w trybie wsadowym. Menu SECBATCH składa się z dwóch części. W pierwszej części menu jest wykorzystywana komenda Wprowadzenie zadania (Submit Job - SBMJOB) w celu skierowania raportów do natychmiastowego przetworzenia wsadowego.

  Druga część menu korzysta z komendy Dodanie pozycji harmonogramu zadań (Add Job Schedule Entry - ADDJOBSCDE). Służy ona do zaplanowania generowania raportów ochrony regularnie w określonym dniu i godzinie.

Opcje menu Narzędzia ochrony

Poniżej przedstawiono część menu SECTOOLS, która odnosi się do profili użytkowników. Aby uzyskać dostęp do tego menu, należy wpisać komendę GO SECTOOLS

```
Narzędzia ochrony (Security Tools - SECTOOLS)

Wybierz jedną z poniższych:

  Praca z profilami
     1. Analiza domyślnych haseł

     2. Wyświetlenie listy aktywnych profili
     3. Zmiana listy aktywnych profili
     4. Analiza aktywności profilu

     5. Wyświetlenie harmonogramu aktywacji
     6. Zmiana pozycji harmonogramu aktywacji

     7. Wyświetlenie harmonogramu ważności
     8. Zmiana pozycji harmonogramu utraty ważności
```

Tabela 231 opisuje wymienione opcje menu i powiązane z nimi komendy:

Tabela 231. Komendy do obsługi profilu użytkownika

Opcja menu [1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
1	ANZDFTPWD	Komenda Analiza domyślnych haseł (Analyze Default Passwords) służy do generowania raportów o profilach użytkowników, które mają hasło takie, jak nazwa profilu, i do podejmowania działań wobec tych profili.	QASECPWD[2]
2	DSPACTPRFL	Komenda Wyświetlenie listy aktywnych profili (Display Active Profile List) służy do wyświetlania lub drukowania listy profili użytkowników, które nie podlegają przetwarzaniu przez komendę ANZPRFACT.	QASECIDL[2]

Tabela 231. Komendy do obsługi profilu użytkownika (kontynuacja)

Opcja menu [1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
3	CHGACTPRFL	Komenda Zmiana listy aktywnych profili (Change Active Profile List) służy do dodawania profili użytkowników do listy wyjątków dla komendy ANZPRFACT i usuwania ich z niej. Profil użytkownika, który znajduje się na liście aktywnych profili, jest aktywny na stałe (do momentu usunięcia go z listy). Komenda ANZPRFACT nie blokuje profilu, który jest na liście aktywnych profili, niezależnie od tego, jak długo był on nieaktywny.	QASECIDL[2]
4	ANZPRFACT	Komenda Analiza aktywności profilu (Analyze Profile Activity) służy do blokowania profili użytkowników, które nie były używane przez określoną liczbę dni. Po uruchomieniu komendy ANZPRFACT w celu podania liczby dni, system uruchamia zadanie ANZPRFACT w nocy. Aby niektóre profile nie zostały zablokowane, należy użyć komendy CHGACTPRFL.	QASECIDL[2]
5	DSPACTSCD	Komenda Wyświetlenie harmonogramu aktywacji profili (Display Profile Activation Schedule) służy do wyświetlania lub drukowania informacji o harmonogramie uaktywniania i blokowania określonych profili użytkowników. Harmonogram tworzy się za pomocą komendy CHGACTSCDE.	QASECACT[2]
6	CHGACTSCDE	Komenda Zmiana pozycji harmonogramu aktywacji (Change Activation Schedule Entry) służy do uaktywniania profilu użytkownika tylko w określonych porach dnia lub dniach tygodnia. Dla każdego profilu użytkownika, który ma pozycję w harmonogramie, system tworzy pozycje harmonogramu zadań odpowiadające godzinom uaktywnienia i zablokowania.	QASECACT[2]
7	DSPEXPSCDE	Komenda Wyświetlenie harmonogramu ważności (Display Expiration Schedule) służy do wyświetlania lub drukowania listy profili użytkowników, które w przyszłości mają zostać zablokowane lub usunięte z systemu. Aby określić, czy profil użytkownika utracił ważność, należy użyć komendy CHGEXPSCDE.	QASECEXP[2]
8	CHGEXPSCDE	Komenda Zmiana pozycji harmonogramu utraty ważności (Change Expiration Schedule Entry) służy do zaplanowania usunięcia profilu użytkownika. Profil można usunąć tymczasowo (blokując go) lub usunąć go z systemu. Komenda ta używa pozycji harmonogramu zadań, która jest uruchamiana codziennie o godzinie 00:01 (1 minuta po północy). Zadanie sprawdza zbiór QASECEXP, aby określić, czy w danym dniu mają stracić ważność jakieś profile użytkowników. Za pomocą komendy DSPEXPSCD można wyświetlić te profile użytkowników.	QASECEXP[2]

Tabela 231. Komendy do obsługi profilu użytkownika (kontynuacja)

Opcja menu [1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
9	PRTPRFINT	Tę opcję należy wybrać, aby wydrukować raport zawierający wewnętrzne informacje dotyczące liczby pozycji w obiekcie profilu użytkownika (*USRPRF).	

Uwagi:

1. Są to opcje z menu SECTOOLS.
2. Zbiór ten znajduje się w bibliotece QUSRSYS.

Aby zobaczyć dodatkowe opcje, można przejść do następnej strony menu. Tabela 232 opisuje opcje menu i powiązane z nimi komendy służące do kontroli ochrony:

Tabela 232. Komendy do kontroli ochrony

Opcja menu [1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
10	CHGSECAUD	Komenda Zmiana kontroli ochrony (Change Security Auditing) służy do konfigurowania kontroli ochrony i zmiany wartości systemowych, które sterują kontrolą ochrony. Po uruchomieniu komendy CHGSECAUD system tworzy kronikę kontroli ochrony (QAUDJRN), jeśli jeszcze nie istnieje. Komenda CHGSECAUD udostępnia opcje, które ułatwiają ustawienie wartości systemowych QAUDLVL (poziom kontroli) oraz QAUDLVL2 (rozszerzenie poziomu kontroli). Aby uaktywnić wszystkie możliwe ustawienia poziomu kontroli, można podać *ALL. Aby uaktywnić najczęściej używane ustawienia (*AUTFAIL, *CREATE, *DELETE, *SECURITY i *SAVRST), można podać *DFTSET. **Uwaga:** Używając narzędzi ochrony do konfigurowania kontroli, należy zaplanować zarządzanie dziennikami kontroli. W przeciwnym przypadku wkrótce moga pojawić się problemy z wykorzystaniem dysku.	
11	DSPSECAUD	Komenda Wyświetlenie kontroli ochrony (Display Security Auditing) służy do wyświetlania informacji o kronice kontroli ochrony i wartości systemowych, które sterują kontrolą ochrony.	

Uwagi:

1. Są to opcje z menu SECTOOLS.

Jak używać menu Zadania wsadowe ochrony

Poniżej znajduje się pierwsza część menu SECBATCH:

```
SECBATCH
   Wprowadzenie raportów ochrony do zadania wsadowego lub zaplanowanie ich
            (Submit or Schedule Security Reports To Batch)
                                                          System:
Wybierz jedną z poniższych:

  Wprowadzenie raportów do zadania wsadowego
     1. Adoptowanie obiektów
     2. Pozycje kroniki kontroli
     3. Uprawnienia do listy autoryzacji
     4. Uprawnienia do komendy
     5. Uprawnienia prywatne do komendy
     6. Ochrona komunikacji
     7. Uprawnienia do katalogów
     8. Uprawnienia prywatne do katalogów
     9. Uprawnienia do dokumentów
    10. Uprawnienia prywatne do dokumentów
    11. Uprawnienia do zbiorów
    12. Uprawnienia prywatne do zbiorów
    13. Uprawnienia do folderów
```

Po wybraniu opcji z tego menu wyświetlany jest ekran Wprowadzenie zadania (Submit Job - SBMJOB), podobny do poniższego:

```
                          Wprowadzenie zadania (Submit Job - SBMJOB)
Wpisz i naciśnij Enter.
Komenda do wykonania . . . . . > PRTADPOBJ USRPRF(*ALL
_____________________________________________
_____________________________________________
_____________________________________________...
Nazwa zadania  . . . . . .  *JOBD        Nazwa, *JOBD
Opis zadania . . . . . .  . *USRPRF      Nazwa, *USRPRF
  Biblioteka . . . . . .  . __           Nazwa, *LIBL, *CURLIB
Kolejka zadań  . . . . . .  *JOBD        Nazwa, *JOBD
  Biblioteka . . . . . .  . __           Nazwa, *LIBL, *CURLIB
Priorytet zadania (w JOBQ) . . .  *JOBD  1-9, *JOBD
Priorytet wyjścia (w OUTQ) . . .  *JOBD  1-9, *JOBD
Drukarka . . . . . .  . . . .  *CURRENT  Nazwa, *CURRENT, *USRPRF...
```

Aby zmienić domyślne opcje dla komendy, można nacisnąć klawisz F4 (Podpowiedź) w wierszu *Komenda do wykonania*.

Aby wyświetlić Raporty harmonogramu zadań wsadowych, należy przejść do następnej strony menu SECBATCH. Używając opcji tej części menu można, na przykład, skonfigurować system, aby regularnie generował zmienione wersje raportów.

```
SECBATCH
   Wprowadzenie raportów ochrony do zadania wsadowego lub zaplanowanie ich
            (Submit or Schedule Security Reports To Batch)
                                                        System:
Wybierz jedną z poniższych:

    28. Obiekty użytkownika
    29. Informacje o profilu użytkownika
    30. Dane wewnętrzne profilu użytkownika
    31. Sprawdzenie integralności obiektu

Harmonogram raportów wsadowych
    40. Adoptowanie obiektów
    41. Pozycje kroniki kontroli
    42. Uprawnienia do listy autoryzacji
    43. Uprawnienia do komendy
    44. Uprawnienia prywatne do komendy
    45. Ochrona komunikacji
    46. Uprawnienia do katalogów
```

Aby wyświetlić dodatkowe opcje menu, należy przejść do następnej strony. Po wybraniu opcji z tej części menu jest wyświetlany ekran Dodanie pozycji harmonogramu zadań (Add Job Schedule Entry - ADDJOBSCDE):

```
                     Dodanie pozycji harmonogramu zadań (Add Job Schedule Entry - ADDJOBSCDE)

Wpisz i naciśnij Enter.
Nazwa zadania  . . . . . .  _____                    Nazwa, *JOBD
Komenda do wykonania . . . . . > PRTADPOBJ USRPRF(*ALL)
_____________________________________________
_____________________________________________
_____________________________________________
_____________________________________________...
Częstotliwość  . . . . . .  _________    *ONCE, *WEEKLY, *MONTHLY
Data w harmonogramie lub . . . .  *CURRENT     Data, *CURRENT, *MONTHST
Dzień w harmonogramie  . . . . .  *NONE        *NONE, *ALL, *MON, *TUE.
+ więcej wartości
Godzina w harmonogramie  . . . .  *CURRENT     Godzina, *CURRENT
```

Aby wybrać inne ustawienia dla raportu, można ustawić kursor w wierszu *Komenda do wykonania* i nacisnąć klawisz F4 (Podpowiedź). Należy wpisać taką nazwę zadania, aby je rozpoznać podczas wyświetlania pozycji harmonogramu zadań.

Opcje menu Zadania wsadowe ochrony

Tabela 233 na stronie 624 opisuje opcje menu i powiązane z nimi komendy dotyczące raportów ochrony.

Generując raporty ochrony, system drukuje tylko informacje spełniające kryteria zarówno podane przez użytkownika, jak i obowiązujące dla narzędzia. Na przykład opisy zadań, które zawierają nazwę profilu użytkownika, są związane z ochroną. W związku z tym raport opisów zadań (PRTJOBDAUT) zawiera opisy zadań w podanej bibliotece tylko wtedy, gdy uprawnienie publiczne dla opisu zadania nie ma wartości *EXCLUDE *oraz* jeśli w opisie zadania, w parametrze USER, jest określona nazwa profilu użytkownika.

Podobnie, podczas wyświetlania informacji o podsystemie (komenda PRTSBSDAUT) system uwzględnia informacje o podsystemie tylko wtedy, gdy jego opis zawiera pozycję dotyczącą komunikacji, w której jest podany profil użytkownika.

Jeśli w określonym raporcie jest mniej informacji, niż można się spodziewać, należy skorzystać z pomocy online, aby zapoznać się z kryteriami wyboru raportu.

Tabela 233. Komendy raportów ochrony

Opcja menu [1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
1, 40	PRTADPOBJ	Komenda Drukowanie obiektów adoptujących (Print Adopting Objects) służy do drukowania listy obiektów, które adoptują uprawnienia określonego profilu użytkownika. Można podać pojedynczy profil, ogólną nazwę profilu (na przykład wszystkie profile zaczynające się od Q) lub wszystkie profile użytkowników w systemie. Ten raport ma dwie wersje. Pełny raport zawiera wszystkie obiekty adoptujące, które spełniają kryteria wyboru. Raport zmian zawiera różnice pomiędzy obiektami adoptującymi, które są obecnie w systemie, a tymi, które były w systemie w momencie poprzedniego generowania raportu.	QSECADPOLD[2]
2, 41	DSPAUDJRNE	Komenda Wyświetlenie pozycji kroniki kontroli (Display Audit Journal Entries) służy do wyświetlania lub drukowania informacji o pozycjach w kronice kontroli ochrony. Można wybrać określone typy pozycji, użytkowników i przedział czasu.	QASYxxJ5[3]
3, 42	PRTPVTAUT *AUTL	Komenda Drukowanie uprawnień prywatnych (Print Private Authorities) użyta dla obiektów *AUTL umożliwia wyświetlenie wszystkich list autoryzacji w systemie. Raport zawiera użytkowników z uprawnieniami do każdej listy oraz informacje o uprawnieniach, jakie ci użytkownicy posiadają do tych list. Informacje te są pomocne podczas analizowania źródeł uprawnień do obiektów w systemie. Ten raport ma trzy wersje. Pełny raport zawiera wszystkie listy autoryzacji w systemie. Raport zmian zawiera wykaz uprawnień, które zostały dodane lub zmienione od ostatniego generowania raportu. Raport usunięć zawiera użytkowników, których uprawnienia do listy autoryzacji zostały usunięte od ostatniego generowania raportu. Podczas drukowania pełnego raportu można wydrukować listy obiektów chronionych przez listy autoryzacji. System utworzy oddzielny raport dla każdej listy autoryzacji.	QSECATLOLD[2]
6, 45	PRTCMNSEC	Komenda Drukowanie ochrony komunikacji (Print Communications Security) służy do drukowania ustawień związanych z ochroną dla obiektów, które mają wpływ na komunikację w systemie. Ustawienia te określają, jaki dostęp do systemu mają użytkownicy i zadania. Komenda ta generuje dwa raporty: jeden zawiera ustawienia dla list konfiguracji w systemie, drugi zawiera parametry opisów linii, kontrolerów i urządzeń dotyczące ochrony. Każdy z tych raportów ma dwie wersje: pełny raport i raport zmian.	QSECCMNOLD[2]

Tabela 233. Komendy raportów ochrony (kontynuacja)

Opcja menu [1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
15, 54	PRTJOBDAUT	Komenda Drukowanie uprawnień dla JOBD (Print Job Description Authority) służy do drukowania listy opisów zadań, które zawierają profile użytkowników i których uprawnienie publiczne ma wartość inną niż *EXCLUDE. Raport zawiera uprawnienia specjalne dla profilu użytkownika, który został podany w opisie zadania. Ten raport ma dwie wersje. Pełny raport zawiera wszystkie obiekty opisów zadań, które spełniają kryteria wyboru. Raport zmian zawiera różnice pomiędzy obiektami opisów zadań, które są obecnie w systemie, a tymi, które były w systemie w momencie poprzedniego generowania raportu.	QSECJBDOLD[2]
Patrz uwaga 4	PRTPUBAUT	Komenda Drukowanie obiektów z uprawnieniami publicznymi (Print Publicly Authorized Objects) służy do drukowania listy obiektów, których uprawnienie publiczne jest inne niż *EXCLUDE. Podczas uruchamiania komendy należy podać typ obiektu i bibliotekę lub biblioteki dla raportu. Komendy PRTPUBAUT należy używać do uzyskiwania informacji o obiektach, do których ma dostęp każdy użytkownik w systemie. Ten raport ma dwie wersje. Pełny raport zawiera wszystkie obiekty, które spełniają kryteria wyboru. Raport zmian zawiera różnice między obiektami, które są obecnie w systemie, a obiektami (tego samego typu i w tej samej bibliotece), które były w systemie w momencie poprzedniego generowania raportu.	QPBxxxxxx[5]
Patrz uwaga 2.	PRTPVTAUT	Komenda Drukowanie uprawnień prywatnych (Print Private Authorities) służy do drukowania listy uprawnień prywatnych do obiektów określonego typu w określonej bibliotece. Można go użyć do określenia źródła uprawnienia do obiektu. Ten raport ma trzy wersje. Pełny raport zawiera wszystkie obiekty, które spełniają kryteria wyboru. Raport zmian zawiera różnice pomiędzy obiektami, które są obecnie w systemie, a obiektami (tego samego typu i w tej samej bibliotece), które były w systemie w momencie poprzedniego generowania raportu. Raport usunięć zawiera użytkowników, których uprawnienia do obiektu zostały zmienione od ostatniego drukowania raportu.	QPVxxxxxx[5]

Tabela 233. Komendy raportów ochrony (kontynuacja)

Opcja menu [1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
24, 63	PRTQAUT	Komenda Drukowanie uprawnień dla kolejki (Print Queue Report) służy do drukowania ustawień ochrony dla kolejek wyjściowych i kolejek zadań w systemie. Ustawienia te określają, kto może przeglądać i zmieniać pozycje w kolejce wyjściowej lub kolejce zadań. Ten raport ma dwie wersje. Pełny raport zawiera wszystkie obiekty kolejki wyjściowej i kolejki zadań, które spełniają kryteria wyboru. Raport zmian zawiera różnice między obiektami kolejki wyjściowej i kolejki zadań, które są obecnie w systemie, a tymi, które były w systemie w momencie poprzedniego generowania raportu.	QSECQOLD[2]
25, 64	PRTSBSDAUT	Komenda Drukowanie opisu podsystemu (Print Subsystem Description) służy do drukowania pozycji komunikacji dotyczących ochrony dla opisów podsystemów w systemie. Ustawienia te określają, jak dane są wprowadzane do systemu i jak działają zadania. Raport zawiera opis podsystemu tylko wtedy, gdy są w nim pozycje związane z komunikacją, w których jest podana nazwa profilu użytkownika. Ten raport ma dwie wersje. Pełny raport zawiera wszystkie obiekty opisów podsystemów, które spełniają kryteria wyboru. Raport zmian zawiera różnice między obiektami opisów podsystemów, które są obecnie w systemie, a tymi, które były w systemie w momencie poprzedniego generowania raportu.	QSECSBDOLD[2]
26, 65	PRTSYSSECA	Komenda Wydruk atrybutów ochrony systemu (Print System Security Attributes) służy do drukowania listy wartości systemowych i atrybutów sieciowych dotyczących ochrony. Raport zawiera wartość bieżącą i zalecaną.	
27, 66	PRTTRGPGM	Komenda Drukowanie programów wyzwalaczy (Print Trigger Programs) służy do drukowania listy programów wyzwalanych, które są powiązane ze zbiorami bazy danych w systemie. Ten raport ma dwie wersje. Pełny raport zawiera każdy program wyzwalacza, który jest przypisany do bazy i spełnia kryteria wyboru. Raport zmian zawiera programy wyzwalaczy, które zostały przypisane od ostatniego generowania tego raportu.	QSECTRGOLD[2]

Tabela 233. Komendy raportów ochrony (kontynuacja)

Opcja menu [1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
28, 67	PRTUSROBJ	Komenda Drukowanie obiektów użytkownika (Print User Objects) służy do drukowania listy obiektów użytkownika (niedostarczonych przez IBM), które znajdują się w bibliotece. Raportu tego można używać do drukowania listy obiektów użytkownika, które są w bibliotece (na przykład QSYS) znajdującej się na liście bibliotek systemowych. Ten raport ma dwie wersje. Pełny raport zawiera wszystkie obiekty użytkownika, które spełniają kryteria wyboru. Raport zmian zawiera różnice pomiędzy obiektami użytkownika, które są obecnie w systemie, a tymi, które były w systemie w momencie poprzedniego generowania raportu.	QSECPUOLD[2]
29, 68	PRTUSRPRF	Komenda Drukowanie profilu użytkownika (Print User Profile) służy do analizowania profili użytkowników, które spełniają określone kryteria. Profile użytkowników można wybierać w oparciu o uprawnienia specjalne, klasę użytkownika lub niezgodności pomiędzy uprawnieniami specjalnymi a klasą użytkownika. Można wyświetlać informacje o uprawnieniach, środowisku i hasłach.	
30, 69	PRTPRFINT	Tę opcję należy wybrać, aby wydrukować raport zawierający wewnętrzne informacje dotyczące liczby pozycji w obiekcie profilu użytkownika (*USRPRF).	
31, 70	CHKOBJITG	Komenda Sprawdzenie integralności obiektu (Check Object Integrity) służy do określania, czy obiekty uruchamialne (takie jak programy) zostały zmienione bez użycia kompilatora. Komenda ta pomaga w wykryciu prób wprowadzenia wirusa do systemu lub zmiany programu tak, aby wykonywał on instrukcje, do których nie jest uprawniony.	

Uwagi:

1. Są to opcje z menu SECBATCH.
2. Zbiór ten znajduje się w bibliotece QUSRSYS.
3. xx jest dwuznakowym typem pozycji kroniki. Na przykład modelowy plik wyjściowy pozycji kroniki AE to QSYS/QASYAEJ5. Modelowe pliki wyjściowe są opisane w Dodatku F tej książki.
4. Menu SECTOOLS zawiera opcje dla typów obiektu, które zwykle leżą w obszarze zainteresowań administratorów ochrony. Na przykład, aby uruchomić komendę PRTPUBAUT dla obiektów *FILE, należy użyć opcji 11 lub 50. Opcje ogólne (18 i 57) służą do podania typu obiektu. Opcje 12 i 51 uruchamiają komendę PRTPVTAUT dla obiektów *FILE. Opcje ogólne (19 i 58) służą do podania typu obiektu.
5. Znaki xxxxxx w nazwie zbioru określają typ obiektu. Na przykład zbiór dla obiektów programów nazywa się QPBPGM dla uprawnień publicznych i QPVPGM dla uprawnień prywatnych. Zbiory te znajdują się w bibliotece QUSRSYS.

   Zbiór zawiera podzbiór dla każdej biblioteki, w której wydrukowano raport. Nazwa podzbioru jest taka sama, jak nazwa biblioteki.

Komendy dostosowywania ochrony

Tabela 234 na stronie 628 opisuje komendy, których można użyć, aby dostosować ochronę w systemie. Opcje znajdują się w menu SECTOOLS:

Tabela 234. Komendy dostosowywania systemu

Opcja menu [1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
60	CFGSYSSEC	Komenda Konfigurowanie ochrony systemu (Configure System Security) służy do ustawiania zalecanych wartości systemowych dotyczących ochrony. Komenda ta konfiguruje również kontrolę ochrony w systemie. Sekcja “Wartości ustawiane za pomocą komendy Konfigurowanie ochrony systemu” opisuje działanie komendy.	
61	RVKPUBAUT	Komenda Odwołanie uprawnień publicznych (Revoke Public Authority) służy do ustawienia uprawnienia publicznego *EXCLUDE dla zestawu komend istotnych dla ochrony. Sekcja “Co robi komenda Odwołanie uprawnień publicznych” na stronie 630 zawiera listę czynności wykonywanych przez komendę RVKPUBAUT.	

Uwagi:

1. Są to opcje z menu SECTOOLS.

Wartości ustawiane za pomocą komendy Konfigurowanie ochrony systemu

Tabela 235 zawiera wartości systemowe, które są ustawiane podczas uruchamiania komendy CFGSYSSEC. Komenda CFGSYSSEC uruchamia program QSYS/QSECCFGS.

Tabela 235. Wartości ustawiane za pomocą komendy CFGSYSSEC

Nazwa wartości systemowej	Ustawienie	Opis wartości systemowej
QAUTOCFG	0 (Nie)	Automatyczne konfigurowanie nowych urządzeń
QAUTOVRT	0	Liczba opisów urządzeń wirtualnych, które system tworzy automatycznie, jeśli żadne urządzenie nie jest dostępne.
QALWOBJRST	*NONE	Określa, czy mogą być odtwarzane programy systemowe i programy, które adoptują uprawnienia
QDEVRCYACN	*DSCMSG (Odłączenie po komunikacie)	Działanie systemu, gdy komunikacja jest ustanawiana ponownie
QDSCJOBITV	120	Okres, po jakim system podejmie działania dla odłączonego zadania
QDSPSGNINF	1 (Tak)	Określa, czy użytkownicy widzą ekran informacyjny wpisywania się
QINACTITV	60	Okres, po jakim system podejmie działania dla nieaktywnego zadania interaktywnego
QINACTMSGQ	*ENDJOB	Działanie, które podejmie system dla nieaktywnego zadania
QLMTDEVSSN	1 (Tak)	Określa, czy użytkownicy mają ograniczoną możliwość wpisania się do więcej niż jednego urządzenia w tym samym czasie
QLMTSECOFR	1 (Tak)	Określa, czy użytkownicy z uprawnieniami *ALLOBJ i *SERVICE są ograniczeni do określonych urządzeń
QMAXSIGN	3	Określa liczbę dozwolonych kolejnych, niepomyślnych prób wpisania się
QMAXSGNACN	3 (Oba)	Określa, czy system wyłącza stację roboczą lub profil użytkownika, gdy osiągnięty zostanie limit wartości QMAXSIGN.
QRMTSIGN	*FRCSIGNON	Określa w jaki sposób system obsługuje próby zdalnego wpisania się (przez tranzyt lub TELNET).
QRMTSVRATR	0 (Wyłączone)	Umożliwia zdalne analizowanie systemu.

Tabela 235. Wartości ustawiane za pomocą komendy CFGSYSSEC (kontynuacja)

Nazwa wartości systemowej	Ustawienie	Opis wartości systemowej
QSECURITY [1]	50	Wymuszony poziom ochrony
QPWDEXPITV	60	Określa częstotliwość zmiany haseł użytkowników
QPWDMINLEN	6	Określa minimalną długość hasła
QPWDMAXLEN	8	Określa maksymalną długość hasła
QPWDPOSDIF	1 (Tak)	Określa, czy każda pozycja nowego hasła musi różnić się od takiej samej pozycji poprzedniego hasła
QPWDLMTCHR	Patrz uwagi w sekcji 2	Określa znaki, które są niedozwolone w haśle
QPWDLMTAJC	1 (Tak)	Określa, czy niedozwolone są przylegające numery w haśle
QPWDLMTREP	2 (Nie mogą być kolejno powtarzane)	Określa, czy powtarzanie znaków w haśle jest zabronione
QPWDRQDDGT	1 (Tak)	Określa, czy hasło powinno zawierać przynajmniej jedną liczbę
QPWDRQDDIF	1 (32 unikalne hasła)	Określa, ile unikalnych haseł należy podać, przed ponownym powtórzeniem hasła
QPWDVLDPGM	*NONE	Określa program użytkownika do obsługi wyjścia, który system wywołuje w celu sprawdzenia haseł

Uwagi:

1. Jeśli w systemie wartość QSECURITY jest ustawiona na 30 lub mniej, przed zmianą na wyższy poziom ochrony należy zapoznać się z informacjami z Rozdziału 2 tego podręcznika.
2. Znaki zastrzeżone przechowywane są w komunikacie ID CPXB302 w pliku komunikatów QSYS/QCPFMSG. Początkowo są to znaki AEIOU@$#. Aby je zmienić należy skorzystać z komendy Zmiana opisu komunikatu (Change Message Description - CHGMSGD).

Komenda CFGSYSSEC ustawia także hasło na wartość *NONE dla wymienionych poniżej profili użytkowników IBM:

QSYSOPR

QPGMR

QUSER

QSRV

QSRVBAS

Komenda CFGSYSSEC konfiguruje także kontrolę ochrony według wartości podanych za pomocą komendy Zmiana kontroli ochrony (Change Security Auditing - CHGSECAUD).

Zmienianie programu

Jeśli niektóre z tych ustawień nie są odpowiednie dla instalacji użytkownika, można utworzyć własną wersję programu, który przetwarza komendę. W tym celu należy wykonać następujące czynności:

__ Krok 1. Aby skopiować źródło programu uruchamianego podczas używania komendy CFGSYSSEC, wywołaj komendę Odtworzenie źródła CL (Retrieve CL Source - RTVCLSRC). Wczytywany program to QSYS/QSECCFGS. Po jego wczytaniu nadaj mu *inną nazwę*.

__ Krok 2. Wprowadź zmiany w programie. Następnie skompiluj go. Podczas kompilowania upewnij się, że program QSYS/QSECCFGS dostarczony przez IBM *nie jest* zastępowany. Twój program powinien mieć inną nazwę.

__ Krok 3. Aby zmienić program do przetwarzania parametru komendy (PGM) dla komendy CFGSYSSEC, wywołaj komendę Zmiana komendy (Change Command - CHGCMD). Jako wartość PGM podaj nazwę swojego programu. Na przykład jeśli w bibliotece QGPL utworzono program MOJ_PROG_SECCFG, należy wpisać następującą komendę:

```
CHGCMD CMD(QSYS/CFGSYSSEC) PGM(QGPL/MOJ_PROG_SECCFG)
```

Uwaga: Jeśli zmieniono program QSYS/QSECCFGS, IBM nie gwarantuje lub nie implikuje niezawodności, użyteczności, wydajności lub funkcjonalności tego programu. Domniemane gwarancje przydatności handlowej lub użyteczności do określonego celu są wyraźnie odrzucone.

Co robi komenda Odwołanie uprawnień publicznych

Komenda Odwołanie uprawnień publicznych (Revoke Public Authority - RVKPUBAUT) służy do ustawiania uprawnień publicznych *EXCLUDE dla zestawu komend i programów. Komenda RVKPUBAUT uruchamia program QSYS/QSECRVKP. Jeśli program QSECRVKP jest dostępny, odwołuje uprawnienia publiczne (ustawiając je na wartość *EXCLUDE) dla komend, które zawiera Tabela 236 oraz aplikacyjnych interfejsów programistycznych (API), które zawiera Tabela 237. W dostarczanym systemie uprawnienia publiczne dla tych komend i interfejsów API są ustawione na wartość *USE.

Komendy, które zawiera Tabela 236 oraz interfejsy API, które zawiera Tabela 237 wykonują w systemie funkcje, które mogą spowodować szkody. Administrator systemu powinien jawnie nadawać uprawnienia użytkownikom, którzy mogą uruchamiać te komendy i programy, a nie udostępniać je wszystkim użytkownikom w systemie.

Podczas uruchamiania komendy RVKPUBAUT należy podać bibliotekę, która zawiera komendy. Domyślnie jest to biblioteka QSYS. Jeśli w systemie ustawiono więcej niż jeden język narodowy, komendę należy uruchomić dla każdej biblioteki QSYSxxx.

Tabela 236. Komendy, dla których uprawnienia publiczne ustawiane są za pomocą komendy RVKPUBAUT

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGERMVWSE
ADDPJE	CHGWSE	RSTLIBRSTOBJRSTS36F
ADDRTGE	CPYCFGL	RSTS36FLR
ADDWSE	CRTCFGL	RSTS36LIBMSTRRMTSPT STRSBS
CHGAJE	CRTCTLAPPC	WRKCFGL
CHGCFGL	CRTDEVAPPC	
CHGCFGLE	CRTSBSD	
CHGCMNE	ENDRMTSPT	
CHGCTLAPPC	RMVAJE	
CHGDEVAPPC	RMVCFGLE	

Wszystkie interfejsy API, które zawiera Tabela 237 znajdują się w bibliotece QSYS:

Tabela 237. Programy, dla których uprawnienia publiczne ustawiane są za pomocą komendy RVKPUBAUT

QTIENDSUP
QTISTRSUP
QWTCTLTRQWTSETTRQY2FTML

W systemie V3R7, podczas uruchamiania komendy RVKPUBAUT system ustawia uprawnienia publiczne dla katalogu głównego na wartość *USE (chyba że uprawnienia są już ustawione na wartość *USE lub niższą).

Zmienianie programu

Jeśli niektóre z tych ustawień nie są odpowiednie dla instalacji użytkownika, można utworzyć własną wersję programu, który przetwarza komendę. W tym celu należy wykonać następujące czynności:

__ Krok 1. Aby skopiować źródło programu uruchamianego podczas używania komendy RVKPUBAUT, wywołaj komendę Odtworzenie źródła CL (Retrieve CL Source - RTVCLSRC). Wczytywany program to QSYS/QSECRVKP. Po jego wczytaniu nadaj mu *inną nazwę*.

__ Krok 2. Wprowadź zmiany w programie. Następnie skompiluj go. Podczas kompilowania upewnij się, że program QSYS/QSECRVKP dostarczony przez IBM *nie jest* zastępowany. Twój program powinien mieć inną nazwę.

__ Krok 3. Aby zmienić program do przetwarzania parametru komendy (PGM) dla komendy RVKPUBAUT, wywołaj komendę Zmiana komendy (Change Command - CHGCMD). Jako wartość PGM podaj nazwę swojego programu. Na przykład jeśli w bibliotece QGPL utworzono program MOJ_PROG_RVK, należy wpisać następującą komendę:

```
CHGCMD CMD(QSYS/RVKPUBAUT) PGM(QGPL/MOJ_PROG_RVK)
```

Uwaga: Jeśli zmieniono program QSYS/QSECRVKP, IBM nie gwarantuje lub nie implikuje niezawodności, użyteczności, wydajności lub funkcjonalności tego programu. Domniemane gwarancje przydatności handlowej lub użyteczności do określonego celu są wyraźnie odrzucone.

Dodatek H. Uwagi

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

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

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

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

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

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

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

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

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

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

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

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
USA

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

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

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

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

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

Wszelkie ceny podawane przez IBM są propozycjami cen detalicznych; ceny te są aktualne i podlegają zmianom bez wcześniejszego powiadomienia. Ceny dealerów mogą się od nich różnić.

Niniejsza informacja służy jedynie do celów planowania. Informacja ta podlega zmianom do chwili, gdy produkty, których ona dotyczy, staną się dostępne.

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

LICENCJA W ZAKRESIE PRAW AUTORSKICH:

Niniejsza publikacja zawiera przykładowe aplikacje w kodzie źródłowym, ilustrujące techniki programowania w różnych systemach operacyjnych. Te programy przykładowe można kopiować, zmieniać i rozpowszechniać w dowolnej formie bezpłatnie, do celów projektowych, użytkowych, marketingowych lub dystrybucyjnych zgodnie z interfejsem programistycznym dla platformy operacyjnej, dla której przykładowe programy zostały napisane. Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować lub sugerować niezawodności, użyteczności i funkcjonalności tych programów.

Z UWZGLĘDNIENIEM WSZELKICH BEZWZGLĘDNIE OBOWIĄZUJĄCYCH GWARANCJI, KTÓRYCH NIE WOLNO WYKLUCZYĆ, IBM, PROGRAMIŚCI IBM ORAZ DOSTAWCY NIE UDZIELAJĄ W ZAKRESIE TEGO PROGRAMU CZY EWENTUALNEGO WSPARCIA TECHNICZNEGO ŻADNYCH GWARANCJI (W TYM TAKŻE RĘKOJMI), ANI NIE USTALAJĄ WARUNKÓW, WYRAŹNYCH CZY DOMNIEMANYCH, A W

| SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI CZY WARUNKÓW PRZYDATNOŚCI HANDLOWEJ,
| PRZYDATNOŚCI DO OKREŚLONEGO CELU CZY NIENARUSZANIA PRAW STRON TRZECICH.

| W ŻADNYM PRZYPADKU IBM, PROGRAMIŚCI IBM ANI DOSTAWCY NIE PONOSZĄ
| ODPOWIEDZIALNOŚCI ZA PONIŻSZE STRATY LUB SZKODY, NAWET JEŚLI BYLIBY POINFORMOWANI
| O MOŻLIWOŚCI ICH WYSTĄPIENIA:

| 1. UTRATA LUB USZKODZENIE DANYCH;
| 2. SZKODY SZCZEGÓLNE, UBOCZNE LUB POŚREDNIE, A TAKŻE SZKODY, KTÓRYCH NIE MOŻNA
| BYŁO PRZEWIDZIEĆ PRZY ZAWIERANIU UMOWY; ORAZ
| 3. UTRATA ZYSKÓW, KONTAKTÓW HANDLOWYCH, PRZYCHODÓW, REPUTACJI (GOODWILL) LUB
| PRZEWIDYWANYCH OSZCZĘDNOŚCI.

| USTAWODAWSTWA NIEKTÓRYCH KRAJÓW NIE DOPUSZCZAJĄ WYŁĄCZENIA ANI OGRANICZENIA
| ODPOWIEDZIALNOŚCI ZA SZKODY UBOCZNE LUB SZKODY, KTÓRYCH NIE MOŻNA BYŁO
| PRZEWIDZIEĆ PRZY ZAWIERANIU UMOWY, W ZWIĄZKU Z CZYM W ODNIESIENIU DO NIEKTÓRYCH
| KLIENTÓW POWYŻSZE WYŁĄCZENIE LUB OGRANICZENIE MOŻE NIE MIEĆ ZASTOSOWANIA.

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

Przy przeglądaniu tych informacji w formie elektronicznej, fotografie i ilustracje kolorowe mogą się nie pojawić.

Znaki towarowe

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

| 400
| AIX
| AS/400
| COBOL/400
| DB2
| DB2 Universal Database
| Domino
| DRDA
| e(logo)server
| eServer
| i5/OS
| IBM
| iSeries
| Lotus
| MQSeries
| MVS
| NetServer
| Notes
| OfficeVision
| Operating System/400
| OS/2
| OS/400
| Print Services Facility
| PrintManager
| Redbooks

| RPG/400
| SAA
| SecureWay
| SQL/400
| System/36
| System/38
| SystemView
| WebSphere
| zSeries

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

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

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

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

| Warunki pobierania i drukowania informacji

| Zezwolenie na korzystanie z informacji, które Użytkownik zamierza pobrać, jest przyznawane na poniższych | warunkach. Warunki te wymagają akceptacji Użytkownika.

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

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

| Z wyjątkiem zezwoleń wyraźnie udzielonych w niniejszym dokumencie, nie udziela się jakichkolwiek innych | zezwoleń, licencji ani praw, wyraźnych czy domniemanych, odnoszących się do tych informacji oraz danych, | oprogramowania lub innej własności intelektualnej, w nich zawartych.

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

| Użytkownik ma prawo pobierać, eksportować lub reeksportować niniejsze informacje pod warunkiem zachowania | bezwzględnej i pełnej zgodności z obowiązującym prawem i przepisami, w tym ze wszelkimi prawami i przepisami | eksportowymi Stanów Zjednoczonych. IBM NIE UDZIELA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE | RĘKOJMI, DOTYCZĄCYCH TREŚCI TYCH INFORMACJI. INFORMACJE TE SĄ DOSTARCZANE W STANIE, | W JAKIM SIĘ ZNAJDUJĄ (″AS IS″) BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE | RĘKOJMI, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI | PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU CZY NIENARUSZANIA PRAW | STRON TRZECICH.

Wszelkie materiały są chronione prawem autorskim IBM Corporation.

| Pobieranie lub drukowanie informacji z tego serwisu oznacza zgodę na warunki zawarte w niniejszym dokumencie.

Informacje pokrewne

Szczegółowe informacje dotyczące danego tematu zawierają inne publikacje IBM. Przydatne informacje zawierają następujące książki IBM dotyczące systemu iSeries.

Ochrona zaawansowana

- *Wskazówki i narzędzia dotyczące ochrony iSeries*, SC85-0032-07 udostępnia zestaw praktycznych sugestii dotyczących korzystania z opcji zabezpieczających systemu iSeries oraz ustanawiania procedur obsługi, które uwzględniają wymagania ochrony. Ta książka opisuje także, jak konfigurować i korzystać z ochrony oraz jak używać narzędzi ochrony, które są częścią systemu OS/400. Patrz płyta CD-ROM iSeries: Information Center Supplemental Manuals.
- *Implementing iSeries 400 Security, 3rd Edition* by Wayne Madden and Carol Woodbury. Loveland, Colorado: 29th Street Press, oddział Duke Communication International, 1998. Zawiera wskazówki i praktyczne sugestie dotyczące planowania, konfigurowania i zarządzania ochroną systemu iSeries.

  Numer zamówienia ISBN
  1–882419–78–2

Składowanie i odtwarzanie

- *Składowanie i odtwarzanie*, SA12-7269-07 udostępnia informacje na temat planowania strategii składowania i odtwarzania, składowania danych z systemu i ich odtwarzania, informacje na temat puli pamięci dyskowych oraz opcji zabezpieczania dysków. Patrz płyta CD-ROM iSeries: Information Center Supplemental Manuals.
- Dodatkowe informacje na temat składowania i odtwarzania można znaleźć w Centrum informacyjnym. Więcej informacji można znaleźć w sekcji “Informacje wstępne i pokrewne” na stronie xvi.

Podstawowe informacje dotyczące ochrony oraz ochrona fizyczna

- Temat Podstawowa ochrona systemu i jej planowanie w Centrum informacyjnym zawiera informacje wyjaśniające konieczność zastosowania ochrony, wyjaśnia najważniejsze pojęcia i udostępnia informacje dotyczące planowania, implementowania i monitorowania podstawowej ochrony systemu. Więcej informacji na ten temat zawiera sekcja “Informacje wstępne i pokrewne” na stronie xvi.

Program licencjonowany iSeries Access for Windows

- Temat iSeries Access for Windows w Centrum informacyjnego udostępnia informacje techniczne dotyczące programów iSeries Access for Windows dla wszystkich wersji iSeries Access for Windows. Więcej informacji na ten temat zawiera sekcja “Informacje wstępne i pokrewne” na stronie xvi.

Komunikacja i sieć

- *SNA Distribution Services*, SC41-5410-01 udostępnia informacje dotyczące konfigurowania sieci dla usług dystrybucyjnych SNA (Systems Network Architecture distribution services - SNADS) oraz mostu maszyny wirtualnej/pamięci MVS (Virtual Machine/Multiple Virtual Storage - VM/MVS). Dodatkowo w tej książce omówione zostały funkcje dystrybucji obiektów, usługi biblioteki dokumentów oraz usługi katalogu dystrybucyjnego.
- *Remote Work Station Support*, SC41-5402-00, udostępnia informacje dotyczące konfigurowania i używania obsługi zdalnych stacji roboczych, jak funkcji tranzytu terminalu, funkcji DHCF i zdalnych przyłączy 3270. Patrz płyta CD-ROM iSeries: Information Center Supplemental Manuals.
- Centrum informacyjne udostępnia informacje dotyczące przetwarzania zbiorów zdalnych. Opisuje sposób definiowania zbioru zdalnego w systemie zarządzania danymi rozproszonymi OS/400: jak tworzyć zbiór DDM, które programy użytkowe dla zbiorów są obsługiwane za pośrednictwem DDM oraz wymagania systemu DDM OS/400 powiązane z innymi systemami. Więcej informacji na ten temat zawiera sekcja “Informacje wstępne i pokrewne” na stronie xvi.

- W Centrum informacyjnym opisane jest, w jaki sposób skonfigurować TCP/IP i wiele protokołów TCP/IP, takich jak: FTP, SMTP i TELNET. Więcej informacji na ten temat zawiera sekcja “Informacje wstępne i pokrewne” na stronie xvi.

Szyfrowanie

- Podręcznik *Cryptographic Support/400*, SC41-3342-00 opisuje możliwości ochrony danych za pomocą programu licencjonowanego Cryptographic Facility. Wyjaśnia, jak używać tego narzędzia oraz udostępnia informacje uzupełniające dla programistów. Patrz płyta CD-ROM iSeries: Information Center Supplemental Manuals.

Ogólne operacje systemowe

- Temat ″Podstawowe operacje w systemie″ w Centrum informacyjnym udostępnia informacje dotyczące uruchamiania i zatrzymywania systemu oraz pracy z problemami. Więcej szczegółów zawiera sekcja “Informacje wstępne i pokrewne” na stronie xvi.

Instalowanie programów dostarczonych przez IBM i konfigurowanie systemu

- Podręcznik *Konfigurowanie urządzeń lokalnych*, SA12-7264-00 udostępnia informacje dotyczące początkowej konfiguracji oraz jej zmiany. Zawiera także informacje dotyczące konfigurowania urządzeń. Patrz dysk CD-ROM iSeries: Information Center Supplemental Manuals.
- Podręcznik *Instalowanie, aktualizowanie lub usuwanie systemu OS/400 i oprogramowania pokrewnego*, SA12-7263-07 udostępnia procedury przeprowadzające krok po kroku przez instalowanie początkowe, instalowanie programów licencjonowanych, poprawek PTF oraz języków dodatkowych z IBM. Patrz płyta CD-ROM iSeries: Information Center Supplemental Manuals.

Zintegrowany system plików

- Temat Systemy plików i zarządzanie w Centrum informacyjnym udostępnia przegląd zintegrowanego systemu plików, obejmujący takie tematy jak: co to jest zintegrowany system plików, jak może być używany oraz jakie interfejsy są dostępne. Więcej informacji na ten temat zawiera sekcja “Informacje wstępne i pokrewne” na stronie xvi.

Internet

- Podręcznik *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet*, SG24–4929, omawia zagadnienia dotyczące ochrony oraz ryzyko związane z podłączeniem systemu iSeries do sieci Internet. Udostępnia przykłady, zalecenia, wskazówki i techniki dla aplikacji.
- Podręcznik *iSeries and the Internet*, G325–6321, umożliwia określenie potencjalnych obaw dotyczących ochrony podczas podłączania systemu iSeries do sieci Internet. Więcej informacji na ten temat zawiera serwis WWW IBM I/T (Information Technology) Security:

  `http://www.ibm.com/security`
- Podręcznik *Cool Title About the AS/400 and Internet*, SG24-4815, pomoże zrozumieć, a następnie korzystać z sieci Internet (lub własnej sieci intranet) z poziomu systemu iSeries. Pomaga zrozumieć, jak korzystać z różnych funkcji i opcji. Ten podręcznik pomaga szybko rozpocząć pracę z pocztą elektroniczną, przesyłaniem plików, emulowaniem terminali, pracę z protokołami gopher, HTTP i terminalami 5250 to HTML Gateway.

IBM Lotus Domino

- Pod adresem URL, http://www.lotus.com/ldd/doc, można znaleźć informacje dotyczące produktów Lotus Notes, Domino i IBM Domino for iSeries. Z tego serwisu WWW można pobrać informacje w formacie bazy danych Domino (.NSF) lub w formacie Adobe Acrobat (.PDF), przeszukać bazy danych oraz dowiedzieć się, jak otrzymać wydrukowane podręczniki.

Optical Support

- *Optical Support*, SC41-5310-04, zawiera informacje dotyczące funkcji unikalnych dla produktu *Optical Support*. Zawiera także informacje pomocne przy używaniu i zrozumieniu działania urządzeń CD, bezpośrednio podłączonych urządzeń biblioteki nośników optycznych oraz podłączonych za pomocą sieci LAN. Patrz płyta CD-ROM iSeries: Information Center Supplemental Manuals.

Drukowanie

- Centrum informacyjne zawiera informacje dotyczące drukowania i związanych z nim pojęć, zbiorów drukarkowych, a także obsługi buforowania wydruków i podłączania drukarek. Więcej informacji na ten temat zawiera sekcja “Informacje wstępne i pokrewne” na stronie xvi.

Programowanie

- Podręcznik *CL Programming*, SC41-5721-06 udostępnia szerokie omówienie tematów programowania, obejmujących ogólne omówienie obiektów i bibliotek, programowania w języku CL, sterowania przepływem oraz komunikowanie się między programami, pracy z obiektami w programach CL oraz tworzenia programów CL. Inne tematy obejmują predefiniowane i improwizowane komunikaty oraz obsługę komunikatów, definiowanie i tworzenie komend i menu użytkownika, testowanie aplikacji, które obejmuje tryb debugowania, punkty zatrzymania, śledzenie i funkcje wyświetlania. Patrz dysk CD-ROM iSeries: Information Center Supplemental Manuals.
- Temat Komendy CL w Centrum informacyjnym (patrz sekcja "Informacje wstępne i pokrewne" na stronie xvi) udostępnia opis wszystkich komend CL systemu iSeries oraz związanych z nimi komend OS/400. Komendy OS/400 używane są do funkcji żądań programu licencjonowanego Operating System/400 (5738-SS1). Wszystkie komendy CL niedotyczące systemu OS/400 — te związane z innymi programami licencjonowanymi, włączając w to różne wersje językowe i programy użytkowe— opisane są i innych książkach dotyczących tych programów licencjonowanych.
- Temat Programowanie w Centrum informacyjnym udostępnia informacje dotyczące wielu języków i programów użytkowych dostępnych w systemie iSeries. Zawiera podsumowanie:
  - wszystkich komend CL systemu iSeries (w programie OS/400 i innych programach licencjonowanych), w różnych formach,
  - informacji związanych z komendami CL, takich jak komunikaty o błędach, które mogą być monitorowane przez każdą komendę, a także zbiory dostarczone przez IBM, które używane są przez niektóre komendy,
  - obiektów dostarczonych przez IBM, także bibliotek,
  - wartości systemowych dostarczonych przez IBM,
  - słów kluczowych DDS dla zbiorów fizycznych, logicznych, ekranowych, drukarkowych i ICF,
  - instrukcji REXX i funkcji wbudowanych,
  - pozostałych języków (takich jak RPG) i programów użytkowych (takich jak SEU i SDA).
- Centrum informacyjne zawiera kilka tematów dotyczących procedur zarządzania systemem i pracą w systemie iSeries. Niektóre z nich zawierają informacje na temat: danych dotyczących wydajności, zarządzania wartościami i zarządzania pamięcią. Informacje na temat Centrum informacyjnego znajdują się w sekcji "Informacje wstępne i pokrewne" na stronie xvi.
- Podręcznik *Zarządzanie pracą w systemie AS/400*, SA12-7276-03 udostępnia informacje dotyczące tworzenia i zmiany środowiska zarządzania pracą. Patrz dysk CD-ROM iSeries: Information Center Supplemental Manuals.
- Temat API w Centrum informacyjnym (patrz "Informacje wstępne i pokrewne" na stronie xvi, aby uzyskać szczegółowe informacje) zawiera informacje dotyczące tworzenia, używania i usuwania obiektów, które ułatwiają zarządzanie wydajnością systemu, efektywne używanie buforowania i obsługiwanie zbiorów baz danych. Ten podręcznik zawiera także informacje dotyczące tworzenia i obsługiwania programów dla obiektów systemowych i odtwarzania informacji OS/400, pracując z obiektami, zbiorami baz danych, zadaniami i buforowaniem.

Programy użytkowe

- Podręcznik *ADTS for AS/400: Source Entry Utility*, SC09-2605-00 udostępnia informacje dotyczące korzystania z programu narzędziowego SEU Application Development Tools do tworzenia i edytowania podzbiorów źródłowych. Książka wyjaśnia, jak rozpocząć i zakończyć sesję SEU oraz jak korzystać z wielu opcji tego pełnoekranowego edytora tekstowego. Wyjaśnia przykłady pomagające zarówno nowym jak i doświadczonym użytkownikom wykonywanie różnych zadań edycyjnych, od najprostszych komend do korzystania predefiniowanych podpowiedzi dla języków wysokiego poziomu oraz formatów danych. Patrz dysk CD-ROM iSeries: Information Center Supplemental Manuals.
- Temat DB2 Universal Database for iSeries w Centrum informacyjnym udostępnia przegląd dotyczący projektowania, pisania i uruchamiania oraz testowania instrukcji SQL/400*. Opisuje także interaktywny język SQL oraz udostępnia przykłady instrukcji SQL w programach COBOL, RPG, C, FORTRAN i PL/I. Więcej informacji na ten temat zawiera sekcja "Informacje wstępne i pokrewne" na stronie xvi.
- Temat DB2 Universal Database for iSeries w Centrum informacyjnym zawiera informacje dotyczące:
  - budowania, obsługi i uruchamiania zapytań SQL;
  - tworzenia raportów począwszy od prostych do złożonych;

– budowania, aktualizowania, zarządzania, tworzenia zapytań i raportowania dla tabel bazy danych za pomocą interfejsu opartego na formularzach;
– definiowania i sprawdzania zapytań SQL oraz raportowania w celu ich włączenia do aplikacji.

Więcej informacji na ten temat zawiera sekcja “Informacje wstępne i pokrewne” na stronie xvi.

Indeks

Znaki specjalne

A

B

C

D

E

F

G

H

I

J

K

L

Ł

M

N

O

Ó

P

Q

R

S

Ś

T

U

V

W

X

Y

Z

Ż

SC85-0124-08