System i

Bezpieczeństwo
Informacje o bezpieczeństwie

Wersja 6 wydanie 1

SC85-0124-10

System i

Bezpieczeństwo
Informacje o bezpieczeństwie

Wersja 6 wydanie 1

SC85-0124-10

Uwaga

Przed skorzystaniem z tych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje zawarte w sekcji Dodatek I, “Uwagi”, na stronie 753.

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

To wydanie zastępuje SC85-0124-09.

Spis treści

Dodatek F. Układ pozycji kroniki kontroli 581

Co nowego w wersji V6R1

Poniżej omówiono nowe lub znacznie zmienione informacje zawarte w kolekcji tematów o bezpieczeństwie.

Nowe wartości systemowe

Blokada zmiany hasła (Block Password Change - QPWDCHGBLK)
Wartość systemowa Blokada zmiany hasła (Block Password Change - QPWDCHGBLK) definiuje okres, przez który nie można zmienić hasła po uprzedniej, pomyślnie zrealizowanej operacji zmiany.

Ostrzeżenie o wygaśnięciu hasła (Password Expiration Warning - QPWDEXPWRN)
Wartość systemowa Ostrzeżenie o wygaśnięciu hasła (Password Expiration Warning - QPWDEXPWRN) określa, przez ile dni przed utratą ważności hasła system ma wyświetlać komunikaty ostrzegawcze podczas wpisywania się użytkownika.

Reguły haseł (Password rules - QPWDRULES)
Wartość systemowa Reguły hasła (Password Rules - QPWDRULES) określa reguły, na podstawie których sprawdzana jest prawidłowość konstrukcji hasła. Dla wartości systemowej QPWDRULES można podawać kilka ustawień, z wyjątkiem sytuacji, gdy poda się ustawienie *PWDSYSVAL.

Lista specyfikacji szyfrów SSL (Secure Sockets Layer (SSL) cipher specification list - QSSLCSL)
Wartość systemowa Lista specyfikacji szyfrów SSL (Secure Sockets Layer (SSL) cipher specification list - QSSLCSL) określa, jaką listę specyfikacji szyfrów będzie obsługiwał systemowy protokół SSL.

Kontrola szyfru SSL (Secure Sockets Layer cipher control - QSSLCSLCTL)
Wartość systemowa Kontrola szyfru SSL (Secure Sockets Layer cipher control - QSSLCSLCTL) określa, czy system lub użytkownik mogą sterować wartością systemową Wykaz specyfikacji szyfrów SSL (Secure Sockets Layer cipher specification list - QSSLCSL).

Protokoły SSL (Secure Sockets Layer protocols - QSSLPCL)
Wartość systemowa Protokoły SSL (Secure Sockets Layer protocols - QSSLPCL) określa obsługiwane w systemie protokoły SSL.

Znajdowanie nowych lub zmienionych informacji

Aby ułatwić określenie obszarów, w których zostały wprowadzone zmiany techniczne, w Centrum informacyjnym zastosowano:

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

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

Rozdział 1. Wprowadzenie do bezpieczeństwa platformy System i

Rodzina systemów IBM obejmuje szeroki zakres użytkowników. Rozwiązania związane z bezpieczeństwem platformy System i są wystarczająco elastyczne, aby spełnić wymagania szerokiego zakresu użytkowników i sprawdzić się w różnych sytuacjach.

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. Użytkownik musi zrozumieć dostępne funkcje i opcje, tak aby mógł je zaadoptować do własnych wymagań ochrony.

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.
- Zapewnienie wiarygodności danych.

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 kolekcji tematów opisano zalecenia dotyczące doprowadzania systemu do racjonalnego poziomu bezpieczeństwa. 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.

Informacje pokrewne

Planowanie ochrony fizycznej

Ochrona za pomocą blokady

Do sprawdzania i zmiany pozycji kluczyka służy funkcja API Odtworzenie atrybutów IPL (Retrieve IPL Attributes - QWCRIPLA) oraz komenda Zmiana atrybutów IPL (Change IPL Attributes - CHGIPLA).

Blokada na panelu sterowania modelu 940x kontroluje dostęp do różnych funkcji panelu sterowania systemu.

Blokada terminalu umożliwia zdalnemu użytkownikowi dostęp do dodatkowych funkcji dostępnych na panelu sterowania. Kontroluje, na przykład, z i do jakiego środowiska system będzie się przełączać, i5/OS lub Dedicated Service Tools (DST).

Zdalny dostęp jest kontrolowany przez wartość systemową platformy i5/OS QRMTSRVATR. 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.

Odsyłacze pokrewne

“Atrybut zdalnej usługi (QRMTSRVATR)” na stronie 40
Wartość systemowa Atrybut serwisu zdalnego (Remote Service Attribute - QRMTSRVATR) steruje funkcją zdalnej analizy problemów w systemie. Umożliwia zdalne analizowanie systemu.

Poziom bezpieczeństwa

Platforma System i oferuje pięć poziomów bezpieczeństwa. Aby system wymuszał wybrany poziom bezpieczeństwa, należy odpowiednio ustawić wartość systemową poziom bezpieczeństwa (QSECURITY).

Poziom 10:
Poziom 10 nie jest już obsługiwany.

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 bezpieczeństwa 50 jest przeznaczony dla platform System i o wysokich wymaganiach w zakresie bezpieczeństwa i opracowany został z myślą o spełnieniu wymogów bezpieczeństwa Common Criteria (CC).

Odsyłacze pokrewne

Rozdział 2, “Korzystanie z wartości systemowej Bezpieczeństwo systemu (System Security - QSecurity)”, na stronie 9
Poziomy bezpieczeństwa określa się za pomocą wartości systemowej QSECURITY.

Wartości systemowe

Wartości systemowe umożliwiają dostosowanie wielu parametrów platformy System i. Można ich użyć do zdefiniowania ustawień bezpieczeństwa w całym systemie.

Można na przykład określić następujące ustawienia:

- 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.

Pojęcia pokrewne

Rozdział 3, “Wartości systemowe związane z bezpieczeństwem”, na stronie 23
Wartości systemowe umożliwiają dostosowanie wielu charakterystyk systemu. Grupa wartości systemowych używana jest do definiowania ustawień ochrony dla systemu.

Podpisywanie

Integralność można wymusić przez podpisywanie wykorzystywanych obiektów.

Kluczowym komponentem ochrony jest *integralność*, czyli zaufanie, że obiekty w systemie nie były modyfikowane. Oprogramowanie systemu operacyjnego System i jest chronione przez podpisy cyfrowe.

Podpisywanie obiektu oprogramowania jest szczególnie ważne w przypadku, gdy obiekt został przesłany przez internet lub zapisany na nośniku, który mógł zostać zmodyfikowany. 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). Ponadto użytkownik może podpisywać własne programy (wszystkie programy licencjonowane dostarczane z systemem są podpisane).

Istnieje możliwość ograniczenia możliwości dodawania podpisów cyfrowych do bazy certyfikatów i zerowania haseł w bazie certyfikatów za pomocą funkcji API Dodanie weryfikacji (Add Verifier). Narzędzia SST udostępniają nowe opcje menu Praca z ochroną systemu (Work with system security), gdzie można ograniczyć dodawanie certyfikatów cyfrowych.

Informacje pokrewne

Używanie podpisów cyfrowych do zabezpieczenia integralności oprogramowania

Program Digital Certificate Manager

Włączenie pojedynczego wpisywania się

Pojedyncze *wpisywanie się* to proces uwierzytelniania, w którym użytkownik ma dostęp do większej liczby systemów po jednokrotnym wprowadzeniu identyfikatora i hasła. W dzisiejszych różnorodnych sieciach z systemami partycjonowanymi i wieloma platformami, administratorzy muszą radzić sobie ze złożonością zarządzania identyfikacją i uwierzytelnianiem użytkowników sieci.

Do uaktywnienia środowiska pojedynczego wpisywania się IBM udostępnia dwie współdziałające technologie, umożliwiające użytkownikom wpisywanie się przy użyciu ich nazw użytkowników i haseł w systemie Windows, w celu uwierzytelnienia na platformach System i w sieci. Jedną z tych technologii jest usługa uwierzytelniania sieciowego (Network Authentication Service - NAS), drugą odwzorowywanie tożsamości w przedsiębiorstwie (Enterprise Identity Mapping - EIM). Administrator musi je skonfigurować, aby aktywować środowisko pojedynczego wpisywania się. Do uwierzytelniania użytkowników w sieci systemy Windows 2000, Windows XP, AIX i z/OS używają protokołu Kerberos. Jednostki główne (użytkowników Kerberos) uwierzytelnia w sieci bezpieczny, centralny system nazywany centrum dystrybucji kluczy.

Usługa uwierzytelniania sieciowego (NAS) umożliwia platformie System i uczestnictwo w domenie Kerberos, natomiast technologia EIM udostępnia mechanizm łączący jednostkę główną tego protokołu Kerberos z pojedynczym identyfikatorem EIM, który reprezentuje użytkownika w całym przedsiębiorstwie. Z tym identyfikatorem EIM można powiązać inne tożsamości użytkowników, takie jak nazwa użytkownika i5/OS. Gdy użytkownik loguje się do sieci i łączy z platformą System i, nie jest pytany ani o identyfikator użytkownika, ani o hasło. Jeśli uwierzytelnienie Kerberos powiedzie się, programy mogą sprawdzić powiązanie z identyfikatorem EIM w celu odnalezienia nazwy użytkownika i5/OS. Użytkownik nie potrzebuje już hasła w celu wpisania się do platformy System i, ponieważ został uwierzytelniony przez protokół Kerberos. Administratorzy mogą centralnie zarządzać tożsamościami użytkownika za pomocą technologii EIM, natomiast użytkownicy sieci muszą zarządzać tylko jednym hasłem. Pojedyncze wpisywanie się można uaktywnić konfigurując w systemie usługi uwierzytelniania sieciowego (NAS) i odwzorowywanie tożsamości w przedsiębiorstwie (EIM).

Informacje pokrewne

Scenariusz: Tworzenie środowiska testowego pojedynczego wpisywania się

Profile użytkowników

Każdy użytkownik systemu operacyjnego i5/OS 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. Poniższa lista przedstawia kilka istotnych opcji zabezpieczających profil 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.

Pojęcia pokrewne

Rozdział 4, “Profile użytkowników”, na stronie 75
Profile użytkowników to elastyczne narzędzie o dużych możliwościach. Ich dobre zaprojektowanie może pomóc zabezpieczać system oraz dostosować go do potrzeb użytkowników.

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.

Pojęcia pokrewne

“Planowanie profili grupowych” na stronie 246
Profil grupowy jest przydatnym narzędziem, gdy kilku użytkowników ma podobne wymagania ochrony. Profile można tworzyć od razu jako profile grupowe albo zmienić na profil grupowy już istniejący profil. Używając profili grupowych można wydajniej zarządzać uprawnieniami oraz zmniejszyć liczbę pojedynczych uprawnień prywatnych dla obiektów.

“Grupowe prawo własności do obiektów” na stronie 147
Ten temat zawiera szczegółowe informacje o grupowym prawie własności do obiektów.

“Grupa podstawowa obiektu” na stronie 148
Dla obiektu można określić grupę podstawową.

“Kopiowanie profili użytkowników” na stronie 122
Profil użytkownika można utworzyć, kopiując inny profil użytkownika lub profil grupowy.

Bezpieczeństwo zasobów

Możliwość dostępu do obiektu nazywa się *uprawnieniem*. Bezpieczeństwo zasobów w systemie operacyjnym i5/OS umożliwia sterowanie uprawnieniami do obiektów. Można definiować, kto może używać danych obiektów i w jaki sposób.

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 opisano opcje bezpieczeństwa zasobów:

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

Listy autoryzacji
: Obiekty o podobnych wymaganiach bezpieczeństwa można zgrupować na jednej liście. Wówczas można będzie nadawać uprawnienia do całej 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 są zapisywane wraz 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. W celu zarządzania tym uprawnieniem można posługiwać się instrukcjami SQL.

Pojęcia pokrewne

Rozdział 5, “Bezpieczeństwo zasobów”, na stronie 135
Ten rozdział zawiera opisy poszczególnych elementów bezpieczeństwa zasobów oraz opis ich działania. Wyjaśnia także, jak używać komend CL oraz ekranów do konfigurowania ochrony zasobów.

Kronika kontroli bezpieczeństwa

Za pomocą kronik kontroli bezpieczeństwa można sprawdzać skuteczność zabezpieczeń systemu.

System operacyjny i5/OS umożliwia protokołowanie wybranych zdarzeń dotyczących bezpieczeństwa. Są one zapisywane w kronice kontroli bezpieczeństwa. Kontrolę nad tym, które zdarzenia mają być protokołowane, ma kilka wartości systemowych oraz wartości profilu użytkownika i obiektu.

Pojęcia pokrewne

Rozdział 9, “Kontrola bezpieczeństwa na platformie System i”, na stronie 265
W tej sekcji opisano techniki kontroli efektywności zabezpieczeń w systemie.

Ochrona Common Criteria

Common Criteria jest to środowisko służące do niezależnej oceny, analizy i testowania produktów w celu ustanowienia wymagań bezpieczeństwa.

W dniu 10 sierpnia 2005 roku firma IBM otrzymała certyfikację Common Criteria i5/OS V5R3M0 na poziomie Evaluated Assurance Level (EAL) 4, powiększoną o ALC_FLR.2 profilu CAPP (Controlled Access Protection Profile), Wersja 1.d, 8 października 1999 roku. Aby zamówić oceniony system, należy zamówić Common Criteria FC 1930 (numer 5722-SS1).

Z wymienionego numeru opcji powinni korzystać tylko użytkownicy muszący korzystać z konfiguracji Common Criteria.

Produkt znajduje się na stronie Validated Products List (Wykaz sprawdzonych produktów) w serwisie WWW Common Criteria Evaluation and Validation Scheme (Wartościowanie powszechnych kryteriów i schemat sprawdzania poprawności)(http://www.nsa.gov/ia/industry/niap.cfm).

Niezależna pula dyskowa

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* (iASP) oraz *niezależna pula dyskowa* są synonimami.

Niezależna pula dyskowa może być przełączalna między wieloma systemami w środowisku klastrowym lub podłączona prywatnie do pojedynczego systemu. Tak jak w wersji V5R2 zmiany funkcjonalne dotyczące niezależnych pul dyskowych mają wpływ na bezpieczeństwo 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 jest przenoszona do innego systemu, uprawnienia prywatne, prawa własności do obiektu oraz pozycje grupy podstawowej będą dołączone w systemie docelowym do profilu o tej samej nazwie. Jeśli w systemie docelowym taki profil nie istnieje, zostanie on utworzony. Użytkownik nie będzie miał żadnych uprawnień specjalnych, a jego hasło będzie miało wartość *NONE.

Niezależne pule dyskowe obsługują wiele obiektów bazujących na bibliotekach i systemów plików użytkownika. Istnieje jednak kilka obiektów, których nie można umieszczać na niezależnych pulach dyskowych. W wersji i5/OS V5R1 istnieje możliwość korzystania z niezależnych puli dyskowych wyłącznie z systemami plików użytkownika.

Informacje pokrewne

Obsługiwane i nieobsługiwane typy obiektów

Rozdział 2. Korzystanie z wartości systemowej Bezpieczeństwo systemu (System Security - QSecurity)

Poziomy bezpieczeństwa określa się za pomocą wartości systemowej QSECURITY.

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 systemu na system produkcyjny należy przeczytać odpowiednią sekcję dotyczącą migrowania z jednego poziomu ochrony na inny.

Poziomy bezpieczeństwa

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 bezpieczeństwa 40” na stronie 14.

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 bezpieczeństwa: 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]

Tabela 1. Poziomy bezpieczeństwa: porównanie funkcji (kontynuacja)

Funkcja	Poziom 20	Poziom 30	Poziom 40	Poziom 50
Aktywna obsługa ograniczenia możliwości.	Tak	Tak	Tak	Tak
Aktywna ochrona zasobów.	Nie	Tak	Tak	Tak
Dostęp do wszystkich obiektów.	Tak	Nie	Nie	Nie
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
Rozszerzona sprzętowa ochrona pamięci jest wymuszana dla wszystkich 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
Przestrzeń powiązana z programem nie może być modyfikowana bezpośrednio.	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 “Zabezpieczenie przed modyfikowaniem wewnętrznych bloków sterujących” na stronie 21.

Domyślne uprawnienia specjalne

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.

Za pomocą komendy CHGSYSVAL można uniemożliwić użytkownikom posiadającym uprawnienia *SECADM oraz *ALLOBJ zmianę pokrewnych wartości systemowych. 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 związanych z bezpieczeństwem oraz pełną listę tych wartości zawiera temat Wartości systemowe dotyczące bezpieczeństwa.

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

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

	Klasy użytkowników				
Uprawnienia	***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 81 i “Uprawnienia specjalne” na stronie 87.

Uwagi

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.

Użytkownicy na poziomie bezpieczeństwa 30 (i poniżej) mogą wywoływać interfejsy systemowe wymieniające profil użytkownika na QSECOFR lub umożliwiające użytkownikom dostęp do zasobów, które nie są normalnie dostępne. Na poziomie bezpieczeństwa 40 użytkownicy nie mogą bezpośrednio wywoływać tych interfejsów. Dlatego zalecany jest poziom bezpieczeństwa 40 lub wyższy.

Poziom ochrony 40 udostępnia dodatkowe zabezpieczenie integralności bez wpływania na wydajność systemu. Aplikacje niedziałające na poziomie ochrony 40 mają negatywny wpływ na wydajność systemu 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 bezpieczeństwa 50, może być zauważalne pogorszenie wydajności, spowodowane dodatkową kontrolą wykonywaną 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 od samego początku z poziomu bezpieczeństwa 30 umożliwia elastyczne zabezpieczenie pewnych zasobów krytycznych bez konieczności ponownego testowania wszystkich aplikacji.

Pojęcia pokrewne

"Poziom bezpieczeństwa" na stronie 2
Platforma System i oferuje pięć poziomów bezpieczeństwa. Aby system wymuszał wybrany poziom bezpieczeństwa, należy odpowiednio ustawić wartość systemową poziom bezpieczeństwa (QSECURITY).

Zadania pokrewne

"Wyłączanie poziomu bezpieczeństwa 50" na stronie 22
Po zmianie poziomu bezpieczeństwa na poziom 50, może się okazać, że istnieje potrzeba tymczasowego powrotu na poziom bezpieczeństwa 30 lub 40. Na przykład, może zaistnieć konieczność przetestowania nowych aplikacji pod kątem błędów integralności; mogą również wystąpić problemy z integralnością, które nie pojawiają się na niższych poziomach bezpieczeństwa.

Poziom bezpieczeństwa 10

Na poziomie bezpieczeństwa 10 nie ma żadnej ochrony bezpieczeństwa. Dlatego poziom ten nie jest zalecany.

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, "Profile użytkowników IBM", na stronie 329 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 otrzymują uprawnienie specjalne *ALLOBJ, użytkownicy mogą przejść przez każde sprawdzenie uprawnień i uzyskać 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 bezpieczeństwa 20

Poziom bezpieczeństwa 20 udostępnia więcej funkcji zabezpieczeń niż poziom 10. Jednak na tym poziomie wszystkie profile są tworzone domyślnie z uprawnieniem specjalnym *ALLOBJ, dlatego również nie jest on zalecany.

Poziom bezpieczeństwa 20 udostępnia następujące funkcje zabezpieczeń:

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

Zmienianie na poziom 20 z poziomu 10

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

Jeśli planowana jest zmiana poziomu ochrony z 10 na 20 w systemie produkcyjnym, warto rozważyć wykonanie następującej listy działań:

- 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 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 “Wartości domyślne dla profili użytkowników” na stronie 329, patrz Dodatek B, “Profile użytkowników IBM”, na stronie 329, w celu dokonania zmian w profilach automatycznie utworzonych na poziomie ochrony 10.

Zmiana na poziom 20 z poziomu wyższego

Podczas zmiany z wyższego poziomu bezpieczeństwa na poziom 20 do profili użytkowników dodawane są uprawnienia specjalne. Po wprowadzeniu takiej zmiany użytkownik ma przynajmniej domyślne uprawnienia specjalne dla klasy użytkownika.

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

Tabela 2 na stronie 11 opisuje różnice w uprawnieniach specjalnych miedzy poziomem 20 a wyższymi.

Poziom bezpieczeństwa 30

Poziom bezpieczeństwa 30 udostępnia więcej funkcji zabezpieczeń, niż poziom 20.

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.

Zmiana na poziom 30 z poziomu niższego

Gdy zmieniany jest poziom bezpieczeństwa z niższego poziomu na poziom 30, system zmienia wszystkie profile użytkowników, aby zaktualizować uprawnienia specjalne podczas następnego IPL.

Uprawnienia specjalne, które użytkownik otrzymał na poziomie 10 lub 20, lecz nie posiadał na 30 i wyższych, 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 11 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. Należy rozważyć wykonanie następujących 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 profili użytkowników używanych 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 przy użyciu profili testowych, wszystkim produkcyjnym profilom użytkowników, które mają mieć dostęp do aplikacji, należy nadać odpowiednie uprawnienia do obiektów aplikacji,
- jeśli wartość systemowa QLMTSECOFR (ograniczanie dostępu dla osoby odpowiedzialnej za bezpieczeństwo) ma wartość 1 (tak), użytkownicy z uprawnieniami specjalnymi *ALLOBJ lub *SERVICE muszą być autoryzowani do korzystania z urządzeń; tym użytkownikom można nadać uprawnienia *CHANGE do wybranych urządzeń, użytkownikowi QSECOFR uprawnienia *CHANGE do urządzeń 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.

Odsyłacze pokrewne

"Definiowanie sposobów dostępu do informacji" na stronie 136
Użytkownik może zdefiniować, które operacje mogą być wykonywane na obiektach, danych i polach.

Poziom bezpieczeństwa 40

Poziom bezpieczeństwa 40 zapobiega potencjalnym zagrożeniom naruszenia integralności lub ochrony ze strony programów, które mogą obchodzić ochronę w szczególnych przypadkach. Poziom bezpieczeństwa 50 udostępnia rozszerzone zabezpieczenie integralności dla instalacji ze ścisłymi wymaganiami ochrony.

Tabela 3 opisuje porównanie obsługi funkcji na poziomach 30, 40 i 50.

Tabela 3. Porównanie poziomów bezpieczeństwa 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]; operacja nie powiodła się.	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 (program o stanie *USER) próbuje zapisać dane w systemowym obszarze dysku, który zdefiniowany został jako tylko do odczytu lub niedostępny.	Próba ta może się powieść.	Pozycja kroniki AF; [1] operacja nie powiodła się.	Pozycja kroniki AF; [1] operacja nie powiodła się.
Przeprowadzona została próba odtworzenia programu, który nie ma wartości sprawdzania. [2]	Sprawdzanie nie jest przeprowadzane. Program musi być przekonwertowany przed użyciem.	Sprawdzanie nie jest przeprowadzane. Program musi być przekonwertowany przed użyciem.	Sprawdzanie nie jest przeprowadzane. Program musi być przekonwertowany przed użyciem.

Tabela 3. Porównanie poziomów bezpieczeństwa 30, 40 i 50 (kontynuacja)

Opis scenariusza	Poziom 30	Poziom 40	Poziom 50
Przeprowadzona została próba odtworzenia programu, który ma wartość sprawdzania.	Przeprowadzane jest sprawdzanie programu.	Przeprowadzane jest sprawdzanie programu.	Przeprowadzane jest sprawdzanie programu.
Podjęta została próba zmiany przestrzeni powiązanej z programem.	Próba udaje się.	Pozycja kroniki AF; [1] operacja nie powiodła się.	Pozycja kroniki AF; [1] operacja nie powiodła się.
Podjęta została próba zmiany przestrzeni adresowej zadania.	Próba udaje się.	Pozycja kroniki AF; [1] operacja nie powiodła się.	Pozycja kroniki AF; [1] operacja nie powiodła się.
Program użytkownika próbuje wywołać lub przenieść sterowanie do programu domeny systemu.	Próba udaje się.	Pozycja kroniki AF; [1] operacja nie powiodła się.	Pozycja kroniki AF; [1] operacja nie powiodła się.
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 nad nim na stosie wywołań.	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, 3] operacja nie powiodła się.[3]	Pozycja kroniki AF;[1, 3] operacja nie powiodła się.[3]

[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, “Kontrola bezpieczeństwa na platformie System i”, na stronie 265.

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

[3] 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 na stronie 14, 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 korzystaniu z nieobsługiwanych interfejsów

Na poziomie bezpieczeństwa 40 lub wyższym system nie zezwala na bezpośrednie wywołania tych programów systemowych, które nie zostały udokumentowane jako interfejsy z poziomem wywołania.

Na przykład bezpośrednie wywołanie programu przetwarzania komendy dla programu SIGNOFF nie powiedzie się.

Aby zapewnić ten rodzaj ochrony, system korzysta z atrybutów domeny obiektu i atrybutów 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 w domenie *SYSTEM można osiągnąć za pomocą odpowiedniej komendy lub interfejsu API. Stany *SYSTEM i *INHERIT zarezerwowane są dla programów IBM.

  Stan programu można wyświetlić komendą Wyświetlenie programu (Display Program - DSPPGM). Stan programu usługowego można wyświetlić komendą 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:

Gdy spełnione zostaną poniższe warunki, w kronice QAUDJRN tworzona jest pozycja błędu uprawnień (AF) lub naruszenia typu D bądź R:

- Funkcja kontroli jest aktywna.
- Wartość systemowa QAUDLVL obejmuje *PGMFAIL.
- Nastąpiła próba wykorzystania nieobsługiwanego interfejsu.

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 z tym profilem użytkownika. Oznacza to, że zadanie wprowadzone przez nieuprawnionego użytkownika może zostać uruchomione za pomocą profilu użytkownika podanego w opisie zadania.

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

Pozycja kroniki:

Jeśli są spełnione następujące warunki, w kronice kontroli QAUDJRN zapisywana jest pozycja AF typ naruszenia J.

- funkcja kontroli jest aktywna;
- wartość systemowa QAUDLVL obejmuje wartość *AUTFAIL;
- użytkownik wprowadzania zadanie, nie mając uprawnienia profilu użytkownika określonego w opisie zadania.

Wpisywanie się bez identyfikatora użytkownika oraz hasła

Ustawiony poziom bezpieczeństwa określa sposób kontrolowania przez system czynności wpisywania się bez identyfikatora użytkownika oraz 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.

Pozycja kroniki:

Gdy spełnione zostaną następujące warunki, w kronice QAUDJRN tworzony jest wpis błędu uprawnień (AF) lub naruszenie typu S.

- Funkcja kontroli jest aktywna
- wartość systemowa QAUDLVL obejmuje wartość *AUTFAIL
- Użytkownik próbuje wpisać się bez wprowadzania ID użytkownika, a opis podsystemu na to zezwala.

Należy pamiętać, że taka próba zakończy się niepowodzeniam, jeśli poziom bezpieczeństwa wynosi 40 lub więcej.

Pojęcia pokrewne

"Opisy podsystemów" na stronie 211
Opisy podsystemów pełnią różne funkcje w systemie.

Rozszerzona sprzętowa ochrona pamięci masowej

Rozszerzona sprzętowa ochrona pamięci masowej zezwala na istnienie bloków informacji systemowych, zlokalizowanych w pamięci, o atrybutach dozwolonego zapisu i odczytu, tylko do odczytu, lub braku dostępu.

Na poziomie ochrony 40 i wyższym system steruje sposobem, w jaki programy użytkownika (*USER) uzyskują dostęp do tych zabezpieczonych bloków.

Rozszerzoną sprzętową ochronę pamięci masowej obsługują wszystkie modele System i.

Pozycja kroniki:

Gdy spełnione zostaną następujące warunki, w kronice QAUDJRN tworzony jest wpis błędu uprawnień (AF) lub naruszenie typu R.

- Funkcja kontroli jest aktywna
- Wartość systemowa QAUDLVL obejmuje *PGMFAIL.
- Program próbuje zapisać do obszaru pamięci, który jest chroniony przez funkcję sprzętowej ochrony pamięci masowej.

Ochrona przestrzeni związanej z programem

W przypadku programów pierwotnego modelu oprogramowania (OPM) na poziomie ochrony 40 i wyższym program użytkownika nie może bezpośrednio zmieniać związanej przestrzeni obiektu programu. W przypadku programów zintegrowanego środowiska językowego (ILE) program użytkownika nie może bezpośrednio zmieniać związanej przestrzeni obiektu programu na żadnym poziomie ochrony.

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 poprawności parametrów

Interfejsy do systemu operacyjnego i5/OS to programy systemowe w domenie 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. System musi oddzielić domenę użytkownika od domeny systemowej oraz spełniać wymagania poziomu ochrony Common Criteria. Dodatkowe sprawdzanie może nieznacznie pogorszyć wydajność.

Sprawdzanie poprawności odtwarzanych programów

W momencie tworzenia programu system oblicza wartość sprawdzania, która przechowywana jest w programie. Podczas odtwarzania programu ta wartość jest obliczana ponownie i porównywana z wartością sprawdzania przechowywaną w programie.

W przypadku niezgodności wartości sprawdzania system podejmuje działania zgodnie z ustawieniami wartości systemowych Wymuszenie konwersji przy odtwarzaniu (Force Conversion on Restore - QFRCCVNRST) i Umożliwienie odtwarzania obiektu (Allow Object Restore - 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, Weryfikowanie obiektu przy odtwarzaniu (QVFYOBJRST), QFRCCVNRST i QALWOBJRST, działają jako serie filtrów służących do określenia, czy program będzie odtwarzany bez zmian, ponownie tworzony (konwertowany) po odtworzeniu lub czy nie będzie odtworzony w systemie.

Uwaga: Programy systemowe muszą mieć poprawny podpis cyfrowy. W przeciwnym razie nie mogą być odtworzone, niezależnie od ustawień wartości systemowych.

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, do wartości systemowej QALWOBJRST, tylko wtedy, gdy przejdą przez pierwsze dwa filtry. Ta wartość systemowa kontroluje, czy obiekty z atrybutami ochrony mogą być odtwarzane.

Uwagi:

1. Programy tworzone dla systemu i5/OS mogą zawierać informacje, które umożliwiają ponowne tworzenie programu podczas odtwarzania, bez konieczności dostarczenia kodu źródłowego programu.
2. Programy utworzone dla systemu i5/OS w wersji 5 wydanie 1 i nowszych zawierają informacje wymagane podczas ponownego tworzenia, nawet jeśli obserwowalność programu została usunięta.
3. Programy utworzone dla wydań wcześniejszych niż wersja 5, wydanie 1 mogą być ponownie tworzone podczas operacji odtwarzania, jeśli obserwowalność tych programów nie została usunięta.

Odsyłacze pokrewne

“Wartości systemowe związane z ochroną” na stronie 37
W temacie omówiono wartości systemowe związane z bezpieczeństwem w systemie operacyjnym i5/OS.

Zmienianie na poziom bezpieczeństwa 40

Przed przejściem na poziom bezpieczeństwa 40 należy upewnić się, że wszystkie aplikacje można pomyślnie uruchomić na poziomie 30. Poziom bezpieczeństwa 30 umożliwia testowanie ochrony zasobów dla wszystkich aplikacji.

W celu przejścia na poziom bezpieczeństwa 40 należy wykonać następującą procedurę:

1. Jeśli jeszcze tego nie zrobiono, należy aktywować funkcję kontroli ochrony. Temat “Konfigurowanie kontroli bezpieczeństwa” na stronie 300 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 dowolnych aplikacji na poziomie bezpieczeństwa 30 monitoruj kronikę kontroli w poszukiwaniu pozycji *AUTFAIL i *PGMFAIL. Zwróć szczególną uwagę na następujące kody przyczyny w pozycjach typu AF:

   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 poprawności odtwarzanych programów” na stronie 18.

   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 bezpieczeństwa 40

Może się okazać, że istnieje potrzeba przejścia z poziomu 30 na poziom 40 przy testach nowych aplikacji pod kątem problemów z z integralnością. Może się również okazać, że przed przejściem na poziom bezpieczeństwa 40 aplikacja nie została wystarczająco przetestowana.

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.

Ważne: Przy przejściu z poziomu 40 na poziom 20, do wszystkich profili użytkowników dodawane są pewne uprawnienia specjalne. (Patrz Tabela 2 na stronie 11.) Takie działanie usuwa ochronę bezpieczeństwa zasobów.

Poziom bezpieczeństwa 50

Poziom bezpieczeństwa 50 zaprojektowano w celu spełnienia niektórych wymagań zdefiniowanych w profilu Controlled Access Protection Profile (CAPP) dla zgodności z Common Criteria (CC). Udostępnia on zaawansowane zabezpieczenie integralności, oprócz tego, które zapewnia poziom bezpieczeństwa 40, dla instalacji ze ścisłymi wymogami bezpieczeństwa.

Funkcje zabezpieczeń włączone do poziomu bezpieczeństwa 50 zostały opisane 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 z domeny użytkownika

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

Następujące typy obiektów mogą znajdować się w domenie systemowej lub domenie 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, użytkownikowi nie należy zezwalać na przysyłanie informacji dotyczących ochrony do innych użytkowników, jeśli nie ma możliwości zapisania 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 25.

Zadania pokrewne

“Zmiana na poziom bezpieczeństwa 50” na stronie 21
Jeśli bieżącym poziomem bezpieczeństwa jest 10 lub 20, należy przed wykonaniem zmiany poziomu na 50 zmienić poziom bezpieczeństwa na 40. Jeśli bieżącym poziomem bezpieczeństwa jest 30 lub 40, należy ocenić wartość QALWUSRDMN i rekompilować niektóre programy w celu przygotowania do poziomu bezpieczeństwa 50.

Ograniczanie obsługi komunikatu

Komunikaty wysyłane między programami stanowią potencjalne ryzyko naruszające integralność.

Na poziomie bezpieczeństwa 50, można ograniczyć komunikaty przesyłane między programami, aby zabezpieczyć integralność systemu.

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 wywołań, 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.

Zabezpieczenie przed modyfikowaniem wewnętrznych bloków sterujących

Na poziomie bezpieczeństwa 40 i 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.

Zmiana na poziom bezpieczeństwa 50

Jeśli bieżącym poziomem bezpieczeństwa jest 10 lub 20, należy przed wykonaniem zmiany poziomu na 50 zmienić poziom bezpieczeństwa na 40. Jeśli bieżącym poziomem bezpieczeństwa jest 30 lub 40, należy ocenić wartość QALWUSRDMN i rekompilować niektóre programy w celu przygotowania do poziomu bezpieczeństwa 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 na poziom bezpieczeństwa 40” na stronie 18 w celu przygotowania systemu na zmianę poziomu ochrony.

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

- należy ocenić wartość systemową QALWUSRDMN; kontrolowanie obiektów domeny użytkownika jest ważne dla integralności systemu;
- 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,
- Należy rekompilować wszelkie programy RPG* środowiska RPG/400 lub System/38 korzystające ze zbiorów ekranowych, jeśli zostały one skompilowane za pomocą kompilatora w wersji wcześniejszej niż V2R2.

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.

Pojęcia pokrewne

“Ograniczanie obiektów z domeny użytkownika” na stronie 20
Większość obiektów tworzonych jest w domenie systemowej. Gdy system uruchamiany jest na poziomie ochrony 40 lub 50, dostęp do obiektów z domeny systemowej może odbywać się jedynie za pomocą udostępnionych komend i funkcji API.

Wyłączanie poziomu bezpieczeństwa 50

Po zmianie poziomu bezpieczeństwa na poziom 50, może się okazać, że istnieje potrzeba tymczasowego powrotu na poziom bezpieczeństwa 30 lub 40. Na przykład, może zaistnieć konieczność przetestowania nowych aplikacji pod kątem błędów integralności; mogą również wystąpić problemy z integralnością, które nie pojawiają się na niższych poziomach bezpieczeństwa.

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.

Ważne: Przy przejściu z poziomu 50 na poziom 20, do wszystkich profili użytkowników dodawane są pewne uprawnienia specjalne. Powoduje to usunięcie zabezpieczenia ochrony zasobów.

Odsyłacze pokrewne

Rozdział 2, “Korzystanie z wartości systemowej Bezpieczeństwo systemu (System Security - QSecurity)”, na stronie 9
Poziomy bezpieczeństwa określa się za pomocą wartości systemowej QSECURITY.

Rozdział 3. Wartości systemowe związane z bezpieczeństwem

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 ładowania programu początkowego (IPL).

Opcją blokowania można ograniczyć dostęp do następujących wartości systemowych:

Tabela 5. Wartości systemowe, które można zablokować

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

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: Aby zablokować lub odblokować wartości systemowe dotyczące ochrony, konieczne jest posiadanie przez użytkownika ID użytkownika i hasła narzędzi systemowych.

1. Uruchom interfejs znakowy.
2. W wierszu komend wpisz STRSST.
3. Podaj swój ID użytkownika i hasło narzędzi systemowych.
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. Zaloguj się do narzędzi DST za pomocą swojego ID użytkownika i hasła.
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.

Pojęcia pokrewne

"Wartości systemowe" na stronie 3
Wartości systemowe umożliwiają dostosowanie wielu parametrów platformy System i. Można ich użyć do zdefiniowania ustawień bezpieczeństwa w całym systemie.

Wartości systemowe ochrony ogólnej

Ten rozdział zawiera podstawowe informacje na temat ogólnych wartości systemowych, które są używane do kontrolowania bezpieczeństwa w systemie operacyjnym i5/OS.

Przegląd:

Ogólne wartości systemowe związane z bezpieczeństwem umożliwiają ustawienie funkcji zabezpieczeń, które wspomagają podejmowanie decyzji podczas tworzenia strategii bezpieczeństwa. Na przykład strategia bezpieczeństwa może określać, że systemy zawierające informacje poufne, takie jak konta klientów lub listy płac wymagają wyższego poziomu zabezpieczeń niż systemy używane do testowania aplikacji opracowanych w ramach działalności przedsiębiorstwa. Można następnie zaplanować i ustawić w tych systemach poziom bezpieczeństwa odpowiadający decyzjom, które zostały podjęte podczas tworzenia strategii bezpieczeństwa.

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).

Ogólne wartości systemowe, które sterują bezpieczeństwem systemu, są następujące:

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 osoby odpowiedzialnej za bezpieczeństwo

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.

Udostępnienie obiektów domeny użytkownika (QALWUSRDMN)

Podczas tworzenia, każdy obiekt otrzymuje atrybut domeny. Domena to charakterystyka obiektu. Określa, które programy mają dostęp do tego obiektu. Wartość systemowa Dopuszczanie obiektów z domeny użytkownika (Allow user domain objects - QALWUSRDMN) określa biblioteki, które mogą zawierać obiekty z domeny użytkownika typu *USRSPC, *USRIDX i *USRQ.

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. Ograniczenie to nie obowiązuje wobec obiektów z domeny użytkownika typu ″program″ (*PGM), ″program serwerowy″ (*SRVPGM) oraz ″pakiety SQL″ (*SQLPKG).

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Patrz Wartości systemowe dotyczące bezpieczeństwa, gdzie podano szczegółowe informacje o sposobach ograniczania uprawnień do modyfikowania wartości systemowych związanych z bezpieczeństwem, a także pełny wykaz ograniczonych wartości systemowych.

Tabela 6. Dozwolone wartości dla wartości systemowej QALWUSRDMN:

***ALL**	Obiekty domeny użytkownika mogą znajdować się we wszystkich bibliotekach i katalogach systemu. Jest to wartość początkowo ustawiona w systemie.
***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.

Wartość zalecana: w przypadku większości systemów zaleca się wartość *ALL. Jeśli system ma wysokie wymagania ochrony, obiekty domeny użytkownika powinny być ograniczone jedynie do biblioteki QTEMP.

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 posługiwać się interfejsem MI w celu niekontrolowanego odczytu lub zmiany danych w obiektach z 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 z 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 Uprawnienia do nowych obiektów (Authority for New Objects - QCRTAUT) określa uprawnienia publiczne dla obiektu nowo tworzonego.

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. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących bezpieczeństwa i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe związane z bezpieczeństwem.

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.

Wartość zalecana:
*CHANGE

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

Ważne: 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 Wyświetlenie inform. wpisania (Display Sign-On Information - QDSPSGNINF) określa, czy po wpisaniu się do systemu wyświetli się ekran Informacji wpisania.

Ekran Informacje wpisania się (Sign-on Information) zawiera:

- datę ostatniego wpisania się,
- Jakiekolwiek nieważne kontrole poprawności hasła
- Ilość dni, po których upływie hasło straci ważność (jeśli hasło ma wygasnąć w przeciągu okresu dni ostrzeżeń hasła (QPWDEXPWRN)))

```
                          Informacje wpisania
                                                          System:
Poprzednie wpisanie . . . . . . . . . . . . . :   10/30/91  14:15:00

Nieważne kontrole poprawności haseł . . . . . :   3

Ilość dni pozostałych do wygaśnięcia hasła  . . . . . . . :   5
```

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Więcej informacji na temat ograniczania zmian wartości systemowych, oraz pełna lista ograniczonych wartości systemowych, znajduje się w publikacji Wartości systemowe związane z bezpieczeństwem.

Tabela 8. Dozwolone wartości dla wartości systemowej QDSPSGNINF:

0	Ekran nie jest wyświetlany.
1	Ekran jest wyświetlany.

Zalecana wartość: Zaleca się stosowanie 1 (Ekran jest wyświetlany), ponieważ użytkownicy mogą monitorować próby dostępu do ich profili, a także wiedzą, kiedy należy zmienić hasło.

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

Interwał czasu nieaktywności zadania (QINACTITV)

Wartość systemowa Interwał czasu nieaktywności zadania (QINACTITV) określa w minutach, jak długo system zezwala na pozostawienie nieaktywnego zadania przed podjęciem działania.

Jeśli stacja robocza posiada status DSPW, lub oczekuje na komunikat bez ingerencji użytkownika, to uznawana jest za nieaktywną. Przykład ingerencji użytkownika

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

Obejmuje to także sesje emulacji programu System i Access. Wykluczone są zadania lokalne, które wpisane zostały w systemie zdalnym. Wykluczone są także zadania połączone za pomocą protokołu FTP. 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).

Poniższe przykłady przedstawiają, 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 System i Access może być dla systemu nieaktywne, jeśli użytkownik używa funkcji komputera PC, na przykład takich jak edycja dokumentu, bez interakcji z systemem.

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 Kolejka komunikatów nieaktywnego zadania (QINACTMSGQ) określa, jakie działanie podejmuje system, gdy dla zadania zostanie przekroczony interwał czasu nieaktywnego zadania.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Więcej szczegółowych informacji na temat ograniczania zmian wartości systemowych związanych z bezpieczeństwem wraz z pełną listą zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe dotyczące bezpieczeństwa.

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 39. **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.

Tabela 10. Możliwe wartości dla wartości systemowej QINACTMSGQ: (kontynuacja)

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] W temacie Zarządzanie pracą opisano zadania grupowe i zadania alternatywne.	

Zalecana wartość: *DSCJOB, chyba że użytkownicy uruchamiają zadania programu System i Access. Użycie wartości *DSCJOB gdy uruchomione są zadania programu System i Access jest równoznaczne z ich zakończeniem. Może to powodować znaczną utratę informacji. Jeśli zainstalowano program licencjonowany System i Access, należy użyć opcji *kolejka-komunikatów*. W temacie Programowanie w języku CL znajduje się przykład pisania programu obsługującego komunikaty.

Używanie kolejki komunikatów: Użytkownik lub program może monitorować kolejkę komunikatów i podjąć odpowiednie działania, takie jak zakończenie zadania lub wysłanie 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. Metoda ta jest zalecana w przypadku korzystania z programu licencjonowanego System i 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 Ograniczenie sesji urządzeń (Limit Device Sessions - QLMTDEVSSN) określa, czy liczba sesji
| urządzeń dopuszczalnych dla użytkownika jest ograniczona.

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. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących ochrony i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe dotyczące ochrony.

Tabela 11. Możliwe wartości dla wartości systemowej QLMTDEVSSN:

0	Limit sesji urządzeń dla użytkownika nie jest ograniczony do określonej liczby.
1	Limit sesji urządzeń dla użytkownika jest ograniczony do 1.
2 - 9	Limit sesji urządzeń dla użytkownika jest ograniczony do określonej liczby.

Zalecana wartość: zalecana jest wartość 1 (tak), ponieważ nałożenie na użytkowników ograniczenie do pojedynczego urządzenia zmniejsza prawdopodobieństwo współużytkowania haseł lub pozostawiania nienadzorowanych urządzeń.

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

Ograniczanie dostępu dla osoby odpowiedzialnej za bezpieczeństwo (QLMTSECOFR)

Wartość systemowa Ograniczanie dostępu dla osoby odpowiedzialnej za bezpieczeństwo (Limit Security Officer - 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 207.

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. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących ochrony i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe dotyczące ochrony.

Tabela 12. Możliwe wartości dla wartości systemowej QLMTSECOFR:

1	Użytkownik posiadający uprawnienia specjalne *ALLOBJ lub *SERVICE może wpisać się na stacji roboczej tylko w przypadku, gdy został do tego jawnie uprawniony (tj. otrzymał uprawnienie *CHANGE), lub jeśli jego profil QSECOFR posiada uprawnienie *CHANGE dla danej stacji roboczej. Te uprawnienia nie mogą pochodzić z uprawnień publicznych.
0	Użytkownicy z uprawnieniami specjalnymi *ALLOBJ lub *SERVICE mogą wpisywać się na każdą stację roboczą, na której posiadają uprawnienie *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 Maksymalna liczba prób wpisania się (Maximum Sign-On Attempts - QMAXSIGN), ile niepoprawnych prób prób wpisania się lub weryfikacji haseł mogą wykonać pod rząd użytkownicy lokalni i zdalni.

Niepoprawne próby wpisania się lub weryfikacji hasła spowodowane są podaniem niepoprawnego ID użytkownika, niepoprawnego hasła lub brakiem odpowiednich uprawnień do korzystania ze stacji roboczej.

Gdy limit prób wpisania się lub weryfikacji hasła zostanie wyczerpany, podejmowane są odpowiednie działania określane na podstawie wartości systemowej QMAXSGNACN. Komunikat CPF1393 wysyłany jest do kolejki komunikatów QSYSOPR (oraz do kolejki komunikatów QSYSMSG, jeśli istnieje ona w bibliotece QSYS), w celu powiadomienia szefa bezpieczeństwa o możliwym naruszeniu systemu.

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. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących ochrony i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe dotyczące ochrony.

Tabela 13. Możliwe wartości dla wartości systemowej QMAXSIGN:

3	Użytkownik ma maksymalnie 3 próby wpisania się lub weryfikacji hasła.
***NOMAX**	Liczba nieudanych prób wpisania się lub weryfikacji hasła jest nieograniczona. Daje to potencjalnemu intruzowi nieograniczoną liczbę szans odgadnięcia poprawnej kombinacji identyfikatora i hasła użytkownika.
ograniczenie	Należy podać wartość z zakresu od 1 do 25. Zalecaną liczbą prób wpisania się lub weryfikacji hasła jest trzy. Taka liczba prób jest zazwyczaj wystarczająca do poprawienia błędów w pisowni i jednocześnie zabezpiecza przed dostępem użytkowników bez uprawnień.

Zalecana wartość: 3

Działanie podejmowane po przekroczeniu limitu prób wpisania się (QMAXSGNACN)

Wartość systemowa Działanie po przekroczeniu limitu prób wpisania się (Action When Sign-On Attempts Reached - QMAXSGNACN) określa, jakie działanie zostanie podjęte przez system po osiągnięciu limitu prób weryfikacji wpisania się do danej stacji roboczej lub weryfikacji hasła.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących bezpieczeństwa i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe związane z bezpieczeństwem.

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 lub poprawna weryfikacja hasła powoduje wyzerowanie licznika nieudanych prób wpisania się w profilu 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 30.

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 Zachowywanie bezpieczeństwa serwera (Retain Server Security - QRETSVRSEC) określa, czy możliwe do odszyfrowania informacje o uwierzytelnianiu powiązane z profilem użytkownika lub pozycjami listy sprawdzania (*VLDL) można zachowywać w systemie hosta. Nie obejmuje to hasła profilu użytkownika systemu System i.

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 można usunąć z systemu, ustawiając wartość systemową QRETSVRSEC na 0 i uruchamiając komendę Usuwanie danych o bezpieczeństwie serwera (Clear Server Security Data - CLRSVRSEC). Jeśli w systemie istnieje wiele profili użytkownika lub list sprawdzania, to uruchomienie komendy CLRSVRSEC może zająć dużo czasu.

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. Patrz Wartości systemowe dotyczące bezpieczeństwa, gdzie podano szczegółowe informacje o sposobach ograniczania uprawnień do modyfikowania wartości systemowych związanych z bezpieczeństwem, a także pełny wykaz ograniczonych wartości systemowych.

Tabela 15. Dozwolone wartości dla wartości systemowej QRETSVRSEC:

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

Zalecana wartość: 0

Pojęcia pokrewne

“Korzystanie z list sprawdzania” na stronie 250
Obiekty listy sprawdzania dają aplikacjom możliwość bezpiecznego składowania informacji uwierzytelniających użytkowników.

Zdalne włączanie zasilania i restartowanie (Remote power-on and restart - QRMTIPL)

Jednym z elementów tworzenia planu bezpieczeństwa systemu jest decyzja, czy zezwalać użytkownikom zdalnym na włączanie zasilania i restartowanie systemu. Wartość systemowa Zdalne włączanie zasilania i restartowanie (Remote power-on and restart - QRMTIPL) umożliwia uruchomienie systemu zdalnego za pomocą telefonu i modemu albo sygnału SPCN.

Ustawienie tej wartości systemowej na 1 (Tak) oznacza, że każde połączenie telefoniczne spowoduje restart systemu. Chociaż wartość systemowa QRMTIPL dotyczy opcji restartowania systemu, rodzi konsekwencje istotne dla bezpieczeństwa. Nie można oczywiście dopuścić do tego, aby ktoś przypadkowo restartował systemy. Jeśli jednak stosuje się system zdalny do celów administracji, to trzeba umożliwić restartowanie zdalne.

Tabela 16. Dozwolone wartości wartości systemowej Zdalne włączanie zasilania i restartowanie (Remote power-on and restart - QRMTIPL):

0	Zdalne włączanie zasilania i restartowanie jest niedozwolone.
1	Zdalne włączanie zasilania i restartowanie jest dozwolone.

Informacje pokrewne

Wartości systemowe restartowania: umożliwienie zdalnego włączania zasilania i restartowania

Kontrola zdalnego wpisywania się (QRMTSIGN)

Wartość systemowa Sterowanie zdalnym wpisywaniem się (Remote Sign-On Control - QRMTSIGN) określa sposób, w jaki system obsługuje zdalne żądania wpisania się.

Przykładami zdalnego wpisania się jest tranzyt terminalu z innego systemu, funkcja stacji roboczej programu licencjonowanego System i oraz dostęp w sesji TELNET.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Patrz Wartości systemowe dotyczące bezpieczeństwa, gdzie podano szczegółowe informacje o sposobach ograniczania uprawnień do modyfikowania wartości systemowych związanych z bezpieczeństwem, a także pełny wykaz ograniczonych wartości systemowych.

Tabela 17. Dozwolone wartości dla wartości systemowej QRMTSIGN:

***FRCSIGNON**	Żądania zdalnego wpisania się będą podlegać zwykłej procedurze wpisywania się.
***SAMEPRF**	Jeśli źródłowa i docelowa nazwa profilu użytkownika są takie same i zgłoszono automatyczne wpisanie się, można pominąć ekran wpisywania. 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. Ta wartość jest zalecana, jeśli tranzyt oraz dostęp z programu System i Access mają być niedostępne. Jeśli tranzyt lub dostęp z programu System i Access mają być dozwolone, należy użyć wartości *FRCSIGNON lub *SAMEPRF.

Szczegółowe informacje na temat wartości systemowej QRMTSIGN można znakeźć w książce Remote Workstation Support (obsługa zdalnej stacji roboczej) . 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 18. Dozwolone wartości dla wartości systemowej QSCANFS:

***NONE**	Nie będą skanowane żadne obiekty zintegrowanego systemu plików.
***ROOTOPNUD**	Skanowaniu poddane będą obiekty typu *STMF znajdujące się w katalogach typu *TYPE2 w katalogu głównym (/), QOpenSysand oraz system plików użytkownika.

Wartość zalecana: Wartość zalecana to *ROOTOPNUD. Powoduje ona, że katalog główny (/), QOpenSys oraz system plików użytkownika skanowane są za każdym razem, gdy ktoś rejestruje programy wyjścia za pomocą punktów wyjścia zintegrowanego systemu plików związanych ze skanowaniem.

Odsyłacze pokrewne

"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.

Informacje pokrewne

Katalogi *TYPE2

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.

Wartość systemowa QSCANFSCTL współdziała z wartością systemową definiującą skanowanie systemu plików. Zapewnia to szczegółową kontrolę nad sposobem i zakresem skanowania zintegrowanego systemu plików. Do wyboru są różne opcje skanowania; można również użyć opcji domyślnych. Można również wybrać kilka opcji skanowania, sterujących przedmiotem i sposobem skanowania wykonywanego przez zarejestrowane programy obsługi wyjścia. Opcje te opisano w poniższej tabeli:

Tabela 19. Dozwolone 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.

Tabela 19. Dozwolone wartości dla wartości systemowej QSCANFSCTL: (kontynuacja)

***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 zeskanowany raz, po odtworzeniu. Jeśli atrybut obiektu określa, że ″obiekt będzie skanowany tylko wtedy, gdy zostanie zmodyfikowany od czasu poprzedniego skanowania″, obiekt zostanie zeskanowany 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 zeskanowany 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.

Odsyłacze pokrewne

“skanowanie systemów plików (QSCANFS)” na stronie 33
Wartość systemowa skanowanie systemów plików (QSCANFS) umożliwia określenie zintegrowanego systemu plików, którego obiekty mają być przeskanowane.

Sterowanie pamięcią współużytkowaną (QSHRMEMCTL)

Wartość systemowa Sterowanie pamięcią współużytkowaną (QSHRMEMCTL) definiuje, którzy użytkownicy są uprawnieni do korzystania z pamięci współużytkowanej lub pamięci odwzorowanej, która ma możliwość zapisu.

Dane środowisko może zawierać aplikacje, każda z nich uruchamia inne zadania, ale wszystkie współużytkują wskaźniki. Użycie tych funkcji API poprawia wydajność aplikacji oraz usprawnia programowanie aplikacji, umożliwiając współużytkowanie pamięci i plików strumieniowych przez różne aplikacje i zadania. Jednak użycie tych funkcji API może stanowić również ryzyko dla systemu i jego zasobów. Programista może mieć uprawnienie zapisu i może dodawać pozycje do pamięci współużytkowanej lub pliku strumieniowego, zmieniać je i stamtąd usuwać.

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. Więcej szczegółowych informacji na temat ograniczania zmian wartości systemowych związanych z bezpieczeństwem wraz z pełną listą zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe dotyczące bezpieczeństwa.

Tabela 20. 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 Użycie uprawnień adoptowanych (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.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Więcej szczegółowych informacji na temat ograniczania zmian wartości systemowych związanych z bezpieczeństwem wraz z pełną listą zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe dotyczące bezpieczeństwa.

Tabela 21. 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: • Użytkownik nie ma wystarczających uprawnień dla określonej listy autoryzacji. • podczas tworzenia programu lub programu usługowego nie wystąpiły inne błędy.
***NONE**[1]	Wszyscy użytkownicy mogą tworzyć, zmieniać i aktualizować programy i programy usługowe, w celu użycia uprawnienia programu, który je wywołał, jeśli mają niezbędne uprawnienia do tego programu lub programu usługowego.

Tabela 21. Możliwe wartości dla wartości systemowej QUSEADPAUT: (kontynuacja)

[1]	Wartość *NONE oznacza, że w celu dostępu do programów używających uprawnień adoptowanych nie jest używana żadna lista autoryzacji i domyślnie wszyscy użytkownicy mają ten dostęp.

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

W temacie omówiono wartości systemowe związane z bezpieczeństwem w systemie operacyjnym i5/OS.

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 związanych z bezpieczeństwem w systemie. 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: Wartość ta została również omówiona w temacie Wartości systemowe dla zadań: limit czasu nieaktywności dla odłączonych zadań.

QRMTSRVATR
Atrybut zdalnej usługi

QSSLCSL
Lista algorytmów szyfrowania SSL

QSSLCSLCTL
Sterowanie szyfrowaniem protokołu SSL

QSSLPCL
Protokoły SSL

Pojęcia pokrewne

“Sprawdzanie poprawności odtwarzanych programów” na stronie 18
W momencie tworzenia programu system oblicza wartość sprawdzania, która przechowywana jest w programie. Podczas odtwarzania programu ta wartość jest obliczana ponownie i porównywana z wartością sprawdzania przechowywaną w programie.

Automatyczne konfigurowanie urządzenia (QAUTOCFG)

Wartość systemowa Automatyczne konfigurowanie urządzenia (Automatic Device Configuration - QAUTOCFG) automatycznie konfiguruje urządzenia podłączone lokalnie. Umożliwia automatyczne konfigurowanie urządzeń dodawanych do systemu.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących bezpieczeństwa i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe związane z bezpieczeństwem.

Tabela 22. 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 Konfigurowanie automatyczne urządzeń wirtualnych (Automatic Configuration of Virtual Devices - 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 osobę odpowiedzialną za bezpieczeństwo 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. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących bezpieczeństwa i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe związane z bezpieczeństwem.

Tabela 23. 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

Informacje pokrewne

Działanie odzyskiwania urządzenia (QDEVRCYACN)

Wartość systemowa działania dla odtwarzania urządzenia (Device Recovery Action - QDEVRCYACN) określa działanie, jakie ma być podjęte w przypadku wystąpienia błędu we/wy stacji roboczej zadania interaktywnego.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Więcej informacji na temat ograniczania zmian wartości systemowych, oraz pełna lista ograniczonych wartości systemowych, znajduje się w publikacji Wartości systemowe związane z bezpieczeństwem.

Tabela 24. Dozwolone wartości dla wartości systemowej QDEVRCYACN:

***DSCMSG**	Zadanie zostanie odłączone. Podczas kolejnego wpisywania się do programu użytkownika wysyłany jest komunikat błędu.
***MSG**	Wysyła komunikat o błędzie we/wy do aplikacji użytkownika. Program wykona odzyskiwanie po błędzie.
***DSCENDRQS**	Zadanie zostanie odłączone. Przy kolejnym wpisywaniu się wykonywana jest funkcja anulowania żądania, w celu przywrócenia sterowania zadaniem do poziomu ostatniego 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 określono wartość *MSG lub *DSCMSG, działanie dla odtworzenia urządzenia nie jest wykonywane do momentu, w którym zadanie wykona następną operację we/wy. W środowisku LAN/WAN, funkcja ta umożliwia odłączenie jednego urządzenia od adresu, i podłączenie drugiego urządzenia do tego samego adresu, przed wystąpieniem następnej operacji we/wy. Zadanie może odzyskać sprawność operacyjną po komunikacie błędu we/wy, a następnie kontynuować pracę z drugim urządzeniem. Aby tego uniknąć, należy określić działanie dla odtworzenia urządzenia *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.

Interwał czasowy przed przerwaniem odłączonych zadań (QDSCJOBITV)

Wartość systemowa Interwał limitu czasu dla odłączenia zadania (Disconnected Job Time-Out Interval - QDSCJOBITV) określa, czy system powinien zakończyć odłączone zadanie - a jeśli tak, to w jakim momencie. 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. Więcej informacji na temat ograniczania zmian wartości systemowych, oraz pełna lista ograniczonych wartości systemowych, znajduje się w publikacji Wartości

systemowe związane z bezpieczeństwem.

Tabela 25. Dozwolone 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 Atrybut serwisu zdalnego (Remote Service Attribute - QRMTSRVATR) steruje funkcją zdalnej analizy problemów w systemie. Umożliwia zdalne analizowanie systemu.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Patrz Wartości systemowe dotyczące bezpieczeństwa, gdzie podano szczegółowe informacje o sposobach ograniczania uprawnień do modyfikowania wartości systemowych związanych z bezpieczeństwem, a także pełny wykaz ograniczonych wartości systemowych.

Wartości dozwolone dla wartości systemowej QRMTSRVATR to:

Tabela 26. Dozwolone wartości dla wartości systemowej QRMTSRVATR:

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

Zalecana wartość: 0

Pojęcia pokrewne

“Ochrona za pomocą blokady” na stronie 2
Do sprawdzania i zmiany pozycji kluczyka służy funkcja API Odtworzenie atrybutów IPL (Retrieve IPL Attributes - QWCRIPLA) oraz komenda Zmiana atrybutów IPL (Change IPL Attributes - CHGIPLA).

Lista specyfikacji szyfrów SSL (Secure Sockets Layer (SSL) cipher specification list - QSSLCSL)

Wartość systemowa Lista specyfikacji szyfrów SSL (Secure Sockets Layer (SSL) cipher specification list - QSSLCSL) określa, jaką listę specyfikacji szyfrów będzie obsługiwał systemowy protokół SSL.

Systemowa implementacja protokołu SSL używa sekwencji informacji podanych w wartości systemowej QSSLCSL do porządkowania domyślnej listy specyfikacji szyfrów. Pozycje na domyślnej liście specyfikacji szyfrów są definiowane przez system i mogą się zmieniać między poszczególnymi wydaniami. Jeśli domyślny zestaw algorytmów szyfrowania zostanie usunięty z wartości systemowej QSSLCSL, to spowoduje to również usunięcie go z listy specyfikacji szyfrów. Natomiast dodanie domyślnego zestawu algorytmów szyfrowania do wartości systemowej QSSLCSL spowoduje dodanie go również z powrotem na listę specyfikacji szyfrów. Do domyślnej listy specyfikacji szyfrów nie można dodawać innych szyfrów poza zestawem systemowym, zdefiniowanym dla danej wersji. Zestawu algorytmów szyfrowania nie można dodać do wartości systemowej QSSLCSL również wtedy, gdy nie ustawiono wymaganej wartości protokołu SSL tego zestawu w wartości systemowej QSSLPCL (lista protokołów SSL).

Ustawienia wartości systemowej QSSLCSL są przeznaczone tylko do odczytu. Można to zmienić, ustawiając wartość systemową Sterowanie szyfrem SSL (SSL cipher control - QSSLCSLCTL) na *USRDFN.

Wartość systemowa QSSLCSL dopuszcza następujące ustawienia:

- *RSA_AES_128_CBC_SHA
- *RSA_RC4_128_SHA
- *RSA_RC4_128_MD5

- *RSA_AES_256_CBC_SHA
- *RSA_3DES_EDE_CBC_SHA
- *RSA_DES_CBC_SHA
- *RSA_EXPORT_RC4_40_MD5
- *RSA_EXPORT_RC2_CBC_40_MD5
- *RSA_NULL_SHA
- *RSA_NULL_MD5
- *RSA_RC2_CBC_128_MD5
- *RSA_3DES_EDE_CBC_MD5
- *RSA_DES_CBC_MD5

Uwaga: Do zmiany tej wartości systemowej wymagane są uprawnienia specjalne *IOSYSCFG, *ALLOBJ i *SECADM.

Więcej informacji na temat wartości ustawionych fabrycznie można znaleźć w temacie poświęconym liście specyfikacji szyfrów SSL w kolekcji tematów ″Wartości systemowe″.

Informacje pokrewne

Wartości systemowe związane z bezpieczeństwem: lista specyfikacji szyfru protokołu SSL

Właściwości Systemu SSL

Kontrola szyfru SSL (Secure Sockets Layer cipher control - QSSLCSLCTL)

Wartość systemowa Kontrola szyfru SSL (Secure Sockets Layer cipher control - QSSLCSLCTL) określa, czy system lub użytkownik mogą sterować wartością systemową Wykaz specyfikacji szyfrów SSL (Secure Sockets Layer cipher specification list - QSSLCSL).

Wartość systemowa QSSLCSLCTL dopuszcza następujące ustawienia:

- *OPSYS
- *USRDFN

Uwaga: Do zmiany tej wartości systemowej wymagane są uprawnienia specjalne *IOSYSCFG, *ALLOBJ i *SECADM.

Więcej informacji na temat wartości ustawionych fabrycznie można znaleźć w temacie poświęconym kontroli szyfrów SSL w kolekcji tematów ″Wartości systemowe″.

Informacje pokrewne

Wartości systemowe związane z bezpieczeństwem: sterowanie szyfrem Secure Sockets Layer (SSL)

Protokoły SSL (Secure Sockets Layer protocols - QSSLPCL)

Wartość systemowa Protokoły SSL (Secure Sockets Layer protocols - QSSLPCL) określa obsługiwane w systemie protokoły SSL.

Wartość systemowa QSSLPCL dopuszcza następujące ustawienia:

- *OPSYS
- *TLSV1
- *SSLV2
- *SSLV3

Uwaga: Do zmiany tej wartości systemowej wymagane są uprawnienia specjalne *IOSYSCFG, *ALLOBJ i *SECADM.

Więcej informacji na temat wartości ustawionych fabrycznie można znaleźć w temacie poświęconym protokołom SSL w kolekcji tematów ″Wartości systemowe″.

Informacje pokrewne

Wartości systemowe związane z bezpieczeństwem: protokoły Secure Sockets Layer (SSL)

Wartości systemowe odtwarzania związane z ochroną

W temacie omówiono wartości systemowe odtwarzania związane z bezpieczeństwem w systemie operacyjnym i5/OS.

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 związanych z odtwarzaniem obiektów związanych z bezpieczeństwem, które także należy wziąć pod uwagę podczas odtwarzania obiektów. Więcej informacji dotyczących wartości systemowej QSCANFSCTL *NOPOSTRST znajduje się w temacie Tabela 19 na stronie 34.

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.

Pojęcia pokrewne

“Odtwarzanie programów” na stronie 260
Odtwarzanie w systemie programów, które zostały pobrane z nieznanego źródła, stanowi ryzyko naruszenia ochrony. Ten temat zawiera informacje o czynnikach, które należy uwzględnić podczas odtwarzania programów.

Sprawdzenie obiektu podczas odtwarzania (QVFYOBJRST)

Wartość systemowa Sprawdzenie obiektu podczas odtwarzania (Verify Object on Restore - QVFYOBJRST) określa, czy obiekty muszą mieć podpisy cyfrowe, aby mogły zostać odtworzone w danym 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 Sprawdzenie obiektu podczas odtwarzania (Verify Object on Restore - QVFYOBJRST). Służy ona do sterowania odtwarzaniem niektórych obiektów, które mogą być podpisane cyfrowo. Drugim filtrem jest wartość systemowa

Wymuszenie konwersji podczas odtwarzania (Force Conversion on Restore - 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 Dopuszczenie obiektów do odtworzenia (Allow Object on Restore - QALWOBJRST). Określa ona, czy można odtworzyć obiekty z atrybutami istotnymi dla bezpieczeństwa.

Jeśli program Digital Certificate Manager (opcja 34 systemu i5/OS) nie jest zainstalowany w systemie, to wszystkie obiekty oprócz tych podpisywanych przez system są traktowane jak niepodpisane podczas ustalania efektów działania wartości systemowej QVFYOBJRST w trakcie wykonywania operacji odtwarzania.

Program, program usługowy i moduły, które utworzono lub przekonwertowano w systemie wcześniejszym niż V6R1 są traktowane jako niepodpisane w momencie odtwarzania ich w systemie V6R1 lub nowszym. Podobnie program, program usługowy i moduły utworzone lub przekonwertowane w systemie V6R1 lub późniejszym, są traktowane jako niepodpisane w momencie odtwarzania ich w systemie wcześniejszym niż V6R1.

Zmiana tej wartości odnosi natychmiastowy skutek.

Uwagi:

1. Ta wartość systemowa jest wartością zastrzeżoną. Więcej szczegółowych informacji na temat ograniczania zmian wartości systemowych związanych z bezpieczeństwem wraz z pełną listą zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe dotyczące bezpieczeństwa.
2. Obiekty z atrybutem stanu systemowego i obiekty z atrybutem stanu dziedziczenia powinny mieć poprawny podpis pochodzący z zaufanego źródła. Obiekty w poprawkach PTF licencjonowanego kodu wewnętrznego powinny mieć poprawny podpis pochodzący z zaufanego źródła. Jeśli obiekty te nie mają ważnego podpisu, nie zostaną odtworzone niezależnie od ustawienia wartości systemowej QVFYOBJRST.

Ważne: W momencie dostarczania systemu wartość systemowa QVFYOBJRST jest ustawiona na 3. Jeśli została ona zmieniona, to przed zainstalowaniem nowego wydania systemu i5/OS należy ponownie nadać jej wartość 3 lub mniejszą.

Tabela 27. Możliwe wartości dla wartości systemowej QVFYOBJRST:

1	Nie sprawdzaj podpisów podczas odtwarzania. Odtwarzaj wszystkie obiekty w stanie użytkownika niezależnie od ich podpisów. Nie należy używać tej wartości, chyba że w przypadku odtwarzania podpisanych obiektów, dla których sprawdzenie podpisu nie powiedzie się z przyczyn możliwych do przyjęcia.
2	Sprawdzaj obiekty podczas odtwarzania. Odtwarzaj niepodpisane komendy i obiekty użytkownika. Odtwarzaj podpisane komendy i obiekty użytkownika, nawet jeśli podpisy nie są poprawne. Wartości tej należy używać tylko jeśli pewne obiekty, które mają być odtworzone, zawierają niepoprawne podpisy. Zwykle niezalecane jest odtwarzanie w systemie obiektów z niepoprawnymi 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 27. 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. Wartości tej należy używać tylko jeśli pewne obiekty, które mają być odtworzone, zawierają niepoprawne podpisy, ale obiekty niepodpisane nie mają być odtwarzane. Zwykle niezalecane jest odtwarzanie w systemie obiektów z niepoprawnymi 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.

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 wartości 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, włącznie z tymi obszarami obiektu komendy.

Zalecana wartość: 3

Wymuszenie konwersji podczas odtwarzania (QFRCCVNRST)

Za pomocą wartości systemowej Wymuszanie konwersji przy odtwarzaniu (Force Conversion on Restore - QFRCCVNRST) można wymuszać konwersję pewnych typów obiektów podczas odtwarzania. Można także uniemożliwić odtwarzanie niektórych obiektów.

Wartość systemowa QFRCCVNRST określa, czy podczas odtwarzania ma zachodzić konwersja następujących typów obiektów:

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

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 Sprawdzenie obiektu podczas odtwarzania (Verify Object on Restore - 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 Zezwalanie na odtwarzanie obiektów (Allow Object Restore - QALWOBJRST), która określa, czy obiekty z atrybutami istotnymi dla bezpieczeństwa mogą być odtwarzane.

Jeśli program Digital Certificate Manager (opcja 34 systemu i5/OS) nie jest zainstalowany w systemie, to wszystkie obiekty z wyjątkiem tych podpisywanych przez system traktowane są jak niepodpisane podczas ustalania efektów działania wartości systemowej QFRCCNVRST w trakcie wykonywania operacji odtwarzania.

Programy, programy usługowe i obiekty modułowe utworzone lub przekonwertowane w systemie o wersji wcześniejszej niż V6R1 będą po odtworzeniu do systemu V6R1 lub nowszej wersji traktowane jako niepodpisane. Podobnie, programy, programy usługowe i obiekty modułowe utworzone lub przekonwertowane w wersji V6R1 lub późniejszej, będą po odtworzeniu do systemu starszego niż V6R1 traktowane jako niepodpisane.

Fabrycznie ustawiana wartość QFRCCVNRST wynosi 1. Niezależnie od wartości QFRCCVNRST, nie będą odtwarzane obiekty, które powinny zostać przekonwertowane, ale nie jest to możliwe. 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. Patrz Wartości systemowe dotyczące bezpieczeństwa, gdzie podano szczegółowe informacje o sposobach ograniczania uprawnień do modyfikowania wartości systemowych związanych z bezpieczeństwem, a także pełny wykaz ograniczonych wartości systemowych.

Poniższa tabela zawiera dopuszczalne wartości dla QFRCCVNRST:

Tabela 28. Wartości QFRCCVNRST

0	Nie konwertuj niczego. Nie zapobiegaj odtwarzaniu.
1	Konwertowane będą obiekty z błędami sprawdzania.
2	Obiekty będą konwertowane, jeśli będzie tego wymagać bieżący system operacyjny na komputerze lub jeśli obiekty te będą generowały błędy sprawdzania poprawności.
3	Konwertowane będą obiekty, co do których istnieje podejrzenie, że były manipulowane, które zawierają błędy sprawdzania oraz obiekty, które wymagają konwertowania w celu używania ich w bieżącej wersji systemu operacyjnego lub na bieżącej maszynie.
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): co do których istnieje podejrzenie manipulacji, które wygenerowały błędy sprawdzania poprawności lub które wymagają konwersji w celu użycia w bieżącej wersji systemu operacyjnego lub na bieżącej maszynie; 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:** W przypadku niepowodzenia konwersji nie zostaną odtworzone obiekty, co do których istnieje podejrzenie manipulacji, które wygenerowały błędy sprawdzania poprawności lub które wymagają konwersji w celu użycia w bieżącej wersji systemu operacyjnego lub na bieżącej maszynie.
6	Konwertowane będą wszystkie obiekty, które nie mają poprawnego podpisu cyfrowego. **Uwaga:** Konwertowany będzie obiekt z poprawnym podpisem cyfrowym, który generuje błędy sprawdzania poprawności lub co do którego istnieje podejrzenie manipulacji. W przypadku braku możliwości przekonwertowania takiego obiektu, 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)

Zezwolenie na odtwarzanie obiektów istotnych dla bezpieczeństwa (Allow restoring of security-sensitive objects - QALWOBJRST) określa, czy w systemie można odtwarzać obiekty, które mają istotne znaczenie dla jego bezpieczeństwa.

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 Sprawdzenie obiektu podczas odtwarzania (Verify Object on Restore - QVFYOBJRST). Służy ona do sterowania odtwarzaniem niektórych obiektów, które mogą być podpisane cyfrowo. Drugim filtrem jest wartość systemowa Wymuszanie konwersji przy odtwarzaniu (Force Conversion on Restore - 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 Zezwolenie na odtwarzanie obiektu (Allow Object on Restore - QALWOBJRST). Określa ona, czy można odtworzyć obiekty z atrybutami istotnymi dla bezpieczeństwa. Można jej użyć, aby uniemożliwić każdemu użytkownikowi odtwarzanie obiektu systemowego lub obiektu adoptującego uprawnienia.

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 i5/OS,
- 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. Patrz Wartości systemowe dotyczące bezpieczeństwa, gdzie podano szczegółowe informacje o sposobach ograniczania uprawnień do modyfikowania wartości systemowych związanych z bezpieczeństwem, a także pełny wykaz ograniczonych wartości systemowych.

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

Tabela 29. Dozwolone wartości dla wartości systemowej QALWOBJRST:

***ALL**	Użytkownik z odpowiednimi uprawnieniami może odtworzyć w systemie dowolny obiekt.
***NONE**	Obiekty istotne dla bezpieczeństwa, takie jak programy systemowe lub programy adoptujące uprawnienia nie mogą być odtwarzane.
***ALWSYSSTT**	Można odtwarzać obiekty typu system-state i inherit-state.
***ALWPGMADP**	Można odtwarzać obiekty adoptujące 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).

Tabela 29. Dozwolone wartości dla wartości systemowej QALWOBJRST: (kontynuacja)

***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 często odtwarzane są programy i aplikacje, wartość systemową QALWOBJRST należy ustawić na *ALWPGMADP.

Wartości systemowe mające zastosowanie dla haseł

W tym temacie omówiono wartości systemowe, które dotyczą haseł. 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.

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 wprowadzone zostaną natychmiast (z wyjątkiem zmian dla wartości QPWDLVL). Przeprowadzenie IPL nie jest wymagane.

Wartości systemowe sterujące hasłami:

QPWDCHGBLK
Blokowanie zmiany hasła

QPWDEXPITV
Okres ważności

QPWDEXPWRN
Ostrzeżenie o wygaśnięciu hasła

QPWDLVL
Poziom hasła

QPWDLMTCHR
Znaki zastrzeżone

QPWDLMTAJC
Ograniczenie znaków przylegających

QPWDLMTREP
Ograniczenie powtarzania znaków

QPWDMINLEN
Długość minimalna

QPWDMAXLEN
Długość maksymalna

QPWDPOSDIF
Różnica w położeniu znaku

QPWDRQDDIF
Wymagana różnica

QPWDRQDDGT
Wymaganie znaków numerycznych

QPWDRULES
Reguły hasła

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.

W wymienionych poniżej sytuacjach system uniemożliwia ustawienie hasła identycznego z nazwą profilu użytkownika za pomocą komendy CHGPWD, menu ASSIST lub funkcji API QSYCHGPW:

- gdy wartość systemowa Reguły hasła (Password Rules - QPWDRULES) jest równa *PWDSYSVAL, natomiast wartość systemowa Minimalna długość hasła (Password Minimum Length - QPWDMINLEN) nie jest równa 1,
- gdy wartość systemowa Reguły hasła (Password Rules - QPWDRULES) jest równa *PWDSYSVAL, natomiast wartość systemowa Maksymalna długość hasła (Password Maximum Length - QPWDMAXLEN) nie jest równa 10,
- gdy wartość systemowa Reguły hasła (Password Rules - QPWDRULES) jest równa *PWDSYSVAL i zmieniono dowolną inną wartość systemową sterującą hasłem w taki sposób, że ma ustawienie inne niż domyślne.

Jeśli użytkownik zapomni hasła, to osoba odpowiedzialna za bezpieczeństwo może użyć komendy Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF), aby ustawić hasło identyczne z nazwą profilu. Może też ustawić dowolną inną wartość hasła. Pole Ustawienie hasła jako wygasłe w profilu użytkownika może być użyte do żądania zmiany hasła podczas następnego wpisywania się.

Informacje pokrewne

Wartości systemowe: przegląd haseł

Blokada zmiany hasła (Block Password Change - QPWDCHGBLK)

Wartość systemowa Blokada zmiany hasła (Block Password Change - QPWDCHGBLK) definiuje okres, przez który nie można zmienić hasła po uprzedniej, pomyślnie zrealizowanej operacji zmiany.

Zmiana tej wartości odnosi natychmiastowy skutek.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Patrz sekcja Wartości systemowe dotyczące bezpieczeństwa, w której podano szczegółowe informacje o sposobach ograniczania uprawnień do zmiany wartości systemowych związanych z bezpieczeństwem, a także pełny wykaz zastrzeżonych wartości systemowych.

Tabela 30. Dozwolone wartości dla wartości systemowej QPWDCHGBLK:

***NONE**	Hasło można zmienić w dowolnej chwili.
1 - 99	Hasło można zmienić po upływie określonej liczby godzin od poprzedniej, pomyślnej zmiany hasła.

Okres ważności hasła (QPWDEXPITV)

Wartość systemowa Okres ważności hasła (The Password Expiration Interval - QPWDEXPITV) określa ilość dni, po upływie których należy zmienić hasło.

Jeśli użytkownik próbuje wpisać się po wygaśnięciu hasła, system wyświetli ekran żądający zmiany hasła przed wpisaniem się.

```
                          Informacje wpisania
                                                              System:
Hasło wygasło. Aby wpisać się do systemu musisz zmienić
hasło.

Poprzednie wpisanie . . . . . . . . . . . . . :   10/30/99  14:15:00

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

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Więcej informacji na temat ograniczania zmian wartości systemowych, oraz pełna lista ograniczonych wartości systemowych, znajduje się w publikacji Wartości systemowe związane z bezpieczeństwem.

Tabela 31. Dozwolone wartości dla wartości systemowej QPWDEXPITV:

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

Zalecana wartość: 30 do 90

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

Ostrzeżenie o wygaśnięciu hasła (Password Expiration Warning - QPWDEXPWRN)

Wartość systemowa Ostrzeżenie o wygaśnięciu hasła (Password Expiration Warning - QPWDEXPWRN) określa, przez ile dni przed utratą ważności hasła system ma wyświetlać komunikaty ostrzegawcze podczas wpisywania się użytkownika.

Zmiana tej wartości odnosi natychmiastowy skutek.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Patrz sekcja Wartości systemowe dotyczące bezpieczeństwa, w której podano szczegółowe informacje o sposobach ograniczania uprawnień do modyfikowania wartości systemowych związanych z bezpieczeństwem, a także pełny wykaz zastrzeżonych wartości systemowych.

Tabela 32. Dozwolone wartości dla wartości systemowej QPWDEXPWRN:

7	Określa, że wyświetlanie komunikatu ostrzegającego o upływie okresu ważności hasła powinno rozpocząć się z 7-dniowym wyprzedzeniem.
1 - 99	Określa liczbę dni przed upływem ważności hasła, przez które ma być wyświetlany komunikat ostrzegawczy.

Zalecana wartość: 14 (dni).

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.

Ustawienie poziomu hasła umożliwia stosowanie długich haseł jako wartości hasła. Terminem *długie hasło* (ang. passphrase) określa się w branży komputerowej hasło, 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 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 hasła.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących ochrony i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe dotyczące ochrony.

Tabela 33. 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 systemowa QPWDLVL powinna być równa 0, jeśli system komunikuje się z innymi platformami System i połączonymi w sieć, a w tych systemach wartość systemowa QPWDLVL też jest równa 0 lub są to systemy operacyjne w wersji wcześniejszej 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 systemowa QPWDLVL musi być równa 0, jeśli system komunikuje się z produktem i5/OS Support for Windows Network Neighborhood i5/OS NetServer i innymi systemami korzystającymi z haseł o długości 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 systemowa QPWDLVL równa 1 ma działanie takie samo jak wartość systemowa QPWDLVL równa 0 z następującym wyjątkiem: hasła produktu i5/OS NetServer dla klientów systemu Windows 95/98/ME zostaną usunięte z systemu. **Uwaga:** Produkt i5/OS Netserver będzie współpracował z klientami systemu Windows NT/2000/XP/Vista na 1 lub 3 poziomie hasła. Jeśli używana jest obsługa klientów dla produktu i5/OS NetServer, wartość systemowa QPWDLVL nie może być równa 1. Wartość systemowa QPWDLVL równa 1 zapewnia lepszą ochronę platform System i, usuwając z systemu wszystkie hasła produktu i5/OS 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 cofnięcie się do wartości systemowej QPWDLVL równej 0 lub 1, o ile hasło utworzone na poziomie QPWDLVL 2 lub 3 spełnia wymagania dotyczące długości i składni hasła obowiązujące na poziomie QPWDLVL 0 lub 1. • Wartość systemowa QPWDLVL może być równa 2, jeśli system komunikuje się z produktem i5/OS Support for Windows Network Neighborhood i5/OS NetServer, pod warunkiem, że długość hasła wynosi od 1 do 14 znaków. • Wartość systemowa QPWDLVL nie może być równa 2, jeśli system komunikuje się z innymi platformami System i połączonymi w sieć, a w tych systemach wartość systemowa QPWDLVL jest równa 0 lub 1 albo są to systemy operacyjne w wersji wcześniejszej 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.

Tabela 33. Możliwe wartości dla wartości systemowej QPWDLVL: (kontynuacja)

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 systemowa QPWDLVL nie może być równa 3, jeśli system komunikuje się z innymi platformami System i połączonymi w sieć, a w tych systemach wartość systemowa QPWDLVL jest równa 0 lub 1 albo są to systemy operacyjne w wersji wcześniejszej 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 systemowa QPWDLVL nie może być równa 3, jeśli system komunikuje się z produktem i5/OS Support for Windows Network Neighborhood i5/OS NetServer. **Uwaga:** Produkt i5/OS Netserver będzie współpracował z klientami systemu Windows NT/2000/XP/Vista na 1 lub 3 poziomie hasła. 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 wyświetlić bieżące i oczekujące wartości poziomu hasła, należy użyć komendy Wyświetlenie atrybutów bezpieczeństwa (Display Security Attributes - DSPSECA).

Minimalna długość haseł (QPWDMINLEN)

Wartość systemowa Minimalna długość haseł (Minimum Length of Passwords - QPWDMINLEN) określa minimalną liczbę znaków hasła.

Uwagi:

1. Ta wartość systemowa jest wartością zastrzeżoną. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących ochrony i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe dotyczące ochrony.
2. Jeśli do wartości systemowej QPWDRULES jest przypisana inna wartość niż *PWDSYSVAL, ta wartość systemowa zostanie zignorowana podczas sprawdzania poprawności formatowania nowych haseł.

Tabela 34. 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: zalecana jest wartość 6, aby zapobiec podawaniu hasła, które łatwo odgadnąć, takich jak inicjały lub pojedyncze znaki.

Maksymalna długość hasła (QPWDMAXLEN)

Wartość systemowa Maksymalna długość haseł (Maximum Length of Passwords - 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.

Uwagi:

1. Ta wartość systemowa jest wartością zastrzeżoną. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących ochrony i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe dotyczące ochrony.
2. Jeśli wartość systemowa QPWDRULES jest inna niż *PWDSYSVAL, to nie można zmieniać tej wartości systemowej. Podczas sprawdzania poprawności formatu nowych haseł jej ustawienie będzie ignorowane.

Tabela 35. 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 Wymagana różnica haseł (Required difference in passwords - QPWDRQDDIF) określa, czy hasło musi różnić się od wcześniej używanych haseł.

Zastosowanie tej wartości zapewnia dodatkowe zabezpieczenie systemu, ponieważ uniemożliwia użytkownikom wybieranie haseł, które były już wcześniej używane. 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. Ta wartość systemowa jest wartością zastrzeżoną. Patrz Wartości systemowe dotyczące bezpieczeństwa, gdzie podano szczegółowe informacje o sposobach ograniczania uprawnień do modyfikowania wartości systemowych związanych z bezpieczeństwem, a także pełny wykaz ograniczonych wartości systemowych.

Tabela 36. Dozwolone wartości dla wartości systemowej QPWDRQDDIF:

wartość	*Liczba wcześniejszych 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 uniemożliwić ponowne użycie hasła przez co najmniej 6 miesięcy, należy użyć kombinacji wartości systemowej Wymagana różnica haseł (Required difference in passwords - QPWDRQDDIF) i wartości systemowej Okres ważności hasła (Password Expiration Interval - QPWDEXPITV). 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 Znaki zastrzeżone w hasłach (Restricted characters for passwords - QPWDLMTCHR) uniemożliwia używanie w hasłach niektórych znaków.

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.

Uwagi:

1. Ta wartość systemowa jest wartością zastrzeżoną. Patrz Wartości systemowe dotyczące bezpieczeństwa, gdzie podano szczegółowe informacje o sposobach ograniczania uprawnień do modyfikowania wartości systemowych związanych z bezpieczeństwem, a także pełny wykaz ograniczonych wartości systemowych.
2. Jeśli wartość systemowa QPWDRULES jest inna niż *PWDSYSVAL, to nie można zmieniać tej wartości systemowej. Podczas sprawdzania poprawności formatu nowych haseł jej ustawienie będzie ignorowane.

Tabela 37. Dozwolone 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 @ i podkreślenie (_).

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

Ograniczenie kolejnych cyfr w hasłach (QPWDLMTAJC)

Wartość systemowa Ograniczenie użycia kolejnych cyfr w hasłach (Restriction of consecutive digits for passwords - QPWDLMTAJC) uniemożliwia użycie w hasłach kolejnych (występujących obok siebie) znaków numerycznych.

Ta wartość zwiększa bezpieczeństwo systemu poprzez uniemożliwienie użytkownikom tworzenia haseł będących datami urodzin, numerami telefonu lub innymi sekwencjami cyfr.

Uwagi:

1. Ta wartość systemowa jest wartością zastrzeżoną. Patrz sekcja Wartości systemowe dotyczące bezpieczeństwa, w której podano szczegółowe informacje o sposobach ograniczania uprawnień do modyfikowania wartości systemowych związanych z bezpieczeństwem, a także pełny wykaz zastrzeżonych wartości systemowych.
2. Jeśli wartość systemowa QPWDRULES jest inna niż *PWDSYSVAL, to nie można zmieniać tej wartości systemowej. Podczas sprawdzania poprawności formatu nowych haseł jej ustawienie będzie ignorowane.

Tabela 38. Dozwolone 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 Ograniczenie powtarzania znaków w hasłach (QPWDLMTREP) ogranicza wielokrotne użycie w haśle tego samego znaku.

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″.

Uwagi:

1. Ta wartość systemowa jest wartością zastrzeżoną. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących ochrony i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe dotyczące ochrony.
2. Jeśli wartość systemowa QPWDRULES jest inna niż *PWDSYSVAL, to nie można zmieniać tej wartości systemowej. Podczas sprawdzania poprawności formatu nowych haseł jej ustawienie będzie ignorowane.

Tabela 39. 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 40 opisuje przykłady, jakie hasła są dozwolone w zależności od wartości systemowej QPWDLMTREP.

Tabela 40. Hasła z powtórzonymi znakami dla wartości QPWDLVL 0 lub 1

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

Tabela 41. Hasła z powtórzonymi znakami dla wartości QPWDLVL 2 lub 3

Przykład hasła	Wartość QPWDLMTREP 0	Wartość QPWDLMTREP 1	Wartość QPWDLMTREP 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 Różnica pozycji znaków w hasłach (Character position difference for passwords - QPWDPOSDIF) kontroluje poszczególne pozycje nowego hasła.

Użycie tej wartości systemowej zapewnia dodatkową ochronę, zapobiegając używaniu przez użytkowników takich samych znaków (alfabetycznych lub numerycznych) na takiej samej pozycji, co 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″.

Uwagi:

1. Ta wartość systemowa jest wartością zastrzeżoną. Patrz Wartości systemowe dotyczące bezpieczeństwa, gdzie podano szczegółowe informacje o sposobach ograniczania uprawnień do modyfikowania wartości systemowych związanych z bezpieczeństwem, a także pełny wykaz ograniczonych wartości systemowych.
2. Jeśli wartość systemowa QPWDRULES jest inna niż *PWDSYSVAL, to nie można zmieniać tej wartości systemowej. Podczas sprawdzania poprawności formatu nowych haseł jej ustawienie będzie ignorowane.

Tabela 42. Dozwolone 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 Wymaganie znaków numerycznych w haśle (Requirement for numeric character in passwords - QPWDRQDDGT) określa, czy w nowym haśle muszą się pojawić znaki numeryczne. Ta wartość udostępnia dodatkową ochronę zapobiegając używaniu przez użytkowników tylko znaków alfabetu.

Uwagi:

1. Ta wartość systemowa jest wartością zastrzeżoną. Patrz Wartości systemowe dotyczące bezpieczeństwa, gdzie podano szczegółowe informacje o sposobach ograniczania uprawnień do modyfikowania wartości systemowych związanych z bezpieczeństwem, a także pełny wykaz ograniczonych wartości systemowych.
2. Jeśli wartość systemowa QPWDRULES jest inna niż *PWDSYSVAL, to nie można zmieniać tej wartości systemowej. Podczas sprawdzania poprawności formatu nowych haseł jej ustawienie będzie ignorowane.

Tabela 43. Dozwolone wartości dla wartości systemowej QPWDRQDDGT:

0	W nowych hasłach nie są wymagane znaki numeryczne.
1	W nowych hasłach wymagany jest co najmniej jeden znak numeryczny.

Zalecana wartość: 1

Reguły hasła (Password Rules - QPWDRULES)

Wartość systemowa Reguły hasła (Password Rules - QPWDRULES) określa reguły, na podstawie których sprawdzana jest prawidłowość konstrukcji hasła. Dla wartości systemowej QPWDRULES można podać więcej niż jedną wartość, chyba że jest to wartość *PWDSYSVAL.

Zmiany dokonane w tej wartości systemowej obowiązują od następnej zmiany hasła.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Patrz Wartości systemowe dotyczące bezpieczeństwa, gdzie podano szczegółowe informacje o sposobach ograniczania uprawnień do modyfikowania wartości systemowych związanych z bezpieczeństwem, a także pełny wykaz ograniczonych wartości systemowych.

Tabela 44. Dozwolone wartości dla wartości systemowej QPWDRULES:

***PWDSYSVAL**	Takie ustawienie powoduje, że wartość systemowa QPWDRULES jest ignorowana, a do sprawdzania poprawności konstrukcji hasła używane są inne wartości systemowe dotyczące haseł. Są to takie wartości, jak: QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF i QPWDQDDGT. **Uwaga:** Jeśli dla wartości systemowej QPWDRULES zostanie określona wartość inna niż *PWDSYSVAL, wartości systemowe QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF i QPWDRQDDGT są ignorowane podczas sprawdzania, czy nowe hasła są skonstruowane poprawnie. Co więcej, wszelkie próby zmiany tych wartości systemowych będą ignorowane tak długo, dopóki wartość systemowa QPWDRULES będzie zawierała inną wartość, niż *PWDSYSVAL.

Tabela 44. Dozwolone wartości dla wartości systemowej QPWDRULES: (kontynuacja)

***CHRLMTAJC**	Ta wartość określa, że hasło nie może zawierać 2 lub więcej wystąpień tego samego znaku, umieszczonych obok siebie. Spełnia taką samą funkcję, jak wartość 2 podana dla wartości systemowej QPWDLMTREP. Tej wartości nie można podawać, jeśli podano wartość *CHRLMTREP.
	Przykłady:
	`Better.test niepoprawne - tt`
	`fix11bugs niepoprawne - 11`
	`@12/A78 poprawne`
	`A1234A1234 poprawne`

***CHRLMTREP**	Ta wartość określa, że hasło nie może zawierać dwóch lub większej liczby wystąpień tego samego znaku. Spełnia taką samą funkcję, jak wartość 1 podana dla wartości systemowej QPWDLMTREP. Tej wartości nie można podawać, jeśli podano wartość *CHRLMTAJC.
	Przykłady:
	`John.Jones niepoprawne - J o n`
	`THISONEOK niepoprawneno - O`
	`@12/A78 poprawne`
	`AaCcEeFfGg poprawne`

***DGTLMTAJC**	Ta wartość określa, że hasło nie może zawierać dwóch lub większej liczby cyfr umieszczonych obok siebie.
	Przykłady:
	`@12/A78 niepoprawne`
	`!@#$%a1234. niepoprawne`
	`THISONEOK poprawne`
	`A1B2C3DE5 poprawne`

***DGTLMTFST**	Ta wartość określa, że pierwszym znakiem hasła nie może być cyfra. Jeśli podano wartości *LTRLMTFST i *SPCCHRLMTFST, to nie można podać wartości *DGTLMTFST. Jeśli system działa na poziomie haseł 0 lub 1, to zachowuje się tak, jakby wartość *DGTLMTFST została określona.
	Przykłady:
	`16ST-SW-Roch niepoprawne - 1`
	`99BottlesOfBeer niepoprawne - 9`
	`@12/A78 poprawne`
	`Allow-this.1 poprawne`

***DGTLMTLST**	Ta wartość określa, że ostatnim znakiem hasła nie może być cyfra. Jeśli podano wartości *LTRLMTLST i *SPCCHRLMTLFST, to nie można podać wartości *DGTLMTLST.
	Przykłady:
	`John.doe12 niepoprawne - 2`
	`@12/A78 niepoprawne no - 8`
	`THISONEOK poprawne`
	`A1234b123. poprawne`

Tabela 44. Dozwolone wartości dla wartości systemowej QPWDRULES: (kontynuacja)

***DGTMAXn**	Ta wartość określa maksymalną liczbę cyfr, które mogą znaleźć się w haśle. Parametr **n** odpowiada liczbie od 0 do 9.
	
	Można określić tylko jedną wartość *DGTMAXn. Jeśli podano także wartość *DGTMINn, wartość n określona dla wartości *DGTMAXn musi być większa lub równa wartości n określonej dla wartości *DGTMINn.
	Przykłady: dla *DGTMAX2
	`Q12345678 niepoprawne - o 6 cyfr za dużo`
	`3-2-1->Go niepoprawne - o 1 cyfrę za dużo`
	`Rick1 poprawne`
	`Ed1-Jeff3 poprawne`

***DGTMINn**	Ta wartość określa minimalną liczbę cyfr, które mogą znaleźć się w haśle. Parametr **n** odpowiada liczbie od 0 do 9.
	
	Można określić tylko jedną wartość *DGTMINn. Jeśli podano także wartość *DGTMAXn, wartość n określona dla wartości *DGTMAXn musi być większa lub równa wartości n określonej dla wartości *DGTMINn.
	Przykłady: dla *DGTMIN3
	`Rick1 niepoprawne - tylko 1 cyfra`
	`Ed1-Jeff3 niepoprawne - tylko 2 cyfry`
	`3-2-1->Go poprawne`
	`Q12345678 poprawne`

***LMTSAMPOS**	Na pozycji odpowiadającej pozycji w poprzednim haśle nie mogą być takie same znaki. Ta wartość spełnia taką samą funkcję, jak wartość 2 podana dla wartości systemowej QPWDPOSDIF.
	
	Gdy hasło jest ustawiane za pomocą komendy Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF) lub Tworzenie profilu użytkownika (Create User Profile - CRTUSRPRF), kontrola tej reguły konstrukcji jest niemożliwa, ponieważ nie jest podawana poprzednia wartość hasła.
	Przykłady: dla wartości *LMTSAMPOS, gdy poprzednim hasłem było Vote4Me:
	`Victory1 niepoprawne - V na pozycji 1`
	`Mine2love niepoprawne - e na pozycji 4`
	`vOTE-mE poprawne`
	`(różnica wielkości liter)`
	`Allisgood poprawne`

***LMTPRFNAME**	Wartość hasła zapisana wielkimi literami nie może zawierać pełnej nazwy profilu użytkownika na sąsiadujących pozycjach.
	Przykłady: dla wartości *LMTPRFNAME, gdy nazwa profilu to JOHNB:
	`bigJOHNB9 niepoprawne - pozycje 4-8`
	`JohnB78 niepoprawne - pozycje 1-5`
	`J_ohn_B234 poprawne`
	`john_b poprawne`

***LTRLMTAJC**	Ta wartość określa, że hasło nie może zawierać dwóch lub większej liczby liter umieszczonych obok siebie.
	Przykłady:
	`John.Smith niepoprawne`
	`THISONEOK niepoprawne`
	`@12/A78 poprawne`
	`A1234b1234 poprawne`

Tabela 44. Dozwolone wartości dla wartości systemowej QPWDRULES: (kontynuacja)

***LTRLMTFST**	Ta wartość określa, że pierwszym znakiem hasła nie może być litera. Jeśli podano wartości *DGTLMTFST i *SPCCHRLMTFST, to nie można podać wartości *LTRLMTFST. Jeśli wartość QPWDLVL w systemie jest równa 0 lub 1, nie można równocześnie określić wartości *LTRLMTFST i *SPCCHRLMTFST.
	Przykłady:
	`John.Smith niepoprawne - J`
	`THISONEOK niepoprawne - T`
	`@12/A78 poprawne`
	`16ST-SW-Roch poprawne`

***LTRLMTLST**	Ta wartość określa, że ostatnim znakiem hasła nie może być litera. Jeśli podano wartości *DGTLMTLST i *SPCCHRLMTLST, to nie można podać wartości *LTRLMTLST.
	Przykłady:
	`John.Smith niepoprawne - h`
	`1Allow.It niepoprawne - t`
	`@12/A78 poprawne`
	`(pay*rate) poprawne`

***LTRMAXn**	Ta wartość określa maksymalną liczbę liter, które mogą znaleźć się w haśle. Parametr **n** odpowiada liczbie od 0 do 9.
	
	Można określić tylko jedną wartość *LTRMAXn. Jeśli podano także wartość *LTRMINn, wartość n określona dla wartości *LTRMAXn musi być większa lub równa wartości n określonej dla wartości *LTRMINn.
	
	Jeśli zostanie również określona wartość *MIXCASEn, liczba n podana dla wartości *LTRMAXn nie może być mniejsza od podwojonej liczby n podanej dla wartości *MIXCASEn.
	Przykłady: dla *LTRMAX4
	`THISONEOK niepoprawne - 5 za dużo`
	`John.Smith1 niepoprawne - 5 za dużono`
	`John1423 poprawne`
	`A1b2.#456 poprawne`

***LTRMINn**	Ta wartość określa minimalną liczbę liter, które mogą znaleźć się w haśle. Parametr **n** odpowiada liczbie od 0 do 9.
	
	Można określić tylko jedną wartość *LTRMINn. Jeśli zostanie określona również wartość *LTRMAXn, to liczba n podana dla wartości *LTRMAXn nie może być mniejsza od liczby n podanej dla wartości *LTRMINn.
	Przykłady: dla *LTRMIN2
	`@12/A78 niepoprawne - tylko 1 litera`
	`!@#$%a1234 niepoprawne - tylko 1 litera`
	`THISONEOK poprawne`
	`A1234b1234 poprawne`

Tabela 44. Dozwolone wartości dla wartości systemowej QPWDRULES: (kontynuacja)

***MAXLENnnn**	Ta wartość określa maksymalną liczbę znaków w haśle. Parametr **nnn** odpowiada liczbie od 1 do 128 (bez zer wiodących). Wartość *MAXLENnnn pełni taką samą funkcję, jak wartość systemowa QPWDMAXLEN. Jeśli wartość QPWDLVL wynosi 0 lub 1, poprawnym zakresem jest od 1 do 10. Jeśli wartość QPWDLVL w systemie wynosi 2 lub 3, poprawnym zakresem jest od 1 do 128. Określona wartość nnn musi być wystarczająco duża na potrzeby wszystkich wartości *MIXCASEn, *DGTMAXn, *LTRMAXn i *SPCCHRMAXn, ograniczeń dotyczących pierwszego i ostatniego znaku oraz wymagań dotyczących znaków znajdujących się obok siebie. Jeśli podano także wartość *MINLENnnn, wartość nnn określona dla wartości *MAXLENnnn musi być większa lub równa wartości nnn określonej dla wartości *MINLENnnn. Jeśli wartość *MAXLENnnn nie zostanie określona, przyjmowana jest wartość *MAXLEN10, w przypadku, gdy dla systemu określono wartość QPWDLVL równą 0 lub 1, lub wartość *MAXLEN128, w przypadku, gdy dla systemu określono wartość QPWDLVL równą 2 lub 3.
***MINLENnnn**	Ta wartość określa minimalną liczbę znaków w haśle. Parametr **nnn** odpowiada liczbie od 1 do 128 (bez zer wiodących). Jeśli wartość QPWDLVL wynosi 0 lub 1, poprawnym zakresem jest od 1 do 10. Jeśli wartość QPWDLVL w systemie wynosi 2 lub 3, poprawnym zakresem jest od 1 do 128. Jeśli podano także wartość *MAXLENnnn, wartość nnn określona dla wartości *MAXLENnnn musi być większa lub równa wartości nnn określonej dla wartości *MINLENnnn. Jeśli wartość *MINLENnnn nie zostanie określona, przyjmowana jest wartość *MINLEN1.

***MIXCASEn**	Ta wartość określa, że hasło musi zawierać przynajmniej n liter wielkich i n liter małych. Parametr **n** odpowiada liczbie od 0 do 9. Ta wartość jest odrzucana, jeśli dla systemu określono wartość QPWDLVL równą 0 lub 1, ponieważ hasła muszą być zapisane wielkimi literami.
	
	Można określić tylko jedną wartość *MIXCASEn.
	
	Jeśli określono wartość *LTRMAXn, wartość n podana dla wartości *LTRMAXn musi być większa lub równa wartości n podanej dla wartości *MIXCASEn pomnożonej przez dwa. **Przykłady:** dla *MIXCASE2
	`@12/A78bC niepoprawne - brakuje 1 małej litery`
	`THISONEOK niepoprawne - brakuje 2 małych liter`
	`ThisIsOkay poprawne`
	`Allow-It poprawne`

Tabela 44. Dozwolone wartości dla wartości systemowej QPWDRULES: (kontynuacja)

***REQANY3**	Ta wartość określa, że hasło musi zawierać co najmniej trzy z czterech poniższych typów znaków:
	• wielkie litery,
	• małe litery,
	• cyfry,
	• znaki specjalne.
	
	Gdy system działa z wartością QPWDLVL równą 0 lub 1, wartość *REQANY3 ma taki sam skutek jak jednoczesne określenie wartości *DGTMIN1, *LTRMIN1 i *SPCCHRMIN1.
	Przykłady:
	`THISONEOK niepoprawne - tylko 1 typ`
	`@12/-78 niepoprawne - tylko 2 typy`
	`A1234b1234 poprawne - wielkie, małe, cyfry`
	`John.Smith poprawne - wielkie, małe, specjalne`
	`peter(21) poprawne - małe, specjalne, cyfry`

***SPCCHRLMTAJC**	Ta wartość określa, że hasło nie może zawierać dwóch lub większej liczby znaków specjalnych umieszczonych obok siebie. Znak specjalny to taki, którego symbol Unicode ma właściwość określającą, że nie jest ani literą, ani cyfrą.
	Przykłady:
	`Big//Box niepoprawne`
	`this->way niepoprawne`
	`@12/A78 poprawne`
	`John.Smith poprawne`

***SPCCHRLMTFST**	Ta wartość określa, że pierwszym znakiem hasła nie może być znak specjalny.Znak specjalny to taki, którego symbol Unicode ma właściwość określającą, że nie jest ani literą, ani cyfrą.
	
	Jeśli podano wartości *DGTLMTFST i *LTRLMTFST, to nie można podać wartości *SPCCHRLMTFST. Jeśli wartość QPWDLVL w systemie jest równa 0 lub 1, nie można równocześnie określić wartości *LTRLMTFST i *SPCCHRLMTFST.
	Przykłady:
	`(2+2equals4) niepoprawne - (`
	`#fred/#charlie niepoprawne - #`
	`1Good->one12 poprawne`
	`A1234b1234 poprawne`

***SPCCHRLMTLST**	Ta wartość określa, że ostatnim znakiem hasła nie może być znak specjalny. Znak specjalny to taki, którego symbol Unicode ma właściwość określającą, że nie jest ani literą, ani cyfrą.
	
	Jeśli podano wartości *DGTLMTLST i *LTRLMTLST, to nie można podać wartości *SPCCHRLMTLST.
	Przykłady:
	`A1234b123. niepoprawne - .`
	`>John.Doe< niepoprawne - <`
	`THISONEOK poprawne`
	`@12/A78 poprawne`

Tabela 44. Dozwolone wartości dla wartości systemowej QPWDRULES: (kontynuacja)

***SPCCHRMAXn**	Ta wartość określa maksymalną liczbę znaków specjalnych, które mogą znaleźć się w haśle. Parametr **n** odpowiada liczbie od 0 do 9. Znak specjalny to taki, którego symbol Unicode ma właściwość określającą, że nie jest ani literą, ani cyfrą.
	
	Można określić tylko jedną wartość *SPCCHRMAXn. Jeśli podano wartość *SPCCHRMINn, wartość n określona dla wartości *SPCCHRMAXn musi być większa lub równa wartości n określonej dla wartości *SPCCHRMINn.
	Przykłady: dla *SPCCHRMAX3
	`@12/A78.b# niepoprawne - o 1 za dużo`
	`!@#$%a1234 niepoprawne - o 2 za dużo`
	`THISONEOK poprawne`
	`A1234b-234 poprawne`

***SPCCHRMINn**	Ta wartość określa minimalną liczbę znaków specjalnych, które mogą znaleźć się w haśle. Parametr **n** odpowiada liczbie od 0 do 9. Znak specjalny to taki, którego symbol Unicode ma właściwość określającą, że nie jest ani literą, ani cyfrą.
	
	Można określić tylko jedną wartość *SPCCHRMINn. Jeśli podano wartość *SPCCHRMAXn, wartość n określona dla wartości *SPCCHRMAXn musi być większa lub równa wartości n określonej dla wartości *SPCCHRMINn.
	Przykłady: dla *SPCCHRMIN4
	`Su@us.ibm.com niepoprawne - o 1 za mało`
	`123+45=168 niepoprawne - o 2 za mało`
	`A.B@us.ibm.com poprawne`
	`(24/8=3) poprawne`

Program zatwierdzający hasło (QPWDVLDPGM)

Poprawność nowych haseł można sprawdzać za pomocą programu zatwierdzającego hasła (Password Approval Program - 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 puli pamięci dyskowej (ASP) lub podstawowej ASP użytkownika, musi znajdować się program zatwierdzający hasła.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Patrz Wartości systemowe dotyczące bezpieczeństwa, gdzie podano szczegółowe informacje o sposobach ograniczania uprawnień do modyfikowania wartości systemowych związanych z bezpieczeństwem, a także pełny wykaz ograniczonych wartości systemowych.

Tabela 45. Dozwolone 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.

Tabela 45. Dozwolone wartości dla wartości systemowej QPWDVLDPGM: (kontynuacja)

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.

Korzystanie z programu zatwierdzania haseł

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 nowe hasło przejdzie wszystkie testy określone w wartościach systemowych dotyczących kontroli hasła.

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 46. Parametry programu zatwierdzania haseł

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 osobę odpowiedzialną za bezpieczeństwo, a zmiany w programie są ściśle kontrolowane.

Poniższy program napisany w języku CL jest przykładem programu zatwierdzającego hasła w przypadku, gdy dla wartości systemowej QPWDVLDPGM określono nazwę programu. 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:

Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki zapisane w sekcji Rozdział 10, “Licencja na kod oraz Informacje dotyczące kodu”, na stronie 317.

```
/************************************************/
/* 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.                                */
/*********************************************************/

PGM   PARM(&EXINPUT &RTN)
DCL &EXINPUT    *CHAR 1000
DCL &RTN        *CHAR 1

DCL   &UNAME    *CHAR  10
DCL &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)                         */
/* ??? - ???  STARE 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(EXINPUT 61 4))
CHGVAR &NPOFF VALUE(EXINPUT 57 4) + 1)
CHGVAR &UNAME VALUE(EXINPUT 33 10))
CHGVAR &NEWPW VALUE(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(EXINPUT 65 4) = 13488) THEN(DO)
    CHGVAR &INDX2 VALUE(1)
    CHGVAR &INDX3 VALUE(1)
   CVT1:
```

```
   CHGVAR &XLTCHR VALUE(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 NEWPW &INDX3 1) VALUE(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 EXINPUT 65 4) VALUE(X'00000025')
ENDDO

/* Sprawdzenie CCSID wartości nowego hasła - musi mieć format 37     */
IF COND(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 XLTCHR2 2 1) VALUE(NEWPW &INDX2 1))
  CHGVAR &XLTCHR VALUE(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(XLATEC &XLTCHR 1) *NE '.') +
  THEN(CHGVAR NEWPW &INDX3 1) VALUE(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(NEWPW &NPLEN 1) = '0') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '1') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '2') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '3') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '4') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '5') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '6') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '7') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '8') THEN(GOTO ERROR1)
IF COND(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(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(NEWPW &INDX &UNLEN) = 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 sterowania kontrolą

Kontrolowanie działania systemu stanowi ważną część bezpieczeństwa systemu, ponieważ może pomóc w wykryciu nieprawidłowego użycia systemu i włamań do systemu. Do sterowania kontrolą w systemie operacyjnym i5/OS można użyć specjalnych wartości systemowych.

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

Sterowanie kontrolą (QAUDCTL)

Wartość systemowa Sterowanie kontrolą (Auditing Control - QAUDCTL) określa, czy przeprowadzana jest kontrola.

Ta wartość systemowa działa jak włącznik/wyłącznik dla następujących operacji:

- wartości systemowych QAUDLVL i QAUDLVL2,
- kontroli zdefiniowanej dla obiektów za pomocą komend Zmiana kontroli obiektu (Change Object Auditing - CHGOBJAUD), Zmiana wartości kontroli (Change Auditing Value - CHGAUD) oraz 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. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących bezpieczeństwa i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe związane z bezpieczeństwem.

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

Tabela 47. Możliwe wartości dla wartości systemowej QAUDCTL

***NONE**	Dla działań użytkowników i obiektów nie jest wykonywana kontrola.
***NOTAVL**	Ta wartość jest wyświetlana w celu wskazania, że wartość systemowa nie jest dostępna dla użytkownika, ponieważ użytkownik nie posiada uprawnień specjalnych *AUDIT ani *ALLOBJ. Wartości systemowej nie można przypisać tej wartości.
***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. Patrz Rozdział 9, “Kontrola bezpieczeństwa na platformie System i”, na stronie 265 w celu uzyskania dalszych szczegółów. Ta wartość musi być podana razem z wartością *OBJAUD lub *AUDLVL.
	Pełen opis procesu sterowania kontrolą w systemie zawiera sekcja “Planowanie kontroli bezpieczeństwa” na stronie 271.

Działanie zakończenia kontroli (QAUDENDACN)

Wartość systemowa Działanie zakończenia kontroli (Auditing End Action - 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. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących bezpieczeństwa i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe związane z bezpieczeństwem.

Tabela 48. Możliwe wartości dla wartości systemowej QAUDENDACN:

***NOTAVL**	Wartość ta wyświetlana jest wówczas, gdy wartość systemowa nie jest dostępna dla użytkownika, ponieważ użytkownik nie posiada uprawnień specjalnych *AUDIT ani *ALLOBJ. Wartości systemowej nie można przypisać tej wartości.

Tabela 48. Możliwe wartości dla wartości systemowej QAUDENDACN: (kontynuacja)

***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.

Zalecenia 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 Poziom narzucenia kontroli (Auditing Force Level - 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. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących bezpieczeństwa i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe związane z bezpieczeństwem.

Tabela 49. Możliwe wartości dla wartości systemowej QAUDFRCLVL

***NOTAVL**	Wartość ta wyświetlana jest wówczas, gdy wartość systemowa nie jest dostępna dla użytkownika, ponieważ użytkownik nie posiada uprawnień specjalnych *AUDIT ani *ALLOBJ. Wartości systemowej nie można przypisać tej wartości.
***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. Jeśli jednak instalacja wymaga, aby żadne wpisy kontroli nie zostały utracone podczas niepoprawnego zakończenia pracy systemu, należy określić wartość 1. Określenie wartości 1 może mieć negatywny wpływ na wydajność systemu.

Poziom kontroli (QAUDLVL)

Wartość systemowa Poziom kontroli (Auditing Level - QAUDLVL) łącznie z wartością systemową QAUDLVL2 określa, które zdarzenia związane z bezpieczeństwem systemu są protokołowane w kronice kontroli bezpieczeństwa (QAUDJRN) dla wszystkich użytkowników 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. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących bezpieczeństwa i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe związane z bezpieczeństwem.

Tabela 50. Możliwe wartości dla wartości systemowej QAUDCTL

***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.
***NOTAVL**	Wartość ta wyświetlana jest wówczas, gdy wartość systemowa nie jest dostępna dla użytkownika, ponieważ użytkownik nie posiada uprawnień specjalnych *AUDIT ani *ALLOBJ. Wartości systemowej nie można przypisać tej wartości.
***AUDLVL2**	W celu określenia kontrolowanych działań ochrony będą użyte wartości systemowe QAUDLVL i QAUDLVL2.
***ATNEVT**	Protokołowane są zdarzenia ostrzeżeń.
***AUTFAIL**	Protokołowane są zdarzenia błędu uprawnień.
***CREATE**	Protokołowane są operacje tworzenia obiektu.
***DELETE**	Protokołowane są operacje usunięcia obiektu.
***JOBBAS**	Kontrolowane są podstawowe funkcje zadania.
***JOBCHGUSR**	Kontrolowane są zmiany aktywnego profilu użytkownika wątku lub profili grupowych.
***JOBDTA**	Protokołowane są działania wpływające na zadanie. Wartość *JOBDTA jest złożona z dwóch wartości, *JOBBAS oraz *JOBCHGUSR, które umożliwiają lepsze dostosowanie kontroli. Określenie obu wartości jest równoznaczne z podaniem wartości *JOBDTA.
***NETBAS**	Kontrolowane są podstawowe funkcje sieciowe.
***NETCLU**	Kontrolowane są operacje klastra i grupy zasobów klastra.
***NETCMN**	Kontrolowane są funkcje sieci i komunikacji. Wartość *NETCMN jest złożona z kilku wartości umożliwiających lepsze dostosowanie kontroli. Następujące wartości składają się na wartość *NETCMN: *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 składowania i odtwarzania.
***SECCFG**	Kontrolowane jest konfigurowanie ochrony.

Tabela 50. Możliwe wartości dla wartości systemowej QAUDCTL (kontynuacja)

***SECDIRSRV**	Kontrolowane są zmiany lub aktualizacje podczas wykonywania funkcji usług katalogowych.
***SECIPC**	Kontrolowane są zmiany w komunikacji między procesami.
***SECNAS**	Kontrolowane są działania usługi uwierzytelniania sieciowego.
***SECRUN**	Kontrolowane są funkcje uruchamiania ochrony.
***SECSCKD**	Kontrolowane są deskryptory gniazda.
***SECURITY**	Protokołowane są funkcje związane z bezpieczeństwem. Wartość *SECURITY jest złożona z kilku wartości umożliwiających lepsze dostosowanie kontroli. Następujące wartości składają się na wartość *SECURITY: *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**	Protokołowane jest użycie funkcji zarządzania systemami.

Odsyłacze pokrewne

“Planowanie kontroli działań” na stronie 271
Wartość systemowa QAUDCTL (sterowanie kontrolą), wartość systemowa QAUDLVL (poziom kontroli), wartość systemowa QAUDLVL2 (rozszerzenie poziomu kontroli) oraz parametr AUDLVL (kontrola działania) w profilach użytkownika współpracują ze sobą w celu sterowania kontrolą działania:

Rozszerzenie poziomu kontroli (QAUDLVL2)

Wartość systemowa Rozszerzenie poziomu kontroli (Auditing Level Extension - 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. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących bezpieczeństwa i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe związane z bezpieczeństwem.

Tabela 51. Możliwe wartości dla wartości systemowej QAUDLVL2

***NONE**	W tej wartości systemowej nie są zawarte żadne wartości kontroli.
***NOTAVL**	Wartość ta wyświetlana jest wówczas, gdy wartość systemowa nie jest dostępna dla użytkownika, ponieważ użytkownik nie posiada uprawnień specjalnych *AUDIT ani *ALLOBJ. Wartości systemowej nie można przypisać tej wartości.
***ATNEVT**	Protokołowane są zdarzenia ostrzeżeń.

Tabela 51. Możliwe wartości dla wartości systemowej QAUDLVL2 (kontynuacja)

***AUTFAIL**	Protokołowane są zdarzenia błędu uprawnień.
***CREATE**	Protokołowane są operacje tworzenia obiektu.
***DELETE**	Protokołowane są operacje usunięcia obiektu.
***JOBBAS**	Kontrolowane są podstawowe funkcje zadania.
***JOBCHGUSR**	Kontrolowane są zmiany aktywnego profilu użytkownika wątku lub profili grupowych.
***JOBDTA**	Protokołowane są działania wpływające na zadanie. Wartość *JOBDTA jest złożona z dwóch wartości, *JOBBAS oraz *JOBCHGUSR, które umożliwiają lepsze dostosowanie kontroli. Określenie obu wartości jest równoznaczne z podaniem wartości *JOBDTA.
***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. Następujące wartości składają się na wartość *NETCMN: *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 między procesami.
***SECNAS**	Kontrolowane są działania usługi uwierzytelniania sieciowego.
***SECRUN**	Kontrolowane są funkcje wykonawcze bezpieczeństwa.
***SECSCKD**	Kontrolowane są deskryptory gniazda.

Tabela 51. Możliwe wartości dla wartości systemowej QAUDLVL2 (kontynuacja)

***SECURITY**	Protokołowane są funkcje związane z bezpieczeństwem. Parametr *SECURITY składa się z kilku wartości umożliwiających lepsze dostosowanie kontroli. Następujące wartości składają się na wartość *SECURITY: *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**	Protokołowane jest użycie funkcji zarządzania systemami.

Odsyłacze pokrewne

“Planowanie kontroli działań” na stronie 271
Wartość systemowa QAUDCTL (sterowanie kontrolą), wartość systemowa QAUDLVL (poziom kontroli), wartość systemowa QAUDLVL2 (rozszerzenie poziomu kontroli) oraz parametr AUDLVL (kontrola działania) w profilach użytkownika współpracują ze sobą w celu sterowania kontrolą działania:

Kontrola nowych obiektów (QCRTOBJAUD)

Wartość systemowa Kontrola nowych obiektów (Auditing for New Objects - QCRTOBJAUD) jest używana do określania wartości kontrolnej dla nowego obiektu, jeśli wartość domyślna kontroli tworzonego obiektu dla biblioteki lub katalogu 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 kontrolowania obiektów można zmienić za pomocą komend CHGOBJAUD lub CHGAUD.

Uwaga: Ta wartość systemowa jest wartością zastrzeżoną. Więcej szczegółów dotyczących ograniczania zmian w wartościach systemowych dotyczących bezpieczeństwa i pełna lista zastrzeżonych wartości systemowych znajduje się w sekcji Wartości systemowe związane z bezpieczeństwem.

Tabela 52. Możliwe wartości dla wartości systemowej QCRTOBJAUD:

***NONE**	Brak kontroli obiektu.
***NOTAVL**	Wartość ta wyświetlana jest wówczas, gdy wartość systemowa nie jest dostępna dla użytkownika, ponieważ użytkownik nie posiada uprawnień specjalnych *AUDIT ani *ALLOBJ. Wartości systemowej nie można przypisać tej wartości.
***USRPRF**	Kontrolowanie obiektu przeprowadzane jest w oparciu o wartość w profilu użytkownika uzyskującego dostęp do obiektu.
***CHANGE**	Rekord kontroli zapisywany jest za każdym razem, gdy do obiektu wprowadzana jest zmiana mająca związek z ochroną.

Tabela 52. Możliwe wartości dla wartości systemowej QCRTOBJAUD: (kontynuacja)

***ALL**	Rekord kontroli zapisywany jest dla każdej czynności związanej z ochroną, mającej wpływ na zawartość obiektu. Rekord kontroli zapisywany jest również, gdy do obiektu wprowadzana jest zmiana mająca związek z ochroną.

Zalecana wartość: wybrana wartość zależy od wymagań kontroli dla danej instalacji. Sekcja “Planowanie kontroli dostępu do obiektu” na stronie 296 udostępnia informacje dotyczące metod konfigurowania kontrolowania obiektu w systemie. Wartością kontroli można sterować z poziomu katalogu za pomocą parametru CRTOBJAUD komendy Tworzenie katalogu (Make Directory - CRTDIR) i wartości *CRTOBJAUD komendy Zmiana atrybutu (Change Attribute - CHGATR). Wartością kontroli można sterować także z poziomu biblioteki za pomocą parametru CRTOBJAUD komendy CRTLIB i komendy CHGLIB.

Rozdział 4. Profile użytkowników

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 zarządzanie profilami użytkowników oraz grup w systemie

Sposób używania:
Komenda Praca z profilami użytkowników (Work with User Profiles - WRKUSRPRF).

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

Uprawnienia:
Uprawnienie specjalne *SECADM.

Uprawnienie specjalne *AUDIT do zmiany kontroli użytkownika.

Pozycja kroniki:

AD dla zmian kontroli użytkownika.

CO dla utworzenia profilu użytkownika

CP dla zmian profili użytkowników.

DO dla usunięcia profilu użytkownika

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

Pojęcia pokrewne

"Profile użytkowników" na stronie 4
Każdy użytkownik systemu operacyjnego i5/OS ma swój profil użytkownika.

Role profilu użytkownika

Profil użytkownika zawiera hasło użytkownika, listę specjalnych uprawnień przypisanych do użytkownika oraz obiekty, które użytkownik posiada.

Profil użytkownika odgrywa 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. "Wartości domyślne dla profili użytkowników" na stronie 329, Dodatek B, "Profile użytkowników IBM", na stronie 329, 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 specjalnym typem profilu użytkownika, który nadaje takie same uprawnienia grupie użytkowników.

Profil grupowy pełni w systemie 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). Istnieje również możliwość ustawienia typu profilu na grupowy poprzez określenie wartości parametru gid podczas tworzenia profilu. Sekcja “Planowanie profili grupowych” na stronie 246 opisuje przykład konfigurowania profilu grupowego.

Pola parametrów w profilu użytkownika

W temacie przedstawiono informacje szczegółowe dotyczące pól parametrów w profilach użytkownika wyświetlanych w zachęcie komendy Tworzenie profilu użytkownika (Create User Profile).

Podczas tworzenia profilu użytkownika system nadaje mu uprawnienia: *OBJMGT, *CHANGE. Te uprawnienia są wymagane do wykonywania funkcji systemowych i nie powinny być usuwane.

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.

Następujące sekcje ilustrują nazewnictwo pól profilu użytkownika wywoływanych na ekranach podstawowego i pośredniego poziomu asysty.

Tytuł pola
Tytuł sekcji zawiera nazwę pola wyświetlaną w zachęcie komendy Tworzenie profilu użytkownika (Create User Profile). Tytuł ten jest wyświetlany zarówno gdy profil użytkownika jest tworzony w pośrednim poziomie asysty, jak i komendą 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 jest używana komenda Odtworzenie profilu użytkownika (Retrieve User Profile - RTVUSRPRF), jest to długość, której należy użyć do zdefiniowania pola związanego z parametrem.

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 odpowiednie wymienione 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

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).

Podpowiedź ekranu Dodanie użytkownika:
Użytkownik

Parametr CL:
USRPRF

Długość:
10

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 (@).

Nazwa profilu użytkownika nie może rozpoczynać się od cyfry.

Uwagi:

- Ekran Dodanie użytkownika (Add User) zezwala na podanie tylko ośmioznakowej nazwy użytkownika.
- 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 temat Programowanie w języku CL.

Zalecenia dotyczące nazywania profili użytkowników: Podczas podejmowania decyzji o tym 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 używane 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 związane z wersjami w języku narodowym programu licencjonowanego i5/OS.

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 nazewnictwa profili grupowych: Aby łatwo identyfikować profile grupowe w systemie, należy stosować konwencje nazewnictwa. Wszystkie nazwy profili grupowych powinny rozpoczynać się od tych samych znaków, na przykład GRP (od grupa) lub WYD (od wydziału).

Hasło

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.

Podpowiedź ekranu Dodanie użytkownika:
Hasło

Parametr CL:
PASSWORD

Długość:
128

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 Poziom hasła (Password Level - QPWDLVL) jest ustawiona 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 Wpisywanie się (Sign On) litera Q może zostać pominięta. Jeśli na ekranie Zmiana hasła (Change Password) użytkownik podał hasło Q12345, to na ekranie Wpisywanie się (Sign On) może podać albo 12345, albo Q12345. Gdy wartość systemowa QPWDLVL jest ustawiona na 2 lub 3, na ekranie Wpisywanie się się (Sign On) 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 Poziom hasła (Password Level - QPWDLVL) jest ustawiona na 2 lub 3, to w hasłach są rozróżniane małe i wielkie litery. Hasło może też zawierać odstępy. Hasło nie może jednak zaczynać się znakiem gwiazdki (’*’), zaś znaki odstępu na końcu hasła są obcinane.

Uwaga: Hasła można tworzyć przy użyciu znaków dwubajtowych. Jednak hasła zawierającego znaki dwubajtowe nie można użyć w celu wpisania się do systemu na ekranie Wpisywanie się (Sign On). 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, osoba odpowiedzialna za bezpieczeństwo 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. W wymienionych poniżej sytuacjach użytkownik nie może ustawić hasła równego nazwie profilu użytkownika, posługując się komendą CHGPWD, menu ASSIST lub funkcją API QSYCHGPW:

- gdy wartość systemowa QPWDRULES jest równa *PWDSYSVAL, natomiast wartość systemowa Minimalna długość hasła (Password Minimum Length - QPWDMINLEN) nie jest równa 1,
- gdy wartość systemowa QPWDRULES jest równa *PWDSYSVAL, a wartość systemowa Maksymalna długość hasła (Password Maximum Length - QPWDMAXLEN) nie jest równa 10,
- gdy wartość systemowa QPWDRULES jest równa *PWDSYSVAL, natomiast jedna z pozostałych wartości systemowych kompozycji hasła została zmieniona na ustawienie inne niż domyślne.

Więcej informacji na temat ustawiania wartości systemowych kompozycji hasła zawiera temat “Wartości systemowe mające zastosowanie dla haseł” na stronie 47.

Tabela 53. Dozwolone wartości parametru PASSWORD:

***USRPRF**	Hasło dla tego użytkownika jest takie samo, jak jego nazwa profilu. Gdy wartość systemowa Poziom hasła (Password Level - QPWDLVL) jest ustawiona na 2 lub 3, hasło będzie takie samo jak nazwa profilu użytkownika, ale pisana wielkimi literami. Dla profilu JANKOWALSKI, hasło to JANKOWALSKI, a nie jankowalski.
***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.
użytkownik- hasło	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 lub QPWDRULES, aby ograniczyć długość haseł. 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 (Set password to expired)

Pole *Ustawienie hasła jako wygasłe* umożliwia administratorowi ochrony wskazanie w profilu użytkownika, że jego hasło wygasło i musi być zmienione podczas następnego wpisywania się.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
PWDEXP

Długość:
4

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 “Okres ważności hasła” na stronie 93). Użytkownik może nacisnąć klawisz Enter, aby podać nowe hasło, lub klawisz F3 (Wyjście - Exit), 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, należy zmienić
hasło.

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

Rysunek 1. Komunikat o wygaśnięciu hasła

Tabela 54. Dozwolone wartości 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

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.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
STATUS

Długość:
10

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. “Aktywowanie profilu użytkownika” na stronie 127 zawiera przykład programu adoptującego uprawnienia, który umożliwia operatorowi systemu włączanie profilu.

W zależności od ustawień wartości systemowych QMAXSIGN i QMAXSGNACN system może zablokować profil po pewnej liczbie nieudanych prób weryfikowania hasła dla tego profilu.

Za pomocą profilu QSECOFR (osoba odpowiedzialna za bezpieczeństwo) 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 55. 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

Klasa użytkownika używana jest do sterowania tym, jakie opcje menu użytkownik widzi w menu systemu i5/OS. Pomaga to w kontrolowaniu dostępu użytkowników do pewnych funkcji systemu.

Podpowiedź ekranu Dodanie użytkownika:
Rodzaj użytkownika

Parametr CL:
USRCLS

Długość:
10

To niekoniecznie ogranicza użycie komend. To pole *Ograniczenie możliwości* określa, 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 56 opisuje możliwe klasy użytkowników oraz domyślne uprawnienia specjalne każdej z klas. Pozycje wskazują, że uprawnienie jest nadawane tylko na poziomach bezpieczeństwa 10 i 20, na wszystkich poziomach bezpieczeństwa lub wcale nie jest nadawane.

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

Tabela 56. Domyślne uprawnienia specjalne według klasy użytkownika

Uprawnienia 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				

Tabela 56. Domyślne uprawnienia specjalne według klasy użytkownika (kontynuacja)

Uprawnienia specjalne	Klasy użytkowników				
	***SECOFR**	***SECADM**	***PGMR**	***SYSOPR**	***USER**
*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

Pole *Poziom asysty* w profilu użytkownika używane jest do określania domyślnego poziomu asysty podczas tworzenia profilu użytkownika. Platforma System i udostępnia trzy poziomy asysty: basic (podstawowy), intermediate (średni) i advanced (zaawansowany).

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.

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 57 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 57. Jak są zapamiętywane i zmieniane poziomy asysty

Podjęte działanie	Wersja wyświetlonego ekranu	Wersja zapamiętanego 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 średniego poziomu asysty.	Ekran Praca z profilami użytkowników	Zmieniony na średni 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)		Zmieniony na podstawowy poziom asysty

Tabela 57. Jak są zapamiętywane i zmieniane poziomy asysty (kontynuacja)

Podjęte działanie	Wersja wyświetlonego ekranu	Wersja zapamiętanego ekranu
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 “Opcje użytkownika” na stronie 110.

Tabela 58. 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

Termin *biblioteka bieżąca* oznacza bibliotekę określoną jako pierwsza biblioteka użytkownika do przeszukania w odpowiedzi na żądanie wyszukania obiektów przez użytkownika. Jeśli użytkownik utworzy obiekty i określi *CURLIB, obiekty zostaną umieszczone w bibliotece bieżącej.

Podpowiedź ekranu Dodanie użytkownika:
Biblioteka domyślna

Parametr CL:
CURLIB

Długość:
10

Uprawnienie
*USE

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 213 udostępnia więcej informacji dotyczących używania listy bibliotek oraz biblioteki bieżącej.

Tabela 59. Dozwolone wartości dla 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: Za pomocą pola *Biblioteka bieżąca* można kontrolować miejsce, w którym użytkownicy mogą umieszczać nowe obiekty, np. programy Zapytania. Pola *Ograniczenie możliwości* można użyć do zapobiegania zmienianiu przez użytkowników swoich bibliotek bieżących.

Program początkowy

Można podać nazwę programu, który zostanie wywołany po wpisaniu się użytkownika. Taki program nosi nazwę programu początkowego. Program początkowy jest uruchamiany przed wyświetleniem menu początkowego, jeśli takie istnieje.

Podpowiedź ekranu Dodanie użytkownika:
Program wpisywania się

Parametr CL:
INLPGM

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

Uprawnienia:
*USE do programu, *EXECUTE do biblioteki

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 205.

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 60. 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 61. 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

Można podać nazwę 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.

Podpowiedź ekranu Dodanie użytkownika:
Pierwsze menu

Parametr CL:
INLMNU

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

Uprawnienie
*USE do menu, *EXECUTE do biblioteki

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 62. Możliwe wartości parametru MENU:

MAIN	Zostaje wyświetlone Menu Główne systemu System i.
***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 63. 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

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 narzędziem zabezpieczającym przed eksperymentowaniem przez użytkowników w systemie.

Podpowiedź ekranu Dodanie użytkownika:
Ograniczenie użycia wiersza komend

Parametr CL:
LMTCPB

Długość:
10

Użytkownik z ograniczonymi możliwościami może uruchomić tylko te komendy, które zdefiniowano jako dozwolone dla użytkowników z ograniczonymi możliwościami. Następujące 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 i parametr ALWLMTUSR w komendach dotyczą tylko komend uruchamianych z wiersza komend, ekranu wpisywania komend, FTP, REXEC, używając API QCAPCMD, lub opcji z menu grupowania komend. Użytkownicy mogą bez ograniczeń wykonywać następujące czynności:

- wykonywanie komend w programach CL, które uruchamiają komendy jako wynik wyboru opcji z menu,
- wykonywanie komend zdalnych poprzez aplikacje.

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 64 zawiera informacje o możliwych wartościach pola Ograniczenie możliwości i funkcjach dozwolonych dla poszczególnych wartości.

Tabela 64. Funkcje dozwolone dla wartości pola Ograniczenie możliwości

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

[1] Domyślnie dozwolone są następujące 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.

Pojęcia pokrewne

“Planowanie menu” na stronie 235
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.

Tekst

Tekst w profilu użytkownika służy do opisu danego profilu użytkownika oraz jego przeznaczenia.

Podpowiedź ekranu Dodanie użytkownika:
Opis użytkownika

Parametr CL:
TEXT

Długość:
50

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 65. Możliwe wartości tekstu:

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

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

Uprawnienia specjalne

Uprawnienia specjalne są używane do określania typów działań, które użytkownik może wykonać na zasobach systemu. Użytkownik może mieć nadane jedno lub więcej uprawnień specjalnych.

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.

Tabela 66. 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 56 na stronie 81 zawiera 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 *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.

Uprawnienie 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,
- Nadawanie użytkownikowi uprawnienia do kodu dostępu i usuwanie tego uprawnienia.
- nadawać i odbierać użytkownikom zezwolenia na pracę w imieniu innych użytkowników.
- 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 Sterowanie zadaniami (*JOBCTL) umożliwiają użytkownikowi zmianę priorytetu zadań oraz drukowania, zakończenie zadania przed jego wykonaniem oraz usunięcie danych wyjściowych przed ich wydrukowaniem. Uprawnienia specjalne *JOBCTL mogą również dać użytkownikowi dostęp do poufnych buforowanych danych wyjściowych, jeśli dla kolejek wyjściowych został określony parametr OPRCTL(*YES).

Uprawnienia specjalne sterowania zadaniami (*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 217.

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.

Czynniki ryzyka: Użytkownik, który nadużywa uprawnień specjalnych *JOBCTL, może utrudniać wykonywanie pojedynczych zadań, a przez to powodować spadek wydajności całego systemu.

Uprawnienia specjalne *SPLCTL

Uprawnienia specjalne kontroli buforu (*SPLCTL) umożliwiają użytkownikowi wykonywanie wszystkich funkcji dotyczących kontroli buforu, 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.

Uprawnienie 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 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 użytkownik ma tylko uprawnienie *USE oraz wyświetlanie i zmienianie funkcji serwisowych. Pozwalają też użytkownikowi wykonywać funkcje śledzenia.

Funkcja zrzutu może być wykonana bez uprawnień *SERVICE.

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, użytkownikom można nadać uprawnienia do wykonywania śledzenia serwisowego, bez uprawnień specjalnych *SERVICE. Dzięki temu tylko określeni użytkownicy mają możliwość korzystania z komendy śledzenia, która może dać im dostęp do poufnych danych. Użytkownik musi być upoważniony do korzystania z komendy i mieć albo uprawnienie specjalne *SERVICE, albo upoważnienie do funkcji śledzenia serwisowego w systemie operacyjnym i5/OS poprzez Administrowanie aplikacjami w programie System i 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:

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)
TRCTCPAPP	Aplikacja śledzenia TCP/IP
WRKTRC	Praca ze śledzeniem

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

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 potrzebują dostępu do pozostałych narzędzi serwisowych oraz debugowania.

Wykonaj poniższe czynności, aby ograniczyć liczbę użytkowników, którzy mogą mieć dostęp do komend śledzenia bez użycia uprawnień *SERVICE:

1. W programie System i Navigator otwórz element Użytkownicy i grupy.
2. Aby wyświetlić listę profili użytkowników, wybierz opcję **Wszyscy użytkownicy**.
3. Prawym przyciskiem myszy kliknij profil użytkownika, który ma być zmieniony.
4. Wybierz opcję **Właściwości**.
5. Kliknij opcję **Możliwości**.
6. Otwórz zakładkę Aplikacje.
7. Wybierz opcję **Dostęp do**.
8. Wybierz zakładkę **Aplikacje hosta**.
9. Wybierz opcję **System operacyjny**.
10. Wybierz opcję **Usługa**.
11. Odbierz dostęp do komendy śledzenia za pomocą pola wyboru.

Użytkownikom można również przydzielić dostęp do komend śledzenia za pomocą komendy Zmiana wykorzystania funkcji (Change Function Usage - CHGFCNUSG). Wpisz CHGFCNUSG FCNID(QIBM_SERVICE_TRACE) USER(profil_użytkownika) USAGE(*ALLOWED).

Uprawnienia specjalne *AUDIT

Uprawnienia specjalne kontroli (*AUDIT) dają użytkownikowi możliwość wyświetlania i zmiany charakterystyk kontroli.

Użytkownik z uprawnieniami specjalnymi *AUDIT może wykonywać następujące zadania:

- zmieniać i wyświetlać wartości systemowe sterujące kontrolami
- użyć komend CHGOBJAUT, CHGDLOAUD i CHGAUD, aby zmienić kontrolę dla obiektów
- użyć komendy CHGUSRAUD, aby zmienić kontrolę dla użytkownika
- wyświetlić wartości kontroli obiektu
- wyświetlić wartości kontroli profilu użytkownika
- uruchomić niektóre z komend narzędzi bezpieczeństwa, takie jak PRTADPOBJ

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.

Aby zapobiec wyświetlaniu informacji związanych z kontrolą przez zwykłych użytkowników, należy ograniczyć dostęp zwykłych użytkowników do następujących informacji:

- kroniki kontroli ochrony (QAUDJRN)
- innych kronik zawierających dane kontroli
- zbiorów składowania, zbiorów wyjściowych, zbiorów buforowania i wydrukowanych danych zawierających informacje kontroli

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. Użytkownicy o tych uprawnieniach specjalnych mogą dodawać lub usuwać informacje o konfiguracji komunikacji, pracować z serwerami TCP/IP oraz konfigurować serwer ICS (Internet Connection Server). Większość komend do konfigurowania komunikacji wymaga uprawnień specjalnych *IOSYSCFG.

Zalecenia dla uprawnień specjalnych: Nadawanie uprawnień specjalnych użytkownikom stanowi ryzyko naruszenia bezpieczeństwa. 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 działać z uprawnieniami właściciela programu

Programy adoptują uprawnienia specjalne *ALLOBJ właściciela, jeśli:

- programy są tworzone przez użytkowników mających uprawnienia specjalne *ALLOBJ,
- użytkownik określa parametr dla komendy USRPRF(*OWNER) tworzącej program

Środowisko specjalne

Użytkownik może działać w systemie System i5, 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.

Podpowiedź ekranu Dodanie użytkownika:
Brak

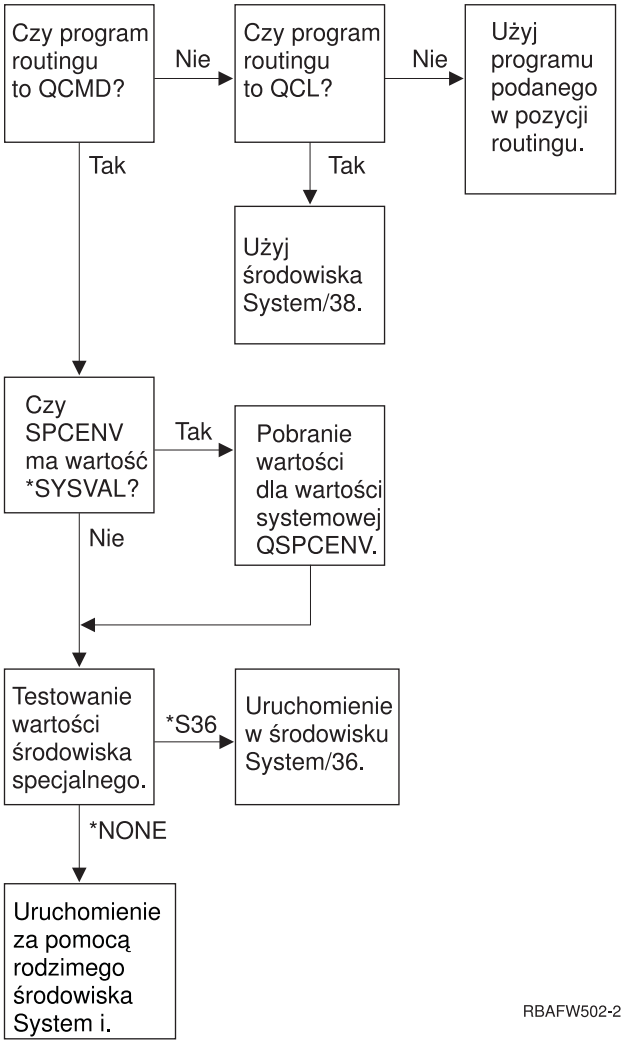
Parametr CL:
SPCENV

Długość:
10

Tabela 67. 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 System i5.
***S36**	Użytkownik działa w środowisku System/36, jeśli jego programem routingu jest program QCMD.

Zalecenia: Jeśli użytkownik uruchamia kombinację aplikacji systemu System i 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 System i.



Rysunek 2. Opis środowiska specjalnego

Opis środowiska specjalnego wRys. 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 wartość jest ustawiona, system pobiera wartość systemową QSPCENV i sprawdza specjalną wartość środowiskową. 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 jest ustawiona na *NONE, system uruchamia zintegrowane środowisko System i.

Wyświetlenie informacji wpisania się

Ekran Informacje wpisywania to narzędzie, które pozwala użytkownikom monitorować profile i wykrywać próby niewłaściwego użytkowania.Pole Wyświetlenie informacji wpisania się określa, czy podczas wpisywania się wyświetlany jest ekran Informacje wpisania się (Sing-On Information).

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
DSPSGNINF

Długość:
7

Rys. 3 opisuje ekran. Informacje o wygasaniu haseł są wyświetlane wyłącznie wtedy, gdy hasło wygasa podczas okresu dni ostrzegania o wygaśnięciu haseł.

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

Nieważne kontrole poprawności haseł . . . . . :   3

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

Rysunek 3. Ekran Informacje wpisania się

Tabela 68. Dozwolone wartości dla 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: Zaleca się wyświetlanie 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

Okres ważności hasła steruje liczbą dni, przez które hasło może być używane, zanim trzeba będzie je zmienić.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
PWDEXPITV

Długość:
5,0

Gdy hasło użytkownika wygaśnie, na ekranie wpisywania się otrzyma on komunikat. Użytkownik może nacisnąć klawisz Enter, aby podać nowe hasło, lub klawisz F3 (Wyjście - Exit), 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. “Okres ważności hasła” pokazuje przykład komunikatu o utracie ważności hasła.

Tabela 69. Dozwolone wartości 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. Pole Okres ważności hasła (Password expiration interval) w profilu użytkownika umożliwia wprowadzenie wymogu częstszej zmiany haseł użytkowników z uprawnieniami specjalnymi *SERVICE, *SAVSYS, *SECADM lub *ALLOBJ.

Blokada zmiany hasła

Parametr blokady zmiany hasła definiuje okres, przez który nie można zmienić hasła po uprzedniej, pomyślnie zrealizowanej operacji zmiany.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
PWDCHGBLK

Długość:
10

Ta wartość parametru nie ogranicza zmian haseł dokonywanych przy użyciu komendy Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF). Ponadto parametr ten nie jest wymuszany, jeśli pole Ustawienie hasła jako wygasłe (Set password to expired - PWDEXP) w profilu użytkownika ma wartość *YES. Umożliwia to administratorowi bezpieczeństwa tworzenie profilu użytkownika z nieważnym hasłem przy jednoczesnym umożliwieniu użytkownikowi wpisania się i zmiany hasła (jednorazowo) bez nakładania ograniczenia przez wartość systemową blokady zmiany hasła.

Tabela 70. Dozwolone wartości parametru PWDCHGBLK:

***SYSVAL**	Używana jest wartość systemowa QPWDCHGBLK.
***NONE**	Hasło można zmienić w dowolnej chwili.
1 - 99	Hasło można zmienić po upływie określonej liczby godzin od poprzedniej, pomyślnej zmiany hasła.

Zalecenia: Wartość tego parametru należy ustawić na *SYSVAL, chyba że zauważy się nietypowe operacje zmiany hasła u konkretnego użytkownika. W takim przypadku należy ustawić ten parametr na pewną wartość, np. 2, aby ograniczyć częstotliwość zmiany hasła przez tego użytkownika.

Lokalne zarządzanie hasłami

Parametr Lokalne zarządzanie hasłami (LCLPWDMGT) określa, czy hasło profilu użytkownika jest zarządzane lokalnie. Jeśli hasło nie jest zarządzane lokalnie, użytkownicy nie mogą uzyskać dostępu przez bezpośrednie wpisanie się, lecz muszą korzystać z pośrednictwa innych platform.

Jeśli hasło zarządzane jest lokalnie, przechowywane jest razem z profilem użytkownika. Jest to tradycyjna metoda przechowywania hasła.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
LCLPWDMGT

Długość:
10

Jeśli hasło nie jest zarządzane lokalnie, lokalne hasło platformy i5/OS i5/OS ma przypisane ustawienie *NONE. Wartość hasła określona w parametrze hasła zostanie wysłana do innych produktów IBM obsługujących synchronizację haseł, takich jak IBM i5/OS Integration for Windows Server. Użytkownicy nie będą mogli zmienić utworzonych przez siebie haseł za pomocą komendy Zmiana hasła (Change Password - CHGPWD). Ponadto nie będą mogli bezpośrednio wpisać się do systemu. Określenie tej wartości wpłynie na inne produkty IBM obsługujące synchronizację haseł, jak IBM i5/OS Integration for Windows Server.

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

Tabela 71. Możliwe wartości parametru LCLPWDMGT:

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

Ograniczenie sesji urządzeń

Pole Ograniczenie sesji urządzeń służy do określenia, czy liczba sesji urządzeń dopuszczalnych dla użytkownika jest ograniczona. Ta wartość nie ogranicza użycia menu System Request lub drugiego wpisywania się do tego samego urządzenia.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
LMTDEVSSN

Długość:
7

Tabela 72. 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.
0	Limit sesji urządzeń dla użytkownika nie jest ograniczony do określonej liczby. Wartość ta ma takie samo znaczenie co wartość *NO.
1	Limit sesji urządzeń dla użytkownika jest ograniczony do 1. Wartość ta ma takie samo znaczenie co wartość *YES.
2 - 9	Limit sesji urządzeń dla użytkownika jest ograniczony do określonej liczby.

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

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

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
KBDBUF

Długość:
10

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 73. 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.

Maksymalna wielkość pamięci

W systemie można określić maksymalną ilość pamięci dyskowej wykorzystywanej do przechowywania obiektów trwałych, których właścicielem jest profil użytkownika. W tej samej pamięci są przechowywane obiekty, które system umieszcza w bibliotece tymczasowej (QTEMP) podczas zadania.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
MAXSTG

Długość:
11,0

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. Z tego powodu ustawienie wartości 5000 oznacza, że profil użytkownika może korzystać z następujących rozmiarów pamięci dyskowej:

- 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 łącznie 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 właścicielami 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.
- System przypisuje pamięć na opisy obiektów, które umieszczane są w bibliotece, właścicielowi tej biblioteki. Dzieje się tak nawet wtedy, gdy właścicielem obiektów jest inny profil użytkownika. Przykładami takich opisów są odniesienia do tekstu i programu.
- System przypisuje profilowi użytkownika pamięć na obiekty tymczasowe, które są wykorzystywane podczas przetwarzania zadania. Przykładem takich obiektów są bloki kontroli transakcji, przestrzenie edycji zbiorów oraz dokumenty.

Tabela 74. Możliwe wartości parametru MAXSTG:

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

Ograniczenie priorytetu

Ograniczenie priorytetu w profilu użytkownika określa maksymalne priorytety planowania (priorytet zadania i wyjścia), które są dozwolone dla zadań wprowadzanych przez użytkownika. Ograniczenie priorytetu steruje priorytetem zadania, gdy jest ono wprowadzane. Steruje również wszystkimi zmianami priorytetu zadania w czasie, gdy zadanie oczekuje w kolejce lub jest wykonywane.

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 można ustawić w opisie zadania lub za pomocą komendy wprowadzania.

Priorytet wyjścia:
Określa priorytet harmonogramu dla wyjścia tworzonego przez zadanie w kolejce wyjściowej. Priorytet wyjścia można ustawić w opisie zadania lub podczas używania komendy wprowadzania.

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 75. 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

Opis zadania zawiera określony zestaw atrybutów związanych z zadaniem, takich jak kolejka zadania, która ma być użyta, priorytet planowania, dane routingu, ważność kolejki komunikatów, lista bibliotek oraz informacje wyjściowe. Atrybuty określają, jak poszczególne zadania są wykonywane w systemie.

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.

Więcej informacji dotyczących opisów zadań oraz ich użycia zawiera sekcja Zarządzanie pracą.

Tabela 76. 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 77. Możliwe wartości 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 (Lista bibliotek użytkownika).

Profil grupowy

Parametr Profil grupowy (GRPPRF) określa, czy użytkownik jest członkiem profilu grupowego. 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.

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 adoptujące uprawnienia właściciela” na stronie 153.

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 numer identyfikacyjny grupy (gid) dla profilu grupowego, o ile profil jeszcze go nie posiada.

W momencie zmiany wartości GRPPRF, zmiana ta wchodzi w życie przy następnym wpisaniu się użytkownika lub przy następnym przełączeniu przez zadanie na profil użytkownika korzystającego z uchwytu lub tokenu profilu, otrzymanego po wprowadzeniu zmiany.

Więcej informacji na temat używania profili grupowych zawiera sekcja “Planowanie profili grupowych” na stronie 246.

Tabela 78. 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

Jeśli użytkownik jest członkiem grupy, można użyć parametru Właściciel w profilu użytkownika w celu określenia, 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 w polu Profil grupowy znajduje się wartość inna niż *NONE.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
OWNER

Długość:
10

Każda zmiana wartości w polu Właściciel zaczyna obowiązywać od następnego wpisania się użytkownika lub od następnego przełączenia zadania na profil użytkownika za pomocą uchwytu lub tokenu profilu otrzymanego po wprowadzeniu zmiany.

Tabela 79. Możliwe wartości w polu Właściciel:

***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.

Uprawnienie grupowe

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.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
GRPAUT

Długość:
10

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.

Kiedy następuje zmiana wartości GRPAUT, odnosi ona skutek przy następnym wpisaniu się użytkownika lub przy następnym przełączeniu przez zadanie na profil użytkownika korzystającego z uchwytu lub tokenu profilu, otrzymanego po wprowadzeniu zmiany.

Tabela 80. 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.

Tabela 80. Możliwe wartości parametru GRPAUT: (kontynuacja)

***EXCLUDE**	Profil grupowy ma wyraźnie odmówiony dostęp do wszystkich obiektów tworzonych przez użytkownika.

Odsyłacze pokrewne

"Definiowanie sposobów dostępu do informacji" na stronie 136
Użytkownik może zdefiniować, które operacje mogą być wykonywane na obiektach, danych i polach.

Typ uprawnień grupowych

Gdy użytkownik tworzy nowy obiekt, parametr Typ uprawnień grupowych w jego profilu określa, jaki typ uprawnień do tego obiektu otrzymuje grupa użytkownika.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
GRPAUTTYP

Długość:
10

Parametr GRPAUTTYP współpracuje z parametrami OWNER, GRPPRF i GRPAUT, aby określić uprawnienia grupy do nowego obiektu.

Kiedy następuje zmiana wartości GRPAUTTYP, odnosi ona skutek przy następnym wpisaniu się użytkownika lub przy następnym przełączeniu przez zadanie na profil użytkownika korzystającego z uchwytu lub tokenu profilu, otrzymanego po wprowadzeniu zmiany.

Tabela 81. 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. Można podać tę wartość tylko wtedy, gdy wartość GRPAUT to *NONE.

[1] Uprawnienia prywatne i uprawnienia grupy podstawowej zapewniają taki sam dostęp do obiektu dla członków grupy, ale mogą mieć inną charakterystykę wydajności. Sekcja "Grupa podstawowa obiektu" na stronie 148 wyjaśnia sposób działania uprawnień grupy podstawowej.

Zalecenia: Podanie wartości *PGP jest metodą na rozpoczęcie korzystania z uprawnień grupy podstawowej. Należy rozważyć skorzystanie z parametru GRPAUTTYP(*PGP) w przypadku użytkowników często tworzących nowe obiekty, do których dostęp muszą uzyskiwać członkowie danego profilu grupowego.

Grupy dodatkowe

Grupy dodatkowe można określić podczas tworzenia lub zmiany profilu użytkownika. Użytkownik nie może mieć dodatkowych profili grupowych, jeśli parametr GRPPRF ma wartość *NONE.

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 adoptujące uprawnienia właściciela” na stronie 153.

Można podać nazwy maksymalnie 15 profili, z których użytkownik otrzyma uprawnienia. Użytkownik staje się członkiem każdego dodatkowego profilu grupowego.

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 oznaczy go jako profil grupowy. Wygeneruje także numer identyfikacyjny grupy dla profilu grupowego, jeśli ten jeszcze takiego nie ma.

W momencie zmiany wartości SUPGRPPRF, zmiana ta odnosi skutek przy następnym wpisywaniu się użytkownika lub przy następnym przełączeniu przez zadanie na profil użytkownika korzystającego z uchwytu lub tokenu profilu, otrzymanego po wprowadzeniu zmiany.

Więcej informacji na temat używania profili grupowych zawiera sekcja “Planowanie profili grupowych” na stronie 246.

Tabela 82. 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. Nazwa profilu określona dla GRPPRF może również zostać określona jako jeden z 15 dodatkowych profili grupowych.

Kod rozliczeniowy

Określenie kodu rozliczeniowego pozwala na zebranie informacji o zasobach systemu używanych przez zadanie.

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).

Zmiana wartości *kodu rozliczeniowego* odnosi skutek po następnym wpisaniu się użytkownika lub po następnym uruchomieniu zadania przy użyciu wartości kodu rozliczeniowego profilu użytkownika.

Więcej informacji na temat rozliczania zadania można znaleźć w temacie Zarządzanie pracą.

Tabela 83. 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

Hasło dla dokumentu kontroluje dostępność i dystrybucję poczty osobistej, gdy jest ona wyświetlana przez osoby pracujące w imieniu użytkownika. Hasło dla dokumentu jest obsługiwane przez produkty obsługujące Document Interchange Architecture (DIA), takie jak Displaywriter.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
DOCPWD

Tabela 84. Dozwolone wartości dla DOCPWD:

***NONE**	Dla danego użytkownika nie jest używane hasło do dokumentów.
hasło-dla- 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

Kolejka komunikatów jest obiektem, w którym umieszczane są komunikaty wysyłane do osoby lub programu. Kolejka komunikatów jest używana, gdy użytkownik wysyła lub otrzymuje komunikaty.

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.

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 85. 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 86. Możliwe wartości 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: Każdemu profilowi użytkownika należy dać unikalną kolejkę komunikatów, najlepiej o tej samej nazwie co profil użytkownika.

Dostarczenie

Tryb dostarczenia kolejki komunikatów określa, czy użytkownik jest powiadamiany o nowym komunikacie w kolejce.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
DLVRY

Długość:
10

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 87. Dozwolone wartości dla DLVRY:

***NOTIFY**	Zadanie, do którego przypisywana jest kolejka komunikatów w chwili, gdy w kolejce pojawi się komunikat. W przypadku zadań interaktywnych przy stacji roboczych, rozbrzmiewa alarm dźwiękowy i rozświetla się kontrolka czekającego komunikatu. 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 zadanie jest zadaniem interaktywnym, rozbrzmiewa alarm (jeśli zainstalowano). 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

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

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
SEV

Długość:
2,0

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 88. 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-poziomu- 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

Dla każdego użytkownika można określić drukarkę, na której będą drukowane dane wyjściowe tego użytkownika. Jeśli jako kolejka wyjściowa (OUTQ) jest podana drukarka (*DEV), zbiory buforowe są umieszczane w kolejce wyjściowej o takiej samej nazwie, jak drukarka.

Podpowiedź ekranu Dodanie użytkownika:
Drukarka domyślna

Parametr CL:
PRTDEV

Długość:
10

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 sekcja Podstawy drukowania.

Tabela 89. 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

Zarówno przetwarzanie interaktywne jak i wsadowe mogą spowodować powstanie zbiorów buforowych, które zostaną wysłane do drukarki. Zbiory buforowe umieszczane są w kolejce wyjściowej. W systemie może być wiele różnych kolejek wyjściowych.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
OUTQ

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

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

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 sekcja Advanced Function Presentation.

Tabela 90. 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 91. 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 której znajduje się kolejka wyjściowa.

Program obsługi klawisza ATTN

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

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
ATNPGM

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

Uprawnienia:
*USE do programu

*EXECUTE do biblioteki

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 205.

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

Tabela 92. Możliwe wartości parametru ATNPGM:

***SYSVAL**	Użyta zostanie wartość systemowa QATNPGM.
***NONE**	Przez tego użytkownika nie jest używany żaden program obsługi klawisza ATTN.

Tabela 92. Możliwe wartości parametru ATNPGM: (kontynuacja)

***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 93. Możliwe wartości 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

Kolejność sortowania jest używana dla danych wyjściowych tego użytkownika. Można użyć tabel sortowania udostępnianych przez system lub utworzyć własne. Tabelę sortowania można powiązać z danym identyfikatorem języka w systemie.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
SRTSEQ

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

Uprawnienia:
*USE do tabeli, *EXECUTE do biblioteki

Tabela 94. 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 95. 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

Dla użytkownika można podać identyfikator języka, który będzie używany przez system.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
LANGID

Długość:
10

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 96. Możliwe wartości parametru LANGID:

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

Identyfikator kraju lub regionu:

Dla użytkownika można podać identyfikator kraju lub regionu, który będzie używany przez system.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
CNTRYID

Długość:
10

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 97. Dozwolone wartości dla 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

Dla użytkownika można podać identyfikator kodowanego zestawu znaków, który będzie używany przez system.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
Identyfikator CCSID

Długość:
5,0

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 98. 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

Atrybut *CHRIDCTL* steruje typem konwersji kodowanego zestawu znaków, która występuje dla zbiorów ekranowych, zbiorów drukarkowych i paneli grupowych.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
CHRIDCTL

Długość:
10

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 99. 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. W momencie otrzymania danych wejściowych, dane znaków przekształcane są w razie potrzeby z CHRID urządzenia na 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

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

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
SETJOBATR

Długość:
160

Tabela 100. 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.
***CCSID**	Użyty zostanie identyfikator kodowanego zestawu znaków (CCSID) 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.

Tabela 100. Możliwe wartości parametru SETJOBATR: (kontynuacja)

***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.

Można podać kombinację następujących wartości:

- *CCSID
- *DATFMT
- *DATSEP
- *DECFMT
- *SRTSEQ
- *TIMSEP

Ustawienia narodowe

Pole Ustawienia narodowe określa nazwę ścieżki ustawień narodowych przypisanych zmiennej środowiskowej LANG dla danego użytkownika.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
LOCALE

Tabela 101. 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.
ścieżka_do_ustawień_narodowych	Nazwa ścieżki ustawień narodowych, które mają być przypisane danemu użytkownikowi.

Opcje użytkownika

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

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
USROPT

Długość:
240 (10 znaków każda)

Tabela 102. 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.

Tabela 102. Możliwe wartości parametru USROPT: (kontynuacja)

***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 (Wyświetl szczegóły). W sekcji “Ekrany uprawnień” na stronie 159 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

Zintegrowany system plików korzysta z numeru identyfikacyjnego użytkownika (UID) w celu identyfikacji użytkownika i weryfikacji jego uprawnień. Każdy użytkownik w systemie ma unikalny numer UID.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
UID

Długość:
10,0

Tabela 103. Możliwe wartości numeru UID:

***GEN**	System wygeneruje unikalny numer UID dla tego użytkownika. Wygenerowany numer UID będzie większy niż 100.
uid	Wartość od 1 do 4294967294, która zostanie przypisana jako numer UID dla tego użytkownika. Numer ten nie może być już przypisany innemu użytkownikowi.

Zalecenia: W przypadku większości instalacji należy pozwolić na wygenerowanie przez system numerów UID dla nowych użytkowników, podając parametr UID(*GEN). Jednak jeśli system jest częścią sieci, może istnieć konieczność przypisywania numerów UID, które są zgodne z tymi w pozostałych systemach. Skonsultuj się z administratorem sieci.

Numer identyfikacyjny grupy

Zintegrowany system plików używa numeru identyfikacyjnego grupy (gid) do identyfikowania tych profili, które są profilami grupowymi. Profil używany jako profil grupowy musi posiadać numer identyfikacyjny grupy (gid).

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
GID

Długość:
10,0

Tabela 104. Możliwe wartości parametru GID:

***NONE**	Ten profil nie posiada numeru identyfikacyjnego grupy (gid). Wartość ta musi zostać podana, jeśli profil użytkownika jest elementem grupy (parametr GRPPRF ma wartość *NONE).

Tabela 104. Możliwe wartości parametru GID: (kontynuacja)

***GEN**	Dla tego profilu system generuje unikalny numer identyfikacyjny grupy (gid). Będzie on większy od 100.
gid	Wartość od 1 do 4294967294, która ma być przypisana jako numer identyfikacyjny grupy (gid) dla tego profilu. Numer identyfikacyjny grupy (gid) nie może być już przypisany innemu profilowi.

Zalecenia: W przypadku większości instalacji należy podać parametr GID(*GEN), co powoduje generowanie numeru identyfikacyjnego grupy (gid) przez system. Jeśli jednak system jest częścią sieci, może być konieczne przypisanie numerów identyfikacyjnych grupy (gid), które są zgodne z tymi w pozostałych systemach. W tym celu należy skonsultować się z administratorem sieci.

Nie można przypisywać numeru identyfikacyjnego grupy (gid) profilowi użytkownika, który nie będzie używany jako profil grupowy. W niektórych środowiskach dla użytkownika, który jest wpisany i posiada numer identyfikacyjny grupy (gid), istnieją graniczenia w wykonywaniu niektórych funkcji.

Katalog osobisty

Katalog osobisty jest początkowym katalogiem roboczym użytkownika w zintegrowanym systemie plików. Katalog osobisty jest katalogiem bieżącym użytkownika, jeśli nie podano innego katalogu bieżącego.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
HOMEDIR

Jeśli katalog osobisty określony w profilu nie istnieje w momencie wpisania się użytkownika, za katalog osobisty użytkownika uznawany jest katalog główny (/).

Tabela 105. 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

Powiązanie EIM określa, czy do identyfikatora EIM tego użytkownika należy dodać powiązanie EIM (odwzorowywanie tożsamości przesiębiorstwa). Opcjonalnie, jeśli identyfikator EIM jeszcze nie istnieje, to zostanie utworzony.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
EIMASSOC

Uwagi:

1. Informacje powiązania EIM 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 106. Dozwolone wartości dla EIMASSOC, wartości pojedyńcze:

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

Tabela 107. Dozwolone wartości dla 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 108. Dozwolone wartości dla EIMASSOC, element 2:

Element 2: Typ powiązania Określa typ powiązania. Zaleca się dodanie informacji docelowej dla użytownikai5/OS. 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 109. Dozwolone wartości dla 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 110. Dozwolone wartości dla 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.

Uprawnienie

Pole Uprawnienia określa uprawnienia publiczne do profilu użytkownika.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
AUT

Uprawnienia do profilu sterują wieloma funkcjami związanymi z profilem, takimi jak:

- zmiana profilu
- wyświetlanie profilu
- usuwanie profilu
- wprowadzenie zadania za pomocą profilu
- określanie profilu w opisie zadania
- przenoszenie do profilu prawa własności do obiektu
- dodawanie członków, jeśli profil jest profilem grupowym

Tabela 111. 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 sposobów dostępu do informacji” na stronie 136.

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

Wartość kontrolowania obiektu dla profilu użytkownika współpracuje z wartością kontrolowania obiektu dla obiektu, w celu określenia, czy użytkownik ma dostęp do kontrolowanego obiektu.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
OBJAUD

Długość:
10

Kontrolowania obiektu dla profilu użytkownika nie można określić w żadnych komendach profilu użytkownika. Aby określić kontrolowanie obiektu dla użytkownika, należy użyć komendy CHGUSRAUD. Komendy CHGUSRAUD może użyć tylko użytkownik z uprawnieniami specjalnymi *AUDIT.

Tabela 112. Możliwe wartości parametru OBJAUD:

***NONE**	Wartość parametru OBJAUD decyduje, czy dla danego użytkownika wykonywane jest kontrolowanie obiektu.
***ALL**	Jeśli wartość parametru OBJAUD dla obiektu jest równa *USRPRF, rekord kontroli jest zapisywany, gdy dany użytkownik zmienia lub odczytuje obiekt.
***CHANGE**	Jeśli wartość parametru OBJAUD dla obiektu jest równa *USRPRF, rekord kontroli jest zapisywany, gdy dany użytkownik zmienia obiekt.

Tabela 112. Możliwe wartości parametru OBJAUD: (kontynuacja)

***NOTAVL**	Wartość ta wyświetlana jest wówczas, gdy wartość parametru jest niedostępna dla użytkownika ze względu na brak uprawnień specjalnych *AUDIT ani *ALLOBJ. Wartości parametru nie można przypisać tej wartości.

Tabela 113 pokazuje, w jaki sposób współpracują ze sobą wartości parametrów OBJAUD dla użytkownika i dla obiektu:

Tabela 113. Kontrolowanie wykonywane dla dostępu do obiektów

Wartości parametru OBJAUD dla obiektu	**Wartości parametru OBJAUD dla użytkownika**		
	***NONE**	***CHANGE**	***ALL**
*ALL	Zmiana i użycie	Zmiana i użycie	Zmiana i użycie
*CHANGE	Zmiana (Change)	Zmiana (Change)	Zmiana (Change)
*NONE	Brak	Brak	Brak
*USRPRF	Brak	Zmiana (Change)	Zmiana i użycie

Zadania pokrewne

“Planowanie kontroli dostępu do obiektu” na stronie 296
System operacyjny i5/OS zapewnia możliwość protokołowania dostępu do obiektu w kronice kontroli bezpieczeństwa, korzystając z wartości systemowych oraz wartości kontrolowania obiektu dla użytkowników i obiektów. Funkcja ta nosi nazwę *kontrolowanie obiektu*.

Kontrola działań

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.

Podpowiedź ekranu Dodanie użytkownika:
Brak

Parametr CL:
AUDLVL

Długość:
640

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 114. Możliwe wartości parametru AUDLVL:

***NONE**	Kontrolą działania steruje wartość systemowa QAUDLVL. Nie jest przeprowadzane żadne dodatkowe kontrolowanie.
***NOTAVL**	Wartość ta jest wyświetlana w celu wskazania, że wartość parametru nie jest dostępna dla użytkownika, ponieważ użytkownik nie posiada uprawnień specjalnych *AUDIT oraz *ALLOBJ. Wartości parametru nie można przypisać tej wartości.
***AUTFAIL**	Kontrolowane są niepowodzenia uwierzytelniania.
***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.

Tabela 114. Możliwe wartości parametru AUDLVL: (kontynuacja)

***JOBBAS**	Kontrolowane są podstawowe funkcje zadania.
***JOBCHGUSR**	Kontrolowane są zmiany aktywnego profilu użytkownika wątku lub profili grupowych.
***JOBDTA**[1]	Protokołowane są zmiany zadania.
***OBJMGT**	Protokołowane są operacje przenoszenia i zmiany nazwy obiektu.
***OFCSRV**	Protokołowane są zmiany katalogu dystrybucyjnego systemu oraz działania poczty.
***NETBAS**	Kontrolowane są podstawowe funkcje sieci.
***NETCLU**	Kontrolowane są operacje klastra lub grupy zasobów klastra.
***NETCMN** [3]	Kontrolowane są funkcje sieciowe i komunikacyjne.
***NETFAIL**	Kontrolowane są awarie sieci.
***NETSCK**	Kontrolowane są zadania gniazd.
***OPTICAL**	Kontrolowane są wszystkie funkcje nośników optycznych.
***PGMADP**	Protokołowane jest uzyskiwanie uprawnień do obiektu z programów, które adoptują uprawnienia.
***PGMFAIL**	Kontrolowane są błędy wykonania programów.
***PRTDTA**	Kontrolowane są funkcje drukowania z parametrem SPOOL(*NO).
***SAVRST**	Protokołowane są operacje składowania i odtwarzania.
***SECCFG**	Kontrolowana jest konfiguracja bezpieczeństwa.
***SECDIRSRV**	Kontrolowane są zmiany lub aktualizacje podczas wykonywania funkcji usług katalogowych.
***SECIPC**	Kontrolowane są zmiany komunikacji między procesami.
***SECNAS**	Kontrolowane są działania usługi uwierzytelniania sieciowego.
***SECRUN**	Kontrolowane są funkcje wykonawcze bezpieczeństwa.
***SECSCKD**	Kontrolowane są deskryptory gniazda.
***SECURITY**[2]	Protokołowane są funkcje związane z bezpieczeństwem.
***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.

Tabela 114. Możliwe wartości parametru AUDLVL: (kontynuacja)

[1]	Wartość *JOBDTA zawiera w sobie dwie wartości, *JOBBAS oraz *JOBCHGUSR, które umożliwiają lepsze dostosowanie kontroli. Określenie obu wartości jest równoznaczne z podaniem wartości *JOBDTA.
[2]	Wartość *SECURITY jest złożona z kilku wartości umożliwiających lepsze dostosowanie kontroli. Określenie wszystkich tych wartości jest równoznaczne z podaniem wartości *SECURITY. Te wartości są następujące: • *SECCFG, • *SECDIRSRV, • *SECIPC, • *SECNAS, • *SECRUN, • *SECSCKD, • *SECVFY, • *SECVLDL.
[3]	Wartość *NETCMN jest złożona z kilku wartości umożliwiających lepsze dostosowanie kontroli. Określenie wszystkich tych wartości jest równoznaczne z podaniem wartości *NETCMN . Te wartości są następujące: • *NETBAS, • *NETCLU, • *NETFAIL, • *NETSCK.

Odsyłacze pokrewne

“Planowanie kontroli działań” na stronie 271
Wartość systemowa QAUDCTL (sterowanie kontrolą), wartość systemowa QAUDLVL (poziom kontroli), wartość systemowa QAUDLVL2 (rozszerzenie poziomu kontroli) oraz parametr AUDLVL (kontrola działania) w profilach użytkownika współpracują ze sobą w celu sterowania kontrolą działania:

Informacje dodatkowe powiązane z profilem użytkownika

W tym temacie omówione zostały uprawnienia prywatne, informacje o posiadanych obiektach oraz informacje o obiektach grupy podstawowej powiązanych z profilem użytkownika.

Odsyłacze pokrewne

“Sposób przechowywania informacji o bezpieczeństwie” na stronie 254
Zaplanowanie odpowiednich procedur tworzenia i odtwarzania kopii zapasowych informacji o bezpieczeństwie wymaga znajomości sposobu przechowywania i zapisywania tych informacji.

Uprawnienia prywatne

Wszystkie uprawnienia prywatne posiadane przez użytkownika 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 są sprawdzane uprawnienia użytkownika do obiektu” na stronie 179.

Uprawnienia prywatne użytkownika dla obiektów opartych o biblioteki można wyświetlić za pomocą komendy Wyświetlenie profilu użytkownika:

```
DSPUSRPRF nazwa_profilu_użytkownika TYPE(*OBJAUT)
```

Za pomocą komendy Praca z obiektami wg. uprawnień prywatnych (Work with Objects by Private Authority - WRKOBJPVT) można pracować z prywatnymi uprawnieniami dla obiektów opartych na bibliotekach i katalogach. Aby zmienić prywatne uprawnienia użytkownika, można użyć komend służących do pracy z uprawnieniami obiektów, takimi jak Edycja uprawnień obiektu (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 użytkownika” na stronie 170.

Uprawnienia grupy podstawowej

Nazwy wszystkich obiektów, dla których profil jest grupą podstawową, składowane są razem z profilem grupowym.

Obiekty oparte na bibliotekach, 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,

Ponieważ wielkość profilu użytkownika może niekorzystnie wpływać na wydajność, zaleca się, aby nie przypisywać wszystkich (lub prawie wszystkich) obiektów do tylko jednego profilu będącego właścicielem.

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.

Uwierzytelnienie za pomocą identyfikatora cyfrowego

Certyfikaty cyfrowe umożliwiają użytkownikom zabezpieczanie komunikacji i zapewnianie integralności komunikatów. Infrastruktura System i zezwala na przeprowadzanie identyfikacji za pomocą certyfikatów cyfrowych x.509.

Funkcje API identyfikatorów cyfrowych umożliwiają tworzenie, dystrybuowanie i zarządzanie certyfikatami cyfrowymi związanymi z profilami użytkowników. Więcej informacji na temat poniższych funkcji API znajduje się w publikacji Funkcje API zarządzania certyfikatami cyfrowymi:

- 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

W temacie opisane zostały komendy i ekrany służące do tworzenia, zmiany i usuwania profili użytkowników w systemie operacyjnym i5/OS.

Aby tworzyć, zmieniać lub usuwać profile użytkowników, wymagane są uprawnienia specjalne *SECADM.

Tworzenie profili użytkowników

Profil użytkownika można utworzyć za pomocą ekranu Praca z profilami użytkowników (Work with User Profiles - WRKUSRPRF), komendy Tworzenie profilu użytkownika (Create User Profile - CRTUSRPRF), opcji Praca z rejestrowaniem użytkowników (Work with User Enrollment) menu SETUP albo za pomocą systemu System i Navigator.

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: Nie można tworzyć profilu użytkownika do niezależnej puli dyskowej komendą Tworzenie profilu użytkownika (Create User Profile - CRTUSRPRF). 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 jest przenoszona do innego systemu, uprawnienia prywatne, prawa własności do obiektu oraz pozycje grupy podstawowej będą dołączone w systemie docelowym do profilu o tej samej nazwie. Jeśli w systemie docelowym taki profil nie istnieje, zostanie on 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 Praca z profilami użytkowników (Work with User Profiles - 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 opcje i naciśnij klawisz Enter.

Profil użytkownika. . . . . .   NEWUSER        Nazwa
Hasło użytkownika . . . . . .   *NONE          Wartość znakowa, *USRPRF...
Ustawienie hasła jako wygasłe . . . .   *YES          *NO, *YES
Status. . . . . .   *ENABLED      *ENABLED, *DISABLED
Klasa użytkownika.  . . . . . .   *USER         *USER, *SYSOPR, *PGMR...
Poziom asysty . . . . . .   *SYSVAL       *SYSVAL, *BASIC, *INTERMED...
Biblioteka bieżąca. . . . . .   *CRTDFT       Nazwa, *CRTDFT
Wywoływany program początkowy . . . .   *NONE         Nazwa, *NONE
  Biblioteka. . . . . .                     Nazwa, *LIBL, *CURLIB
Menu początkowe . . . . . .   MAIN          Nazwa, *SIGNOFF
  Biblioteka. . . . . .   QSYS          Nazwa, *LIBL, *CURLIB
Ograniczenie możliwości . . . . . .   *NO           *NO, *PARTIAL, *YES
Tekst opisu . . . . . .   *BLANK
```

Ekran Tworzenie profilu użytkownika (Create User Profile) zawiera wszystkie pola z 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)

Komenda Tworzenie profilu użytkownika (Create User Profile - CRTUSRPRF) służy do tworzenia profilu użytkownika. Można podać parametry 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)

Aby dodać użytkowników do systemu, można użyć 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        Nazwa
Opis użytkownika  . . . .
Hasło . . . . . . . . . . NEWUSER
Typ użytkownika . . . . .   *USER          Typ, F4=Lista
Grupa użytkownika . . . .   *NONE          Nazwa, F4=Lista

Ograniczenie użycia wiersza komend N       T=Tak, N=Nie

Biblioteka domyślna . . .                  Nazwa
Drukarka domyślna . . . .   *WRKSTN        Nazwa, *WRKSTN, F4=Lista
Program wpisywania się. .   *NONE          Nazwa, *NONE
  Biblioteka. . . . . .                    Nazwa

Menu początkowe . . . . .                  Nazwa
  Biblioteka. . . . . .                    Nazwa

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. . . . . .
```

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.

Kopiowanie profili użytkowników

Profil użytkownika można utworzyć, kopiując inny profil użytkownika lub profil grupowy.

Można utworzyć jeden profil w grupie 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.

Pojęcia pokrewne

“Profile grupowe” na stronie 4
Profil grupowy jest szczególnym typem profilu użytkownika. Można go używać do definiowania uprawnień dla grupy użytkowników, zamiast przyznawania uprawnień każdemu użytkownikowi z osobna.

Kopiowanie z ekranu Praca z profilami użytkowników

Za pomocą ekranu Praca z profilami użytkowników można kopiować informacje dotyczące profili 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 wybór i naciśnij klawisz 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  . . . . . > 'Wydział magazynowy'
```

Na ekranie Tworzenie profilu użytkownika wyświetlane są wszystkie wartości źródłowego profilu użytkownika, poza poniższymi:

Profil użytkownika
Puste. Musi być wypełnione.

Hasło Wartość domyślna komendy CRTUSRPRF

Hasło do dokumentu
*NONE

Kolejka komunikatów
*USRPRF

Ustawienia narodowe zadania
*SYSVAL

Ustawienia narodowe
*SYSVAL

Numer identyfikacyjny użytkownika
*GEN

Numer identyfikacyjny grupy
*NONE

Katalog osobisty
*USRPRF

Powiązanie EIM
*NOCHG

Uprawnienie
*EXCLUDE

Na ekranie Tworzenie profilu użytkownika (Create User Profile) można zmieniać dowolne pola. Prywatne uprawnienia profilu źródłowego nie są kopiowane. Jakiekolwiek obiekty wewnętrzne zawierające preferencje użytkownika oraz inne informacje o nim również nie są kopiowane.

Kopiowanie z ekranu Praca z rejestrowaniem użytkowników (Work with User Enrollment)

Profile użytkowników można również kopiować z ekranu Praca z rejestrowaniem użytkowników (Work with User Enrollment).

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

Biblioteka domyślna . . .   DPTWH
Drukarka domyślna . . . . PRT04
Program wpisywania się  . *NONE
  Biblioteka  . . . . . .
```

Na ekranie Dodawanie użytkownika pojawiają się wszystkie wartości z profilu źródłowego, z wyłączeniem poniższych:

Użytkownik (User)
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 są widoczne na podstawowym poziomie asysty, są kopiowane z profilu źródłowego, za wyjątkiem następujących:

Kolejka komunikatów
*USRPRF

Hasło do dokumentu
*NONE

Numer identyfikacyjny użytkownika
*GEN

Numer identyfikacyjny grupy
*NONE

Powiązanie EIM
*NOCHG

Uprawnienie
*EXCLUDE

Prywatne uprawnienia profilu źródłowego nie są kopiowane.

Kopiowanie uprawnień prywatnych

Za pomocą komendy Nadanie uprawnień użytkownika (Grant User Authority - GRTUSRAUT) można skopiować uprawnienia prywatne z jednego profilu użytkownika do innego.

Nie należy korzystać z tej funkcji zamiast profili grupowych i list autoryzacji. Kopiowanie uprawnień nie pomaga w zarządzaniu podobnymi uprawnieniami oraz może spowodować problemy związane z wydajnością systemu.

Pojęcia pokrewne

"Kopiowanie uprawnień użytkownika" na stronie 170
Za pomocą komendy Nadanie uprawnień użytkownika (Grant User Authority - GRTUSRAUT) można skopiować wszystkie uprawnienia prywatne jednego użytkownika do innego.

Zmiana 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. Można również 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. Przed usunięciem takiego profilu należy najpierw usunąć wszelkie obiekty będące jego własnością, lub przenieść prawo własności tych obiektów do innego profilu.

Nie można usunąć profilu użytkownika, jeśli jest on grupą podstawową dla obiektów. Przy usuwaniu profilu użytkownika przy pomocy pośredniego poziom asysty,można zmienić lub usunąć grupę podstawową dla obiektów. Aby wyświetlić wszystkie obiekty, dla których profil jest grupą podstawową, można użyć komendy WRKOBJPGP.

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 grupy należy zmienić pole GRPPRF lub SUPGRPPRV w każdym jej podzbiorze.

Używanie komendy Usunięcie profilu użytkownika (Delete User Profile)

Aby usunąć profil użytkownika, można użyć bezpośrednio komendy Usunięcie profilu użytkownika (Delete User Profile - DLTUSRPRF), albo opcji 4 (Usunięcie) 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)
Wpisz opcje i naciśnij klawisz Enter.

Profil użytkownika. . . . . . . . . . > HOGANR        Nazwa
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 .
Powiązanie EIM . . . . . .   *DLT          *DLT, *NODLT
```

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 obiektami 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=Wyświetl opis    9=Zmień 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

Do usunięcia profilu użytkownika można użyć opcji Usuwanie użytkownika (Remove User) ekranu Praca z rejestrowaniem użytkowników (Work with User Enrollment).

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 poprzez uprawnienia prywatne

Aby wyświetlić i pracować z obiektami, dla których profil posiada uprawnienia prywatne, można posłużyć się komendą Praca z obiektami poprzez uprawnienia prywatne (Work with Objects by Private Authorities - WRKOBJPVT).

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
```

Aktywowanie profilu użytkownika

Jeśli wartości systemowe QMAXSIGN i QMAXSGNACN w systemie zostały ustawione tak, aby wyłączać profil użytkownika po zbyt wielu nieudanych próbach kontroli poprawności hasła, istnieje szansa, że trzeba będzie uaktywnić profil ponownie, zmieniając jego status na *ENABLED.

Aby uaktywnić profil użytkownika, należy posiadać specjalne uprawnienie *SECADM, a także 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. Stwórz program CL, który jest własnością użytkownika ze specjalnym uprawnieniem *SECADM, oraz uprawnieniami *OBJMGT i *USE do profili użytkownika w systemie. Adoptuj uprawnienia właściciela podczas tworzenia programu, korzystając z opcji USRPRF(*OWNER).
2. Przy pomocy komendy EDTOBJAUT należy utworzyć uprawnienia publiczne do programu *EXCLUDE i przyznać operatorom systemu uprawnienie*USE.
3. Operator uaktywnia 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 użytkownika

Użytkownik może wyświetlać i drukować informacje dotyczące profili użytkowników w różnych formatach.

Wyświetlanie profilu indywidualnego

Aby wyświetlić wartości indywidualnego profilu użytkownika, należy skorzystać z opcji 5 (Ekran) ekranu Praca z rejestr. użytkowników lub ekranu Praca z profilami użytkowników. Można również wykorzystać komendę Wyśw. 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.

```
                          Wyśw. uprawn. użytkowników

                       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.

```
                      Wyśw. uprawn. użytkowników

                   Ostatnia  Hasło      Hasło                  Lokalne
Profil    Profil   zmiana    poziomu    poziomu     Hasło do   zarz.
użytk.    grupowy  hasła     0 lub 1    2 lub 3     Netserver  hasłem
ANGELA             04/21/0x    *YES       *NO         *YES       *YES
ARTHUR             07/07/0x    *YES       *YES        *YES       *YES
CAROL1             05/15/0x    *YES       *YES        *YES       *YES
CAROL2             05/15/0x    *NO        *NO         *NO        *NO
CHUCKE             05/18/0x    *YES       *NO         *YES       *YES
DENNISS            04/20/0x    *YES       *NO         *YES       *YES
DPORTER            03/30/0x    *YES       *NO         *YES       *YES
GARRY              08/04/0x    *YES       *YES        *YES       *YES
JANNY              03/16/0x    *YES       *NO         *YES       *YES
```

Typy ekranów profilu użytkownika

Komenda (Wyśw. profilu użytkownika - The Display User Profile (DSPUSRPRF) zawiera 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.
- Podając parametr output(*OUTFILE), z niektórych ekranów można utworzyć zbiór wyjściowy. Aby utworzyć własne raporty ze zbiorów wyjściowych, należy użyć narzędzia do tworzenia zapytań. “Analizowanie profili użytkowników” na stronie 311 zawiera sugestie raportów.

Typy raportów profilu użytkownika

Raporty profilu użytkownika można generować za pomocą komendy Drukowanie profilu użytkownika (Print User Profile - PRTUSRPRF) lub komendy Analiza domyślnych haseł (Analyze Default Password - ANZDFTPWD).

- Drukowanie profilu użytkownika (Print User Profile - PRTUSRPRF)

  Ta komenda generuje raporty z informacjami o profilach użytkowników w systemie. Do wyboru są cztery rodzaje tego raportu. 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 generuje raport o wszystkich profilach użytkowników w systemie, które mają hasło domyślne. Umożliwia podejmowanie działań wobec takich 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.
- Niekiedy użytkownik nie może zmienić przechowywanych przez aplikacje informacji, które zawierają nazwę użytkownika.

Aplikacje uruchamiane przez użytkownika mogą korzystać z profili aplikacji. Tworzenie nowego profilu użytkownika systemu i5/OS 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. Stara nazwa profilu to SMITHM, natomiast 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. a 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: Użytkownikowi JONESM należy przypisać identyfikator GID, posługując się parametrem GID w komendzie Tworzenie profilu użytkownika (Create User Profile - CRTUSRPRF) lub Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF).
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. Zmień identyfikatory UID i GID użytkownika JONESM na identyfikatory UID i GID, które poprzednio należały do użytkownika SMITHM. Służy do tego komenda Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF):

   ```
   CHGUSRPRF USRPRF(JONESM) UID(uid użytkownika SMITHM)
             GID(gid użytkownika SMITHM)
   ```

   Jeśli użytkownik JONESM jest właścicielem obiektów w katalogu, to nie można zmienić identyfikatorów UID I GID za pomocą komendy CHGUSRPRF. Zamiast tego należy użyć funkcji API QSYCHGID.

Praca z kontrolą użytkownika

Komendą Zmiana kontroli użytkownika (Change User Auditing - CHGUSRAUD) można ustawić charakterystyki kontroli dla użytkowników.

Aby móc korzystać z tej komendy, użytkownik musi posiadać uprawnienia specjalne *AUDIT.

```
         Zmiana kontroli użytkownika (Change User Audit  - CHGUSRAUD)
Wpisz opcje i naciśnij klawisz Enter.

Profil użytkownika . . . . . . . . HOGANR
               + więcej wartości   JONESS
Wartość kontroli obiektu  . . . . .   *SAME
Kontrola działań użytkownika. . . . .   *CMD
               + więcej wartości   *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. Podane wartości nie są dodawane do bieżących wartości parametru AUDLVL dla użytkowników, tylko je zastępują.

Jeśli użytkownik posiada uprawnienia specjalne *ALLOBJ lub *AUDIT, to użyć komendy Wyświetlenie profilu użytkownika (Display User Profile - DSPUSRPRF) aby sprawdzić parametry innego użytkownika.

Praca z profilami w programach CL

W programie CL można pracować z profilami użytkowników.

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 niniejszej sekcji 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 “Korzystanie z programu zatwierdzania haseł” na stronie 62 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.

Punkt wyjścia profilu użytkownika

Aby wykonywać określone funkcje związane z profilem użytkownika, można napisać własny program obsługi wyjścia. Po zarejestrowaniu programu obsługi wyjścia za pomocą dowolnego punktu wyjścia profilu użytkownika, każda operacja tworzenia, zmiany, usuwania lub odtwarzania profilu użytkownika powoduje wysłanie powiadomienia o wykonanej funkcji.

W momencie powiadomienia, program wyjściowy może wykonać dowolną z następujących operacji:

- 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.

Informacje pokrewne

Programy obsługi wyjścia

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 dostarczanych przez IBM.

Aby umożliwić zainstalowanie systemu, hasło dla profilu osoby odpowiedzialnej za bezpieczeństwo (QSECOFR) zawsze jest takie samo dla każdego dostarczanego systemu. Jednak jest ono ustawione jako wygasłe. W nowych systemach należy zmienić hasło po pierwszym wpisaniu się jako 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 IBM”, na stronie 329 zawiera pełną listę wszystkich profili użytkowników IBM oraz wartości pól dla każdego profilu.

Uwaga: Wszystkie profile użytkowników IBM, z wyjątkiem QSECOFR, dostarczane są z hasłem *NONE i nie są przeznaczone do wpisywania się. Profile te są używane przez system operacyjny IBM i5/OS. Dlatego wpisywanie się za pomocą tych profili lub używanie ich do posiadania obiektów użytkownika (nie dostarczonych przez IBM) nie jest zalecane.

Pojęcia pokrewne

“Profile użytkowników IBM” na stronie 266
Zadania kontroli profili użytkowników IBM można wykonać, sprawdzając ich hasła.

Zmiana haseł dla profili użytkowników IBM

Jeśli istnieje potrzeba wpisania się za pomocą jednego z profili użytkowników IBM, można zmienić hasło za pomocą komendy CHGUSRPRF. 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 osoby odpowiedzialnej za bezpieczeństwo (QSECOFR) . . . . . .
  Nowe hasło (weryfikacja) . . . . . .

Nowe hasło operatora systemu (QSYSOPR) . . . . . .
  Nowe hasło (weryfikacja) . . . . . .

Nowe hasło programisty (QPGMR) . . . . . .
  Nowe hasło (weryfikacja) . . . . . .

Nowe hasło użytkownika (QUSER) . . . . . .
  Nowe hasło (weryfikacja) . . . . . .

Nowe hasło serwisanta (QSRV) . . . . . .
  Nowe hasło (weryfikacja) . . . . . .
```

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 (weryfikacja) . . . . . .
```

Praca z identyfikatorami użytkowników narzędzi serwisowych

Istnienie kilka ulepszeń i dodatków do narzędzi serwisowych, ułatwiających ich używanie i 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 informacjynego.

- **Udoskonalenia 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.

Pojęcia pokrewne

“Profile użytkowników IBM” na stronie 266
Zadania kontroli profili użytkowników IBM można wykonać, sprawdzając ich hasła.

Informacje pokrewne

Zarządzanie identyfikatorami użytkownika narzędzi serwisowych

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. Bezpieczeństwo zasobów

Ten rozdział zawiera opisy poszczególnych elementów bezpieczeństwa zasobów oraz opis ich działania. Wyjaśnia także, jak używać komend CL oraz ekranów do konfigurowania ochrony zasobów.

Ochrona zasobów definiuje, jacy użytkownicy uprawnieni są do korzystania z obiektów w systemie oraz jakie operacje na tych obiektach mogą wykonywać.

Rozdział 7, “Projektowanie bezpieczeństwa”, na stronie 227 omawia techniki projektowania ochrony zasobów, a także jej wpływ na projektowanie aplikacji oraz wydajność systemu.

Temat “Jak system sprawdza uprawnienia” na stronie 174 opisuje schematy blokowe oraz uwagi dotyczące sprawdzania uprawnień. Podczas zapoznawania się z poniższymi objaśnieniami warto skonsultować się z informacjami zawartymi w tym temacie.

Pojęcia pokrewne

“Bezpieczeństwo zasobów” na stronie 5
Możliwość dostępu do obiektu nazywa się *uprawnieniem*. Bezpieczeństwo zasobów w systemie operacyjnym i5/OS umożliwia sterowanie uprawnieniami do obiektów. Można definiować, kto może używać danych obiektów i w jaki sposób.

“Ogólne zalecenia dotyczące projektowania ochrony” na stronie 228
Utrzymywanie projektu ochrony tak prostego jak to tylko możliwe, ułatwia zarządzanie i kontrolę ochrony. Zwiększa także wydajność aplikacji oraz tworzenia kopii zapasowych.

Precyzowanie uprawnień dostępu 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:
Uprawnienia publiczne dotyczą dowolnej osoby, która posiada uprawnienia do wpisania się do systemu. Uprawnienia prywatne zdefiniowane są dla każdego obiektu w systemie, chociaż uprawnienia publiczne dla obiektu 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
Indywidualne profile użytkowników mogą uzyskiwać uprawnienia do używania obiektów w systemie. To jeden z typów uprawnień prywatnych.

Uprawnienia grupowe:
Profile grupowe mogą uzyskiwać 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 składowane są wraz z obiektem i są w stanie zapewnić lepszą wydajność niż uprawnienia prywatne nadane profilowi grupowemu. Tylko profil użytkownika z numerem identyfikacyjnym grupy (gid) może być grupą podstawową dla obiektu. Uprawnienia grupy podstawowej nie są uprawnieniami prywatnymi.

Definiowanie sposobów dostępu do informacji

Użytkownik może zdefiniować, które operacje mogą być wykonywane na obiektach, danych i polach.

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 dla obiektów dzieli się na trzy kategorie:

1. **Uprawnienia do obiektów** definiują, jakie operacje mogą być wykonywane na obiekcie jako na całości.
2. **Uprawnienia do danych** definiują, jakie operacje mogą być wykonywane na zawartości obiektu.
3. **Uprawnienia do pól** definiują, jakie operacje mogą być wykonywane na polach danych.

Tabela 115 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, “Uprawnienia wymagane dla obiektów używanych przez komendy”, na stronie 351 udostępnia informacje dotyczące uprawnień, które wymagane są do wykonywania określonych funkcji.

Tabela 115. 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. Wykonanie operacji składowania i odtworzenia dla obiektu [1]. Przekazanie prawa własności do obiektu.
*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].

Tabela 115. Opis typów uprawnień (kontynuacja)

Uprawnienie	Nazwa	Dozwolone funkcje
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.
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 (Read)	Dostęp do zawartości pola. Na przykład wyświetlenie zawartości pola.
*ADD	Dodanie (Add)	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), uprawnienia do istnienia obiektu nie są wymagane do wykonywania operacji składowania i odtwarzania obiektu.

[2] Więcej informacji zawiera temat “Zarządzanie listą autoryzacji” na stronie 143.

Zadania pokrewne

“Zmiana na poziom 30 z poziomu niższego” na stronie 13
Gdy zmieniany jest poziom bezpieczeństwa z niższego poziomu na poziom 30, system zmienia wszystkie profile użytkowników, aby zaktualizować uprawnienia specjalne podczas następnego IPL.

Odsyłacze pokrewne

“Uprawnienie grupowe” na stronie 100
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.

Najczęściej używane uprawnienia

Użytkownik może określić niektóre zestawy uprawnień do obiektów i danych.

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 116 na stronie 138 opisuje uprawnienia zdefiniowane systemowo, które dostępne są podczas używania komend oraz ekranów uprawnień do obiektu.

Tabela 116. 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 117 zawiera uprawnienia zdefiniowane systemowo, które są dostępne podczas używania komend WRKAUT i CHGAUT:

Tabela 117. 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 118 pokazuje, w jaki sposób zezwolenia programu LAN Server odwzorowują uprawnienia do obiektu i do danych:

Tabela 118. Zezwolenia programu LAN Server

Uprawnienie	**Zezwolenia programu LAN Server**
*EXCLUDE	Brak
Uprawnienia do obiektu	
*OBJOPR	Patrz uwaga 1
*OBJMGT	Zezwolenie
*OBJEXIST	Tworzenie, usuwanie

Tabela 118. Zezwolenia programu LAN Server (kontynuacja)

Uprawnienie	Zezwolenia programu LAN Server
*OBJALTER	Atrybut
*OBJREF	Brak odpowiednika
Uprawnienia do danych	
*READ	Odczyt (Read)
*ADD	Tworzenie (Create)
*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.

Precyzowanie dostępu do informacji

Użytkownik może zdefiniować ochronę zasobów dla pojedynczych obiektów w systemie. Można również zdefiniować parametry bezpieczeństwa dla grup obiektów, za pomocą zabezpieczeń biblioteki lub listy autoryzacji.

Bezpieczeństwo biblioteki

Zabezpieczenia biblioteki mogą służyć do ochrony informacji.

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, “Uprawnienia wymagane dla obiektów używanych przez komendy”, na stronie 351 pokazuje, jakie uprawnienia wymagane są przez komendy CL do obiektów oraz bibliotek obiektów.

Podczas obsługiwania prostego schematu bezpieczeństwa, jedną z technik zabezpieczania informacji jest korzystanie z zabezpieczeń biblioteki. Na przykład, aby zabezpieczyć poufne dane dla zestawu aplikacji, należy wykonać następujące czynności:

- 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).

Pomimo że zabezpieczenia bibliotek są dość prostą, efektywną metodą ochrony informacji, mogą okazać się niewystarczające dla danych o wysokich wymaganiach w zakresie bezpieczeństwa. Bardzo wrażliwe obiekty powinny być zabezpieczane pojedynczo lub za pomocą list autoryzacji, nie należy polegać na zabezpieczeniach biblioteki.

Pojęcia pokrewne

“Planowanie bibliotek” na stronie 232
Biblioteka jest podobna do katalogu, w którym można przechowywać obiekty. Na sposób grupowania informacji aplikacji w biblioteki oraz na zarządzanie bibliotekami wpływ ma wiele czynników.

Bezpieczeństwo 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 którego jest określony parametr *LIBL, uprawnienia są sprawdzane na liście 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.

Odsyłacze pokrewne

“Listy bibliotek” na stronie 213

Lista bibliotek dla zadania wskazuje, które biblioteki mają być przeszukiwane, oraz kolejność, w jakiej mają być przeszukiwane.

Uprawnienia do pól

Można określić uprawnienia do pól zbiorów bazy danych.

Uprawnienia pól są obsługiwane dla zbiorów baz danych. Obsługiwane uprawnienia to: Zarządzanie, Zmiana, Odniesienie, Odczyt, Dodaj 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

Obiekt . . . . . :   PLMITXT     Właściciel . . . . . :   PGMR1
  Biblioteka . . :   RLN         Grupa podstawowa . . :   DPTAR
Typ obiektu  . . :   *FILE       Urządzenie ASP . . . :   *SYSBAS

Obiekt chroniony przez listę autoryzacji  . . . . . :   *NONE
                      Obiekt    ---------------Dane---------------
Użytkownik  Grupa     Uprawn.    Odcz. Dod.  Akt.    Usuw.   Uruch.
*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

                          Obiekt    -----Uprawnienia pól-----------
Pole         Użytkownik Uprawn.    Zarz.  Zmn.Ref  Odcz. Dod.   Akt.
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 klawisz Enter.

F3=Wyjście F5=Odśwież F12=Anuluj F16=Powtórz ustawienie na F17=Ustaw na
```

Rysunek 5. Ekran Wyświetlenie uprawnień do pól (Display Field Authority). Po naciśnięciu klawisza "F17=Przejdź do", wyświetlony zostanie znak zachęty listy. Po naciśnięciu klawisza F16, powtórzona zostanie poprzednia pozycja operacji.

Uprawnienia pól obejmują następujące opcje:

- Komenda Drukowanie uprawnień prywatnych (Print Private Authority - PRTPVTAUT) posiada pole określające, czy zbiór posiada uprawnienia pól.
- Komenda Wyświetlenie uprawnień obiektu (Display Object Authority - DSPOBJAUT) posiada parametr typu uprawnień pozwalający na wyświetlenie uprawnień obiektu, uprawnień pól, lub wszystkich uprawnień. jeśli typem obiektu nie jest *FILE, można wyświetlić jedynie uprawnienia do obiektu,
- Informacje zawarte w API Lista użytkowników uprawnionych do obiektu (QSYLUSRA) API określają, czy zbiór posiada uprawnienia 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.

Bezpieczeństwo a środowisko System/38

Niniejsza sekcja zawiera informacje dotyczące bezpieczeństwa w środowisku 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.

Informacje pokrewne

System/38 Environment Programming

Zalecenia dotyczące środowiska System/38

Ten temat zawiera listę zaleceń dotyczących środowiska System/38.

Poniższe działania należy wykorzystać w celu zabezpieczenia systemu przed środowiskiem System/38 oraz programami CL typu CLP38:

- sprawdzić uprawnienia prywatne biblioteki QSYS38. Jeśli są to uprawnienia *ALL lub *CHANGE, to należy zmienić je na *USE.
- sprawdzić uprawnienia prywatne biblioteki QUSER38. Jeśli są to uprawnienia *ALL lub *CHANGE, to należy zmienić je na *USE.
- jeśli biblioteki QUSER38 oraz QSYS38 nie istnieją, należy je utworzyć i nadać im uprawnienia publiczne *USE. zapobiegnie to utworzeniu ich w późniejszym czasie i nadaniu im zbyt dużych uprawnień publicznych.

Bezpieczeństwo katalogu

Do ochrony informacji można użyć funkcji bezpieczeństwa 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.

Należałoby rozważyć wykorzystanie ochrony katalogów w ten sam sposób, jak ochronę bibliotek. Należy ograniczyć dostęp do katalogów oraz użyć uprawnień publicznych do obiektów w katalogu. Ograniczenie liczby uprawnień prywatnych dla obiektów zwiększa wydajność procesu sprawdzania uprawnień.

Bezpieczeństwo list 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. Zawiera on listę wszystkich obiektów zabezpieczonych 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. Powiązanie pomiędzy obiektami z listy autoryzacji zostanie utracone.

Przykłady użycia list autoryzacji opisuje temat “Korzyści wynikające ze stosowania listy autoryzacji” na stronie 171.

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, załóżmy że użytkownik UŻYTKOWNIK_A posiada uprawnienia *CHANGE oraz *AUTLMGT dla listy CPLIST1. 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.

Użycie list autoryzacji do zabezpieczenia obiektów dostarczonych przez IBM

Użytkownik może użyć list autoryzacji do zabezpieczenia obiektów dostarczonych przez IBM. Na przykład, można ograniczyć korzystanie z grupy komend dla 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.

Uprawnienia dla nowych obiektów w bibliotece

Użytkownik może określić uprawnienia dla nowych obiektów w bibliotece.

Każda biblioteka ma parametr CRTAUT (uprawnienie 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 dla większości komend, uprawnienia publiczne dla obiektu ustawiane są na wartość CRTAUT dla biblioteki.

Na przykład, załóżmy że biblioteka CUSTLIB ma wartość CRTAUT ustawioną na *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, załóżmy że biblioteka ITEMLIB ma wartość CRTAUT ustawioną na *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 149 zawiera więcej przykładów przypisywania przez system prawa własności oraz uprawnień do nowych obiektów.

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.

Czynniki ryzyka związane z Uprawnieniami do tworzenia (Create Authority - CRTAUT)

Przed zmianą Uprawnień do tworzenia (Create Authority - CRTAUT) biblioteki aplikacji należy wziąć pod uwagę czynniki ryzyka.

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

Użytkownik może określić uprawnienia dla nowych obiektów w katalogu.

Przy tworzeniu nowego katalogu za pomocą komendy CRTDIR, MD, lub MKDIR, użytkownik określa uprawnienia danych i uprawnienia obiektów otrzymywanych przez wszystkich (uprawnienia publiczne) dla nowego katalogu. Jeśli użytkownik użyje domyślnej opcji *INDIR, uprawnienia dla utworzonego katalogu zostaną ustalone w oparciu o jego katalog nadrzędny. W przeciwnym razie użytkownik podaje wymagane uprawnienia.

W przypadku tworzenia katalogu za pomocą API mkdir()--Make Directory, właściciel, grupa podstawowa i publiczne uprawnienia obiektu dla tworzonego katalogu określane są w oparciu o katalog, w którym jest on tworzony, podczas gdy właściciel, grupa podstawowa i publiczne ustawienia danych ustalane są w oparciu o tryb określony przez wywołanie API.

Dwa następujące przykłady ilustrują różne efekty tworzenia katalogów z różnymi opcjami.

W pierwszym przykładzie nowy katalog tworzony jest za pomocą komendy CRTDIR w głównym systemie plików (/) i określane są uprawnienia *PUBLIC.

Warunki początkowe: Uprawnienia w katalogu nadrzędnym:

```
                                  Wyświetlenie uprawnień (Display Authority)

Obiekt . . . . . . . . . . . . . . :   /sanders/mojtest
Właściciel. . . . . . . . . . . . . :   SANDERS
Grupa podstawowa . . . . . . . . . . :   SANDERSGP3
Lista autoryzacji. . . . . . . . . . :   *NONE

             Dane      -----Uprawnienia obiektu-----
Użytkownik   Uprawn.    Istn.    Zarz. Zmien.    Ref
*PUBLIC      *RWX        X        X      X        X
SANDERS      *RW
SANDERSGP3   *RX
QPGMR        *RWX
QTCM         *RWX        X        X      X        X
```

Użytkownik SANDERS wprowadza następującą komendę:

CRTDIR DIR('/sanders/mojtest/katdousuniecia') DTAAUT(*R) OBJAUT(*NONE)

Wynik: Uprawnienia do tworzonego katalogu:

```
                                  Wyświetlenie uprawnień (Display Authority)

Obiekt . . . . . . . . . . . . . . :   /sanders/mojtest/katdousuniecia
Właściciel. . . . . . . . . . . . . :   SANDERS
Grupa podstawowa . . . . . . . . . . :   SANDERSGP3
Lista autoryzacji. . . . . . . . . . :   *NONE

             Dane      -----Uprawnienia obiektu-----
Użytkownik   Uprawn.    Istn.    Zarz. Zmien.    Ref
*PUBLIC      *R
SANDERS      *RWX
SANDERSGP3   *RX
```

Uwagi:

1. Dane *PUBLIC oraz uprawnienia obiektów ustawiane są w oparciu o parametry DTAAUT i OBJAUT.
2. Uprawnienia danych właściciela (SANDERS) ustawiane są na *RWX, ale uprawnienia obiektów przekazywane są od właściciela katalogu nadrzędnego. Oznacza to, że właściciel katalogu nie posiada uprawnień obiektów dla tego katalogu, ponieważ właściciel katalogu nadrzędnego nie posiada uprawnień obiektów dla katalogu nadrzędnego.
3. Podstawowy profil grupowy nowego katalogu to SANDERSGP3, ponieważ SANDERSGP3 jest podstawowym profilem grupowym katalogu nadrzędnego.

Drugi przykład ilustruje, jak uprawnienia przechodzą z katalogu nadrzędnego na nowy katalog podczas tworzenia katalogu za pomocą komendy CRTDIR w głównym systemie plików (/).

Warunki początkowe: Uprawnienia w katalogu nadrzędnym:

```
                                  Wyświetlenie uprawnień (Display Authority)

Obiekt . . . . . . . . . . . . . . :   /sanders/mojtest
Właściciel. . . . . . . . . . . . . :   SANDERS
Grupa podstawowa . . . . . . . . . :   SANDERSGP3
Lista autoryzacji. . . . . . . . . :   *NONE

              Dane      -----Uprawnienia obiektu-----
Użytkownik   Uprawn.    Istn.    Zarz. Zmien.    Ref
*PUBLIC      *RWX        X        X      X        X
SANDERS      *RW
SANDERSGP3   *RX
QPGMR        *RWX
QTCM         *RWX        X        X      X        X
```

Użytkownik SANDERSUSR wprowadza następującą komendę:

CRTDIR DIR('/sanders/mojtest/katdousuniecia')

Wynik: Uprawnienia do tworzonego katalogu:

```
                                  Wyświetlenie uprawnień (Display Authority)

Obiekt . . . . . . . . . . . . . . :   /sanders/mojtest/katdousuniecia
Właściciel. . . . . . . . . . . . . :   SANDERSUSR
Grupa podstawowa . . . . . . . . . :   SANDERSGP3
Lista autoryzacji. . . . . . . . . :   *NONE

              Dane      -----Uprawnienia obiektu-----
Użytkownik   Uprawn.    Istn.    Zarz. Zmien.    Ref
*PUBLIC      *RWX        X        X      X        X
SANDERSUSR   *RWX
SANDERSGP3   *RX
QPGMR        *RWX
QTCM         *RWX        X        X      X        X
SANDERS      *RW
```

Uwagi:

1. Uprawnienia danych *PUBLIC i obiektów przechodzą z katalogu nadrzędnego. Z tego powodu uprawnienia danych ustawiane są na *RWX w przypadku wszystkich uprawnień obiektów.
2. Uprawnienia danych właściciela (SANDERSUSR) ustawiane są na *RWX, ale uprawnienia obiektów przekazywane są od właściciela katalogu nadrzędnego. Oznacza to, że właściciel katalogu nie posiada uprawnień obiektów dla tego katalogu, ponieważ właściciel katalogu nadrzędnego nie posiada uprawnień obiektów dla katalogu nadrzędnego.
3. Podstawowy profil grupowy nowego katalogu to SANDERSGP3, ponieważ SANDERSGP3 jest podstawowym profilem grupowym katalogu nadrzędnego.
4. Wszyscy użytkownicy posiadający uprawnienia prywatne dla katalogu nadrzędnego (QPGMR, QTCM) oraz właściciel katalogu nadrzędnego (SANDERS) otrzymują takie same uprawnienia prywatne dla nowego katalogu.

Prawo własności do obiektu

W tej sekcji opisane jest prawo własności do obiektu i jego funkcja w systemie.

Do każdego nowo utworzonego obiektu jest przypisywany właściciel. 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 149 pokazano przykłady przypisywania przez system prawa własności do nowych obiektów.

Właściciel obiektu zawsze ma wszystkie uprawnienia do tego obiektu, jeśli wszystkie lub niektóre z nich nie zostały mu specjalnie odebrane. Właściciel obiektu może zdecydować się sam usunąć niektóre uprawnienia szczegółowe ze względu bezpieczeństwa, jeśli nie ma uprawnień specjalnych *ALLOBJ. Na przykład, jeśli istnieje zbiór zawierający krytyczne informacje, użytkownik może usunąć uprawnienie istnienia obiektu w celu zabezpieczenia go przed przypadkowym usunięciem. Jednak, jako właściciel obiektu, użytkownik w dowolnym momencie może nadać sobie dowolne uprawnienia. Właściciel nowo utworzonego obiektu zintegrowanego systemu zbiorów posiada takie same uprawnienia dla obiektu tego zintegrowanego systemu zbiorów jak właściciel katalogu nadrzędnego dla katalogu nadrzędnego. Informacje o regułach uprawnień do obiektów obowiązujących dla wszystkich zbiorów systemowych lub tylko niektórych z nich można znaleźć w sekcji Planowanie i konfigurowanie bezpieczeństwa systemu.

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 niezależnie od tego, czy w grupie znajdują się podzbiory.

Następujące paragrafy dotyczą obiektów opartych zarówno o biblioteki jak i o katalogi.

Podczas zmiany właściciela obiektu można zachować lub odebrać uprawnienia poprzedniemu właścicielowi.

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 będącego właścicielem wielu obiektów ma wpływ na wydajność przy wyświetlaniu i pracy z obiektami uprawnień, których jest właścicielem, oraz podczas składowania i odtwarzania profili. Może to mieć także wpływ na wydajność całego systemu. Aby zapobiec negatywnemu wpływowi na wydajność systemu lub operacji systemowych, nie należy przypisywać obiektów tylko jednemu profilowi właściciela w całym środowisku System i5. 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 “Maksymalna wielkość pamięci” na stronie 96.

Grupowe prawo własności do obiektów

Ten temat zawiera szczegółowe informacje o grupowym prawie 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. Obiekty tworzone w katalogach nie używają wartości OWNER i GRPAUT do określania prawa własności lub uprawnienia grupowego. Właścicielem obiektu będzie zawsze jego twórca.

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 149 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 wyłącznie jeśli wartość systemowa QAUDLVL zawiera *CREATE, zaś wartość systemowa QAUDCTL zawiera *AUDLVL.

  Pojęcia pokrewne

  “Profile grupowe” na stronie 4
  Profil grupowy jest szczególnym typem profilu użytkownika. Można go używać do definiowania uprawnień dla grupy użytkowników, zamiast przyznawania uprawnień każdemu użytkownikowi z osobna.

Grupa podstawowa obiektu

Dla obiektu można określić grupę podstawową.

Nazwa profilu grupy podstawowej oraz uprawnień grupy podstawowej do obiektu przechowywane są razem z obiektem. Podczas sprawdzania uprawnień dla obiektu, korzystanie z uprawnień grupy podstawowej może zapewnić lepszą wydajność niż korzystanie z uprawnień grupy prywatnej.

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 149 zawiera przykłady sposobu przypisywania uprawnień podczas tworzenia nowych obiektów. W przypadku obiektów opartych o katalogi w niektórych systemach plików, obiekt dziedziczy grupę podstawową swojego katalogu nadrzędnego. Na przykład, jeśli grupa podstawowa katalogu nadrzędnego to FRED, to FRED może mieć problemy z tworzeniem czegokolwiek w tym katalogu nadrzędnym. Dzieje się tak ponieważ ten sam profil nie może być jednocześnie właścicielem i grupą podstawową tego samego obiektu.

Grupę podstawową dla obiektów opartych na bibliotekach i katalogach można zmienić za pomocą jednej z następujących komend:

- Zmiana grupy podstawowej obiektu (Change Object Primary Group - CHGOBJPGP)
- Zmiana grupy podstawowej (Change Primary Group - CHGPGP)
- Opcja 9 komendy Praca z obiektami wg. grupy podstawowej (Work with Objects by Primary Group - WRKOBJPGP)

Uprawnienia grupy podstawowej można zmienić za pomocą komendy Edycja uprawnień dla obiektu (Edit Object Authority - EDTOBJAUT) lub za pomocą komend nadawania i odbierania uprawnień. Uprawnienia grupy podstawowej dla obiektu opartego na bibliotece lub katalogu można zmienić za pomocą komendy Zmiana uprawnień (Change Authority - CHGAUT) lub za pomocą komendy Praca z uprawnieniami (Work with Authority - WRKAUT).

Pojęcia pokrewne

"Profile grupowe" na stronie 4
Profil grupowy jest szczególnym typem profilu użytkownika. Można go używać do definiowania uprawnień dla grupy użytkowników, zamiast przyznawania uprawnień każdemu użytkownikowi z osobna.

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.

Następujące sytuacje mogą spowodować nadanie profilowi QDFTOWN praw własności obiektu:

- 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 poprawności odtwarzanych programów" na stronie 18,
- 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 planować ochrony w ten sposób, że profil QDFTOWN posiadałby obiekty w normalnych okolicznościach.

Przypisywanie uprawnień i prawa własności nowym obiektom

W systemie można przypisać uprawnienia 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 na stronie 150 do Rys. 9 na stronie 153 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)
```

lub

```
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:

Domyślną wartością parametru AUT dla większości komend CRTxxx jest *LIBCRTAUT .

Rysunek 6. Przykład nowego obiektu: uprawnienia publiczne z biblioteki, grupa ma nadane uprawnienie 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 uprawnienie 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 uprawnienie 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 z biblioteki, grupa jest właścicielem obiektu

Obiekty adoptujące uprawnienia właściciela

Uprawnienia adoptowane można przypisać do programu użytkownika w celu umożliwienia zmiany zbioru klienta.

W zależności od sytuacji, czasami użytkownik potrzebuje różnych uprawnień do obiektu lub do aplikacji. Na przykład, użytkownik może być w stanie zmienić informacje w zbiorze klientów, za pomocą programów 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 takiej sytuacji byłoby 1) przydzielenie użytkownikowi uprawnień *USE dla informacji o klientach, co pozwoliłoby na wysyłanie zapytań zbiorów, oraz 2) użycie uprawnień adoptowanych w programach obsługi klientów, aby pozwolić użytkownikowi na 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.

Należy zapoznać się z tematem Ograniczenie użycia uprawnień adoptowanych dotyczącym uwarunkowań bezpieczeństwa i uprawnień adoptowanych podczas korzystania z pakietów SQL.

Następujący opis dotyczy uprawnień adoptowanych:

- 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 wywołań. Na przykład, załóżmy że PGMA korzysta z uprawnień adoptowanych:
  - Jeśli program PGMA uruchamia program PGMB korzystając z komendy CALL, stosy wywołań przed i po użyciu komendy CALL wyglądają następująco:

Tabela 119. Uprawnienia adoptowane i komenda CALL

Stos wywołań przed użyciem komendy CALL:	**Stos wywołań po użyciu komendy CALL:**
QCMD • • • PGMA	QCMD • • • PGMA PGMB

Ponieważ program PGMA pozostaje na stosie wywołań 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 ignorujące uprawnienie adoptowane” na stronie 156),

  - Jeśli program PGMA uruchamia program PGMB za pomocą komendy Kontrola transferu (Transfer Control - TFRCTL), stosy wywołań wyglądają następująco:

Tabela 120. Uprawnienia adoptowane i komenda TFRCTL

Stos wywołań przed użyciem komendy TFRCTL:	**Stos wywołań po użyciu komendy TFRCTL:**
QCMD • • • PGMA	QCMD • • • PGMB

Program PGMB nie korzysta z uprawnień adoptowanych programu PGMA, ponieważ program PGMA został zdjęty ze stosu wywołań.

- jeśli program 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 posiadać uprawnienia uruchamiania programu obsługi klawisza ATTN lub programu początkowego zadania grupy. W przeciwnym razie 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,
- Uprawnienia adoptowane nie są używane przez zintegrowane systemy plików, m.in. ″root″ (/), QOpenSys, QDLS, i systemy plików użytkownika.
- 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,
- wszelkie utworzone obiekty, w tym zbiory buforowe, mogące zawierać dane poufne, należą do użytkownika programu lub do jego profilu grupowego, nie zaś do właściciela programu.
- uprawnienia adoptowane mogą zostać określone w komendzie tworzącej program (CRTxxxPGM), zmieniającej program(CHGPGM) lub zmieniającą program usługowy (CHGSRVPGM).
- jeśli program jest tworzony z parametrem REPLACE(*YES) komendy 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* - User profile) i czy używa uprawnień adoptowanych z poprzedniego programu ze stosu wywołań (pole *Użycie uprawnień adoptowanych* - Use adopted authority). 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 komendy.

“Schemat blokowy 8: Jak są sprawdzane uprawnienia adoptowane” na stronie 187 udostępnia więcej informacji dotyczących uprawnień adoptowanych. Temat “Używanie uprawnień adoptowanych w projekcie menu” na stronie 237 pokazuje przykład sposobu użycia uprawnień adoptowanych w aplikacji.

Uprawnienia adoptowane i 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.

Czynniki ryzyka związane z uprawnieniami adoptowanymi i zalecenia

Uprawnień adoptowanych należy używać z rozwagą, aby zapobiec wystąpieniu ryzyka związanego z bezpieczeństwem.

Umożliwienie uruchamiania programu z uprawnieniami adoptowanymi jest zamierzonym pozbawieniem kontroli. Zezwala się użytkownikowi na posiadanie uprawnień dla obiektów oraz uprawnień specjalnych, których w normalnych warunkach użytkownik by nie posiadał. 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 monitorować funkcje udostępniane przez programy, które adoptują uprawnienia; Należy upewnić się, że programy te nie dają użytkownikom możliwości uzyskania dostępu do obiektów znajdujących się poza kontrolą programu, takich jak możliwość wprowadzania komend.
- należy upewnić się, że programy nie adoptują uprawnień i wywołują inne programy do wykonywania kwalifikowanych wywoływań bibliotek. 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 ignorujące uprawnienie adoptowane

Podanie parametru użycia uprawnień adoptowanych (USEADPAUT) umożliwia określenie, czy program będzie używał uprawnień adoptowanych.

Administrator może nie życzyć sobie, aby niektóre programy korzystały z uprawnień adoptowanych poprzednich programów znajdujących się na stosie wywołań. Na przykład, jeśli użytkownik korzysta z programu menu początkowego, adoptującego uprawnienia właściciela, to może nie życzyć sobie, aby programy wywoływane poprzez ten program korzystały z 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 jest tworzony z

parametrem REPLACE(*YES) komendy CRTxxxPGM, nowa kopia programu ma takie same wartości parametrów USRPRF, USEADPAUT i AUT, jakie miał zastępowany program.

Temat “Ignorowanie uprawnień adoptowanych” na stronie 240 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 36.

Ważne: 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 okazać się pomocne, jeśli użytkownik nie zna ustawienia USEADPAUT wywoływanej funkcji.

Pojęcia pokrewne

“Ignorowanie uprawnień adoptowanych” na stronie 240
Technika użycia uprawnień adoptowanych w projekcie menu wymaga, aby przed uruchomieniem zapytań użytkownik powrócił do menu początkowego. Jeśli ma być zapewniona wygoda uruchamiania zapytań z menu aplikacji, a także z menu początkowego, można tak ustawić program QRYSTART, aby ignorował uprawnienia adoptowane.

Magazyny uprawnień

Magazyn uprawnień jest narzędziem do przechowywania uprawnień do zbiorów bazy danych opisanych przez program, które aktualnie nie istnieją w systemie.

Podstawowym zastosowaniem magazynu uprawnień jest jego 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. Następujące opisy dotyczą magazynów uprawnień:

- 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 służą wyłącznie do przechowywania zbiorów baz danych opisywanych przez programy i zbiorów logicznych.
- Po utworzeniu magazynu uprawnień, należy nadać mu uprawnienia w ten sam sposób, w jaki nadaje się je zbiorom. 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; Na ekranach nie ukazują się informacje dotyczące istnienia zbioru, ani posiadania przez zbiór magazynu 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 również użyć jej w celu utworzenia zbioru wyjściowego (OUTFILE) w celu 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 systemu 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).

Czynniki ryzyka dla magazynu uprawnień

Jeśli używany jest magazyn uprawnień, należy wziąć pod uwagę bezpieczeństwo.

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 tworzy, przenosi, lub zmienia nazwę zbioru, to może on utworzyć magazyn uprawnień dla nowego zbioru. Użytkownik uzyskuje tym samym 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

W temacie niniejszym przedstawiono najczęściej używane metody konfigurowania, obsługiwania i wyświetlania informacji o uprawnieniach dotyczących systemu.

Dodatek A, “Komendy bezpieczeństwa”, na stronie 319 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

W tej sekcji opisano niektóre parametry ekranów wyświetlających uprawnienia do obiektów.

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).

Rys. 10 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 10. Wyświetlenie uprawnień dla obiektu, ekran

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

                       Obiekt          ----------Obiekt-----------
Użytkownik  Grupa      Uprawn,    Opr  Zarz. Istn. Zmien. Ref
*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

                       Obiekt     ---------------Dane---------------
Użytkownik  Grupa      Uprawn.    Odcz. Dod.  Akt.    Usuw.   Uruch.
*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

                      Obiekt     -----------Obiekt-----------
Użytkownik  Grupa     Uprawn,    Opr  Zarz. Istn. Zmien. Ref
*ADOPTED              USER DEF         X     X      X     X
*PUBLIC                *EXCLUDE
PGMR1                  *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

               OBIEKT     -----Obiekt------   ------Dane--------
Użytk.  Grupa  Uprawn.     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).

Informacje pokrewne

Narzędzia bezpieczeństwa systemu

Praca z bibliotekami

Można określić uprawnienia do bibliotek oraz nowych obiektów utworzonych w bibliotekach.

Na uprawnienia mają wpływ dwa parametry komendy Tworzenie biblioteki (Create Library - CRTLIB):

Uprawnienia (AUT): Parametr AUT może służyć do określenia dowolnego z poniższych uprawnień:

- 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 chroniony listą 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 określający komendę CRTLIB jest właścicielem biblioteki, chyba że profil użytkownika ma określoną opcję 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 . . . . . . . . . . . . . . . . :   TESTLIB

Typ. . . . . . . . . . . . . . . . . . . . :   PROD
Numer ASP. . . . . . . . . . . . . . . . . :   1
Urządzenie ASP . . . . . . . . . . . . . . :   *SYSBAS
Uprawnienie do tworzenia . . . . . . . . . :   OBJLST
Kontrola tworzonego obiektu  . . . . . . . :   *SYSVAL
Tekst opisu. . . . . . . . . . . . . . . . :   Rek klienta
```

Tworzenie obiektów

Można określić uprawnienie do nowego obiektu.

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:

```
                         Wyśw. uprawnień dla obiektu
Obiekt . . . . . . :   DTA1        Właściciel . . . . . . . . :   PGMR1
  Biblioteka . . . :   TESTLIB     Grupa podstawowa . . :   *NONE
Typ obiektu. . . . :   *DTAARA     Urządzenie ASP . . . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji . . . . . :   OBJLST

                       ObiektUżytkownik  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:

```
                         Wyśw. uprawnień dla obiektu
Obiekt . . . . . :   DTA2         Właściciel  . . . . . :   PGMR1
  Biblioteka . . :   TESTLIB    Grupa podstawowa . . :   *NONE
Typ obiektu. . . :   *DTAARA     Urządzenie ASP . . . . . :   *SYSBAS

Obiekt zabezpieczony listą autoryzacji . . . . . :   *NONE

                       ObiektUżytkownik  Grupa       do obiektu
*PUBLIC                *CHANGE
PGMR1                   *ALL
```

Praca z uprawnieniami jednego obiektu

Można zmienić uprawnienia dla obiektu.

Aby zmienić uprawnienia dla obiektu, użytkownik musi posiadać jedno z następujących uprawnień:

- 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). Ekran ten można przywołać bezpośrednio poprzez użycie komendy Edycja uprawnień dla obiektu (Edit Object Authority - EDTOBJAUT) lub wybór odpowiedniej opcji z ekranu Praca z obiektami wg użytkownika, Praca z obiektami wg uprawnień prywatnych, Praca z obiektami wg grupy podstawowej lub Praca z obiektami.

```
                          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

W temacie znajdują się informacje dotyczące określania 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

                       Obiekt          ----------Obiekt-----------
Użytkownik  Grupa      Uprawn,    Opr  Zarz. Istn. Zmien. Ref
*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

                       Obiekt     ---------------Dane---------------
Użytkownik  Grupa      Uprawn.    Odcz. Dod.  Akt.    Usuw.   Uruch.
*PUBLIC                *AUTL
PGMR1                  USER DEF    X     X     X       X        X
```

Nadawanie uprawnień nowym użytkownikom

Można nadać uprawnienia 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.

            Obiekt
Użytkownik  do obiektu
USER1       *USE
USER2       *CHANGE
PGMR2       *ALL
```

Usuwanie uprawnień użytkownika

Uprawnienia użytkownika do obiektu można również usuwać.

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.

Uwaga: Uprawnienia *EXCLUDE profilu grupy mogą zostać unieważnione jeśli użytkownik posiada inny profil gtupowy z uprawnieniami prywatnymi dla obiektu.

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:

```
                      Wyśw. uprawnień dla obiektu (Display Object Authority)

Obiekt . . . . . :   ZBIORB     Właściciel  . . . . . :   PGMR1
  Biblioteka . . . :   BIB_B     Grupa podstawowa . . :   *NONE
Typ obiektu . . . :   *FILE      Urządzenie ASP . . . :   *SYSBAS

  Obiekt jest chroniony przez listę autoryzacji.. . . . . :   *NONE

                     Obiekt    --------Obiekt------------
Użytk.  Grupa     Uprawn,  Opr   Zarz. Istn.   Zmien. Ref
USERB            USER DEF         X    X       X       X
```

```
                      Wyśw. uprawnień dla obiektu (Display Object Authority)

Obiekt . . . . . :   ZBIORB     Właściciel  . . . . . :   PGMR1
  Biblioteka . . . :   BIB_B     Grupa podstawowa . . :   *NONE
Typ obiektu. . . :   *FILE     Urządzenie ASP . . . . . :   *SYSBAS

Obiekt zabezpieczony przez listę autoryzacji . . . . . .   *NONE

                       Obiekt     ---------------Dane---------------
Użytkownik  Grupa      Uprawn.    Odcz. Dod.  Akt.    Usuw.   Uruch.
USERB                  USER DEF
```

Praca z uprawnieniami dla wielu obiektów

Informacje o wykonywaniu zmian uprawnień jednocześnie w wielu obiektach.

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)

Podaj wybrane opcje i naciśnij klawisz 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 niektóre obiekty w bibliotece TESTLIB posiadają uprawnienia prywatne *CHANGE, wyświetlona komenda nie zmniejszy ich uprawnień prywatnych do *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)

Podaj wybrane opcje i naciśnij klawisz 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)
Podaj wybrane opcje i naciśnij klawisz 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)
Podaj wybrane opcje i naciśnij klawisz Enter.

Obiekt . . . . . .   AR*
  Biblioteka  . . . . . .   TESTLIB
Typ obiektu  . . . . . .  *FILE
Urządzenie ASP. . . . . .  *
Użytkownicy. . . . . .   *PUBLIC
              + więcej wartości
Uprawnienie. . . . . .   *AUTL
```

Praca z prawami własności do obiektu

Prawo własności do obiektu można zmienić na kilka sposobów.

Aby zmienić właściciela obiektu, należy posłużyć się jedną 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 obiektami 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=Wyświetl opis    9=Zmień 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 124 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 jest wyświetlany znak większości (>). Aby wyświetlić bezwzględną nazwę ścieżki, należy umieścić kursor na nazwie ścieżki i nacisnąć klawisz F22.

Praca z uprawnieniami grupy podstawowej

Można zmienić grupę podstawową lub uprawnienia grupy podstawowej do obiektu.

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 podstawową grupę obiektu, użytkownik musi posiadać następujące uprawnienia:

- 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 musi być właścicielem 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.

Korzystanie z obiektu odniesienia

Zarówno ekran Edycja uprawnień dla obiektu (Edit Object Authority), jak i komenda GRTOBJAUT, umożliwiają nadanie uprawnień do obiektu (lub grupy obiektów) na podstawie uprawnień 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 “Korzyści wynikające ze stosowania listy autoryzacji” na stronie 171.

Kopiowanie uprawnień 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 129 pokazuje przykład takiej operacji.

Komenda GRTUSRAUT kopiuje jedynie uprawnienia prywatne. Nie kopiuje ona uprawnień specjalnych, nie przekazuje też praw własności obiektów.

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.

Zadania pokrewne

“Kopiowanie uprawnień prywatnych” na stronie 124
Za pomocą komendy Nadanie uprawnień użytkownika (Grant User Authority - GRTUSRAUT) można skopiować uprawnienia prywatne z jednego profilu użytkownika do innego.

Praca z listami autoryzacji

Sekcja zawiera czynności związane z tworzeniem listy 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 wykonywać w dowolnej kolejności.

Korzyści wynikające ze stosowania listy autoryzacji

Listy autoryzacji służą do zabezpieczenia obiektów w systemie.

Lista autoryzacji daje następujące korzyści:

- Listy autoryzacji ułatwiają zarządzanie uprawnieniami. Definiuje 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 zostanie odtworzony na innym systemie, lista autoryzacji nie zostanie dowiązana, chyba że wraz z komendą odtwarzania określony zostanie parametr ALWOBJDIF(*ALL) lub ALWOBJDIF(*AUTL).
- Z punktu widzenia zarządzania ochroną, listy autoryzacji są preferowaną metodą zarządzania obiektami mającymi takie same wymagania ochrony. Nawet w przypadku, gdy istnieje tylko kilka obiektów, które są zabezpieczone przez listę, wykorzystanie listy autoryzacji jest bardziej opłacalne, niż wykorzystanie uprawnień prywatnych. 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.

Tworzenie listy autoryzacji

Aby utworzyć listę autoryzacji, należy użyć komendy Tworzenie listy autoryzacji (Create Authorization List - CRTAUTL).

Aby utworzyć listę autoryzacji w bibliotece QSYS, nie są potrzebne żadne uprawnienia do tej biblioteki. Należy użyć komendy Tworzenie listy autoryzacji (Create Authorization List - CRTAUTL).

```
                    Tworzenie listy autoryzacji (Create Authorization List - CRTAUTL)

Wpisz wybór i naciśnij klawisz Enter.

Lista autoryzacji . . . . . .   custlst1      Nazwa
Tekst opisu . . . . . .   Zbiory wyzerowane pod koniec miesiąca

                         Dodatkowe parametry
                       (Additional Parameters)

Uprawnienie  . . . . . .  *use          *CHANGE, *ALL, *USE, *EXCLUDE
```

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

Ekran Edycja listy autoryzacji (EDTAUTL) umożliwia nadanie użytkownikom uprawnień do wcześniej utworzonej 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 143.

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

Obiekt . . . . . :   CUSTLST1        Właściciel . . . . . :   PGMR1
  Biblioteka . . . :     QSYS          Grupa podstawowa . . :   *NONE

Wpisz zmiany obecnych uprawnień i naciśnij Enter.

            Obiekt    Lista
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

Obiekt . . . . . :   CUSTLST1     Właściciel . . PGMR1
  Biblioteka . . . :     QSYS

Wpisz nowych użytkowników i naciśnij Enter.

            Obiekt    Lista
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:

- Dodanie pozycji listy autoryzacji (Add Authorization List Entry - ADDAUTLE), aby zdefiniować uprawnienia dla dodatkowych użytkowników.
- Zmiana pozycji listy autoryzacji (Change Authorization List Entry - CHGAUTLE), aby zmienić uprawnienia dla użytkowników, którzy już posiadają uprawnienia dla listy.
- komenda Usunięcie pozycji listy autoryzacji (Remove Authorization List Entry - RMVAUTLE) do usunięcia uprawnień użytkownika z listy.
- Praca z uprawnieniami (Work with Authority - WRKAUT), aby wyświetlić listę użytkowników autoryzowanych dla danego obiektu.
- Zmiana uprawnień (Change Authority - CHGAUT), aby zmienić uprawnienia użytkownika dla obiektu.

Zabezpieczanie 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.

Do zabezpieczenia obiektu za pomocą listy autoryzacji należy użyć ekranu Edycja uprawnień dla obiektu (Edit Object Authority) i komendy GRTOBJAUT, WRKAUT lub CHGAUT:

```
                          Edycja uprawnień dla obiektu (Edit Object Authority)
Obiekt . . . . . :   ARWRK1       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

           Uprawnienie
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) można użyć klawisza F15 (Wyświetlenie obiektów listy autoryzacji), aby wyświetlić wszystkie obiekty zabezpieczone przez listę:

```
                    Wyświetlenie obiektów listy autoryzacji (Display
Authorization List Objects)
Lista autoryzacji  . . . . . :   CUSTLST1
  Biblioteka . . . . . :   CUSTLIB
Właściciel . . . . . :   OWNAR
Grupa podstawowa . . . . . :   DPTAR

                                          Grupa
Obiekt      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. Można również użyć komendy Wyświetlenie obiektów listy autoryzacji (Display Authorization List Objects - DSPAUTLOBJ), aby wyświetlić lub wydrukować wszystkie obiekty zabezpieczone przez tę listę.

Konfigurowanie listy autoryzacji

Konfiguracja list autoryzacji ułatwia zmianę osób autoryzowanych do korzystania z obiektów oraz zabezpieczanie nowych obiektów za pomocą takich samych uprawnień, jak istniejące obiekty.

W firmie JKL Toy Company lista autoryzacji używana jest do zabezpieczania wszystkich zbiorów roboczych, które są używane podczas przetwarzania stanów magazynowych 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.

Aby skonfigurować listę autoryzacji, wykonaj następujące czynności:

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)
```

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.

Usuwanie listy autoryzacji

Może zaistnieć potrzeba usunięcia utworzonej listy autoryzacji.

Jeśli lista autoryzacji używana jest do zabezpieczania jakichkolwiek obiektów, nie można jej usunąć. Komenda DSPAUTLOBJ umożliwi wyświetlenie wszystkich obiektów zabezpieczanych przez tę listę. Aby zmienić uprawnienia dla każdego z obiektów, należy skorzystać z komend Zmiana uprawnień (Change Authority - CHGAUT), ekranu Edycja uprawnień dla obiektu lub komendy Odwołanie uprawnień dla obiektu (Revoke Object Authority -RVKOBJAUT). Gdy lista autoryzacji nie zabezpiecza już żadnych obiektów, można ją usunąć za pomocą komendy Usunięcie listy autoryzacji (Delete Authorization List - DLTAUTL).

Jak system sprawdza uprawnienia

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 adoptujące uprawnienia właściciela” na stronie 153.

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: Możliwa jest kumulacja uprawnień z kilku grup użytkownika w celu znalezienia wystarczających uprawnień dla obiektu, do którego użytkownik próbuje uzyskać dostęp.

Schematy blokowe sprawdzania uprawnień

Ta sekcja zawiera wprowadzenie do schematów blokowych, 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 dla obiektu, czynności niektórych schematów blokowych należało będzie powtórzyć kilkakrotnie.

Liczby w lewym górnym rogu bloków na schematach blokowych używane są w przykładach następujących po tych schematach.

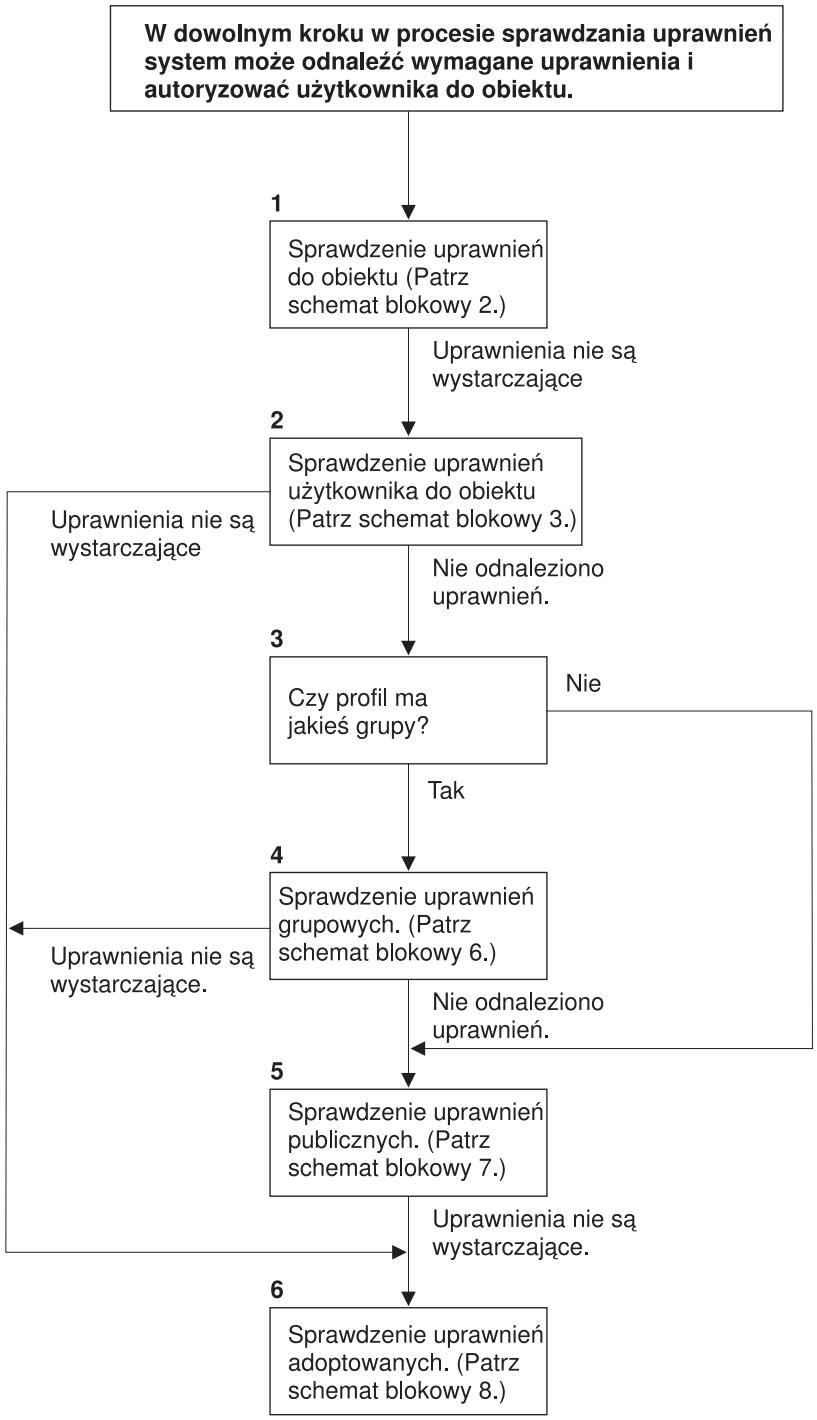
Wymienione poniżej czynności reprezentują wyszukiwanie uprawnień prywatnych profilu:

- Krok 6, Rys. 13 na stronie 179
- Krok 6, Rys. 16 na stronie 185
- Krok 2, Rys. 19 na stronie 190

Powtarzanie tych czynności może spowodować problemy związane z wydajnością procesu sprawdzania uprawnień.

Schemat blokowy 1: Proces sprawdzania uprawnień

Kroki schematu blokowego 1 prezentują główny proces wykonywany przez 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 11. Schemat blokowy 1: Proces sprawdzania uprawnień

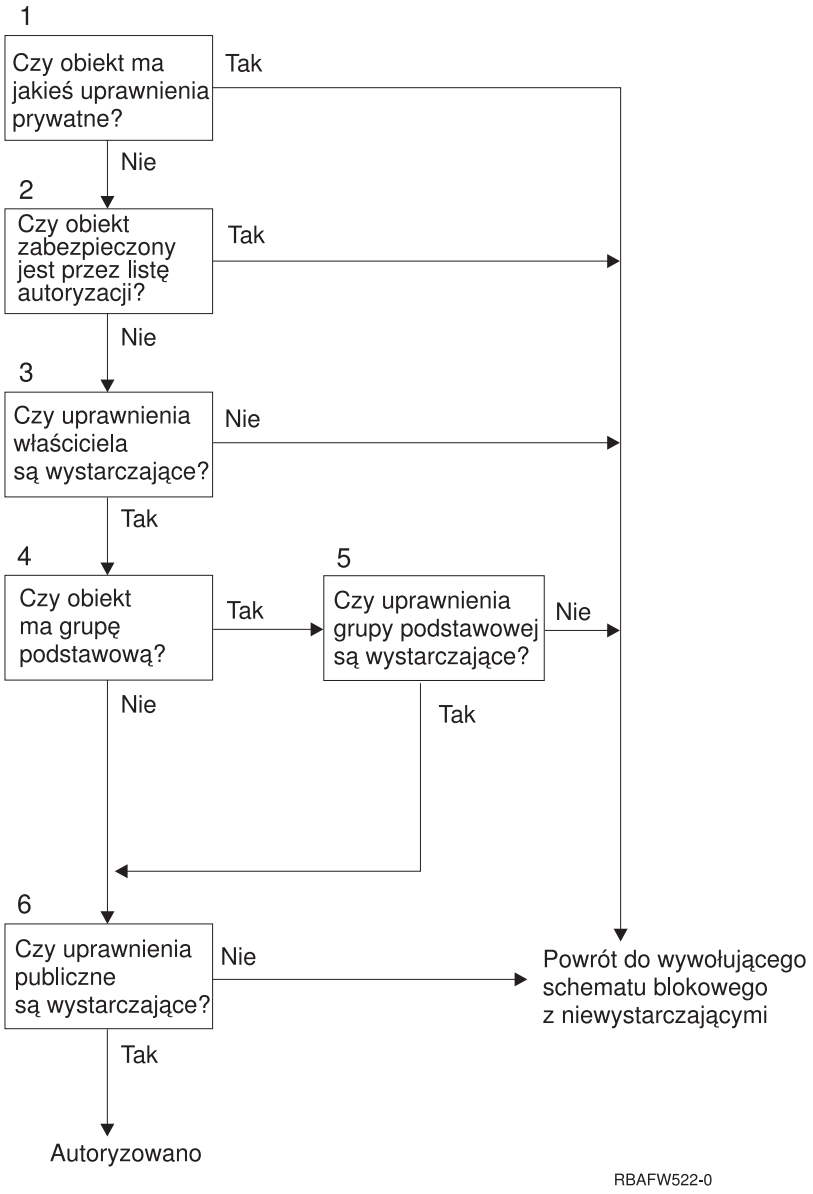
Opis schematu blokowego 1: Główny proces sprawdzania uprawnień

Uwaga: W czasie dowolnej czynności procesu sprawdzania uprawnień istnieje możliwość, że system nie znajdzie wystarczających uprawnień, aby dać użytkownikowi dostęp 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 czynności 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 czynności 3. Jeśli system stwierdzi, że uprawnienia użytkownika są niewystarczające, przechodzi do czynności 6.
3. System sprawdza, czy profil użytkownika należy do jakiejś grupy. Jeśli tak jest, system przechodzi do czynności 4. W przeciwnym przypadku system przechodzi do czynności 5.
4. System określa uprawnienia grupowe. (Patrz Schemat blokowy 6). Jeśli system stwierdzi, że nie istnieje uprawnienie grupowe do obiektu, przechodzi do czynności 5. Jeśli stwierdzi, że uprawnienie grupowe do obiektu jest niewystarczające, przechodzi do czynności 6.
5. System sprawdza uprawnienia publiczne do obiektu. (Patrz Schemat blokowy 7). Jeśli system stwierdzi, że uprawnienia publiczne są niewystarczające, przechodzi do czynności 6.
6. System sprawdza uprawnienia adoptowane do obiektu. (Patrz Schemat blokowy 8).

Schemat blokowy 2: Krótka ścieżka sprawdzania uprawnień do obiektu

Czynności pokazane na schemacie blokowym 2 są wykonywane przy użyciu informacji przechowywanych z obiektem. Jest to najszybsza metoda autoryzowania użytkownika do obiektu.



Rysunek 12. Schemat blokowy 2: Krótka ścieżka uprawnień do obiektu

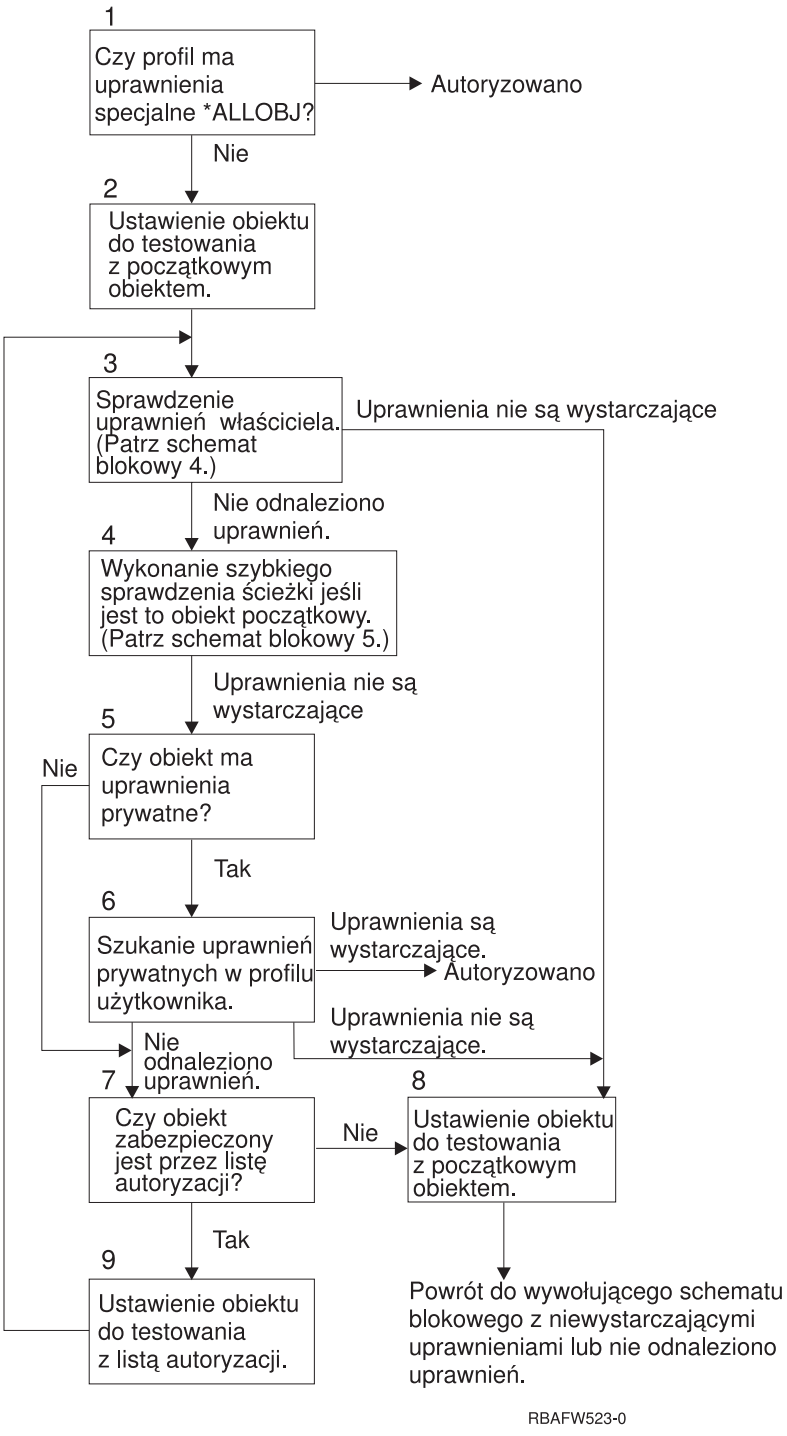
Opis Schematu blokowego 2: Krótka ścieżka uprawnień do obiektu

1. System sprawdza, czy obiekt ma uprawnienia prywatne. Jeśli tak jest, system wraca do wywołującego schematu blokowego z wystarczającymi uprawnieniami. Jeśli nie ma, system przechodzi do czynności 2.
2. System sprawdza, czy obiekt jest chroniony przez listę autoryzacji. Jeśli tak jest, system wraca do wywołującego schematu blokowego z wystarczającymi uprawnieniami. Jeśli nie, przechodzi do czynności 3.
3. System sprawdza, czy właściciel obiektu ma wystarczające uprawnienia. Jeśli tak nie jest, system wraca do wywołującego schematu blokowego z niewystarczającymi uprawnieniami. Jeśli tak jest, system przechodzi do czynności 4.
4. System sprawdza, czy obiekt ma grupę podstawową. Jeśli tak jest, system przechodzi do czynności 5. W przeciwnym przypadku system przechodzi do czynności 6.
5. System sprawdza, czy grupa podstawowa obiektu ma wystarczające uprawnienia. Jeśli tak jest, system przechodzi do czynności 6. W przeciwnym przypadku system wraca do wywołującego schematu blokowego z niewystarczającymi uprawnieniami.

6. System sprawdza, czy uprawnienia publiczne są wystarczające. Jeśli są, obiekt jest autoryzowany. Jeśli tak nie jest, system wraca do wywołującego schematu blokowego z niewystarczającymi uprawnieniami.

Schemat blokowy 3: Jak są sprawdzane uprawnienia użytkownika do obiektu

Czynności przedstawione w schemacie blokowym 3 są wykonywane dla pojedynczego profilu użytkownika.



Rysunek 13. Schemat blokowy 3: Sprawdzanie uprawnień użytkownika

Opis schematu blokowego 3: Sprawdzanie uprawnień użytkownika

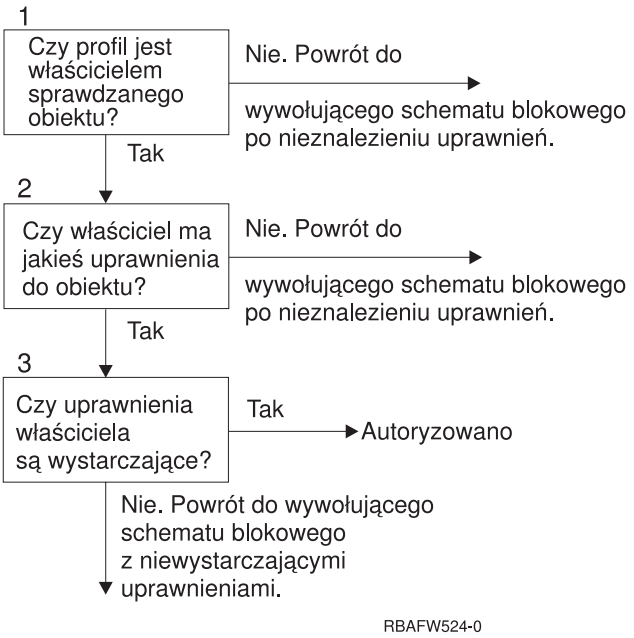
1. System sprawdza, czy profil użytkownika ma uprawnienia *ALLOBJ. Jeśli je ma, następuje autoryzowanie profilu. Jeśli profil nie ma uprawnień *ALLOBJ, proces sprawdzania uprawnień przechodzi do czynności 2.
2. System ustawia uprawnienia obiektu na równe początkowemu obiektowi. Proces sprawdzania uprawnień przechodzi do czynności 3.
3. System sprawdza uprawnienia właściciela. Jeśli uprawnienia nie są wystarczające, wtedy przechodzi do czynności 8. Jeśli nie zostaną odnalezione żadne uprawnienia, przechodzi do czynności 4.
4. System kończy krotką ścieżkę sprawdzania uprawnień obiektu początkowego. (Patrz Schemat blokowy 5). Jeśli uprawnienia nie są wystarczające, proces sprawdzania uprawnień przechodzi do czynności 5.
5. System określa, czy obiekt ma uprawnienia prywatne. Jeśli tak, proces sprawdzania uprawnień przechodzi do czynności 6. Jeśli nie, przechodzi do czynności 7.
6. System sprawdza uprawnienia prywatne profilu użytkownika. Jeśli są wystarczające, użytkownik zostaje autoryzowany. Jeśli nie są wystarczające, proces sprawdzania uprawnień przechodzi do czynności 8. Jeśli nie znaleziono żadnych uprawnień, proces sprawdzania przechodzi do czynności 7.
7. System sprawdza, czy obiekt jest chroniony przez listę autoryzacji. Jeśli nie, przechodzi do czynności 8. Jeśli jest chroniony przez listę autoryzacji, przechodzi do czynności 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 czynności 3.

Schemat blokowy 4: Sprawdzanie uprawnienia właściciela

W schemacie blokowym 4 jest pokazany proces sprawdzania uprawnienia 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.



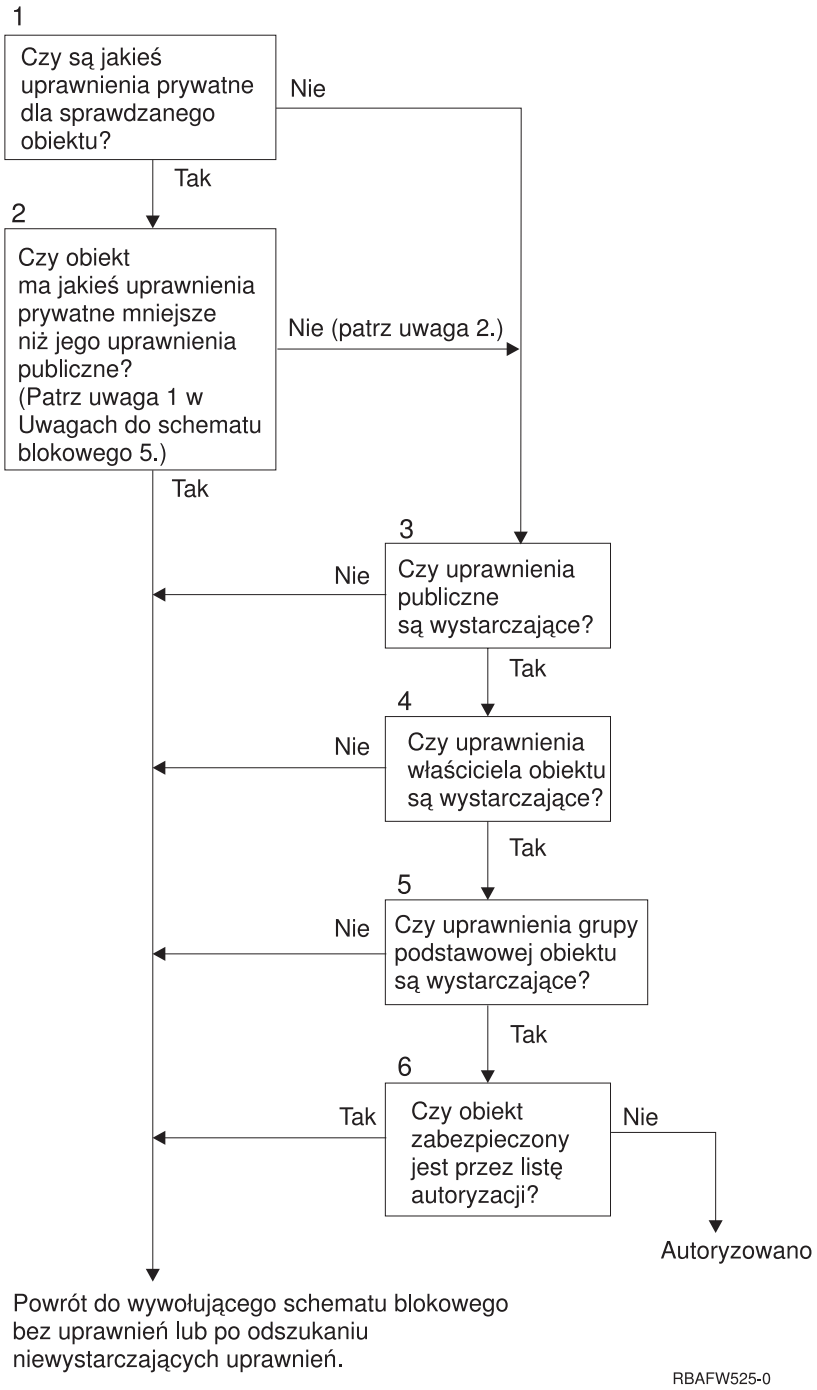
Rysunek 14. Schemat blokowy 4: Sprawdzanie uprawnienia właściciela

Opis schematu blokowego 4: Sprawdzanie uprawnienia właściciela

1. System określa, czy profil użytkownika jest właścicielem sprawdzanego obiektu. Jeśli profil użytkownika jest właścicielem obiektu, system przechodzi do czynności 2. W przeciwnym wypadku system wraca do wywołującego schematu blokowego z niewystarczającymi uprawnieniami.
2. Jeśli profil użytkownika jest właścicielem obiektu, system określa czy, właściciel ma uprawnienia do obiektu. Jeśli właściciel ma uprawnienie do obiektu, proces sprawdzania uprawnień przechodzi do czynności 3. Jeśli system stwierdzi, że właściciel nie ma uprawnienia 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

Schemat blokowy 5 pokazuje krótką ścieżkę do testowania uprawnień użytkownika bez przeszukiwania uprawnień prywatnych.



Rysunek 15. Schemat blokowy 5: Krótka ścieżka do uprawnień użytkownika

Uwagi do schematu blokowego 5:

1. Uprawnienia są uważane za mniejsze niż publiczne, jeśli dowolne uprawnienia, które są obecne dla *PUBLIC, nie są obecne dla innego użytkownika. Tabela 121 na stronie 183 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 121. Uprawnienia publiczne a uprawnienia prywatne

Uprawnienie	Użytkownicy			
	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 na pewno 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 uprawnień do 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 istnieją uprawnienia prywatne dla obiektu, procedura sprawdzania uprawnień przechodzi do czynności 2. W przeciwnym wypadku procedura przechodzi do czynności 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 czynności 3.
3. Jeśli obiekt nie ma uprawnień prywatnych lub nie ma on 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 czynności 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 czynności 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 czynności 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: Sposób sprawdzania uprawnień grupowego

Użytkownik może być członkiem maksymalnie 16 grup. Grupa może posiadać uprawnienia prywatne dla obiektu, lub może być jego grupą podstawową.

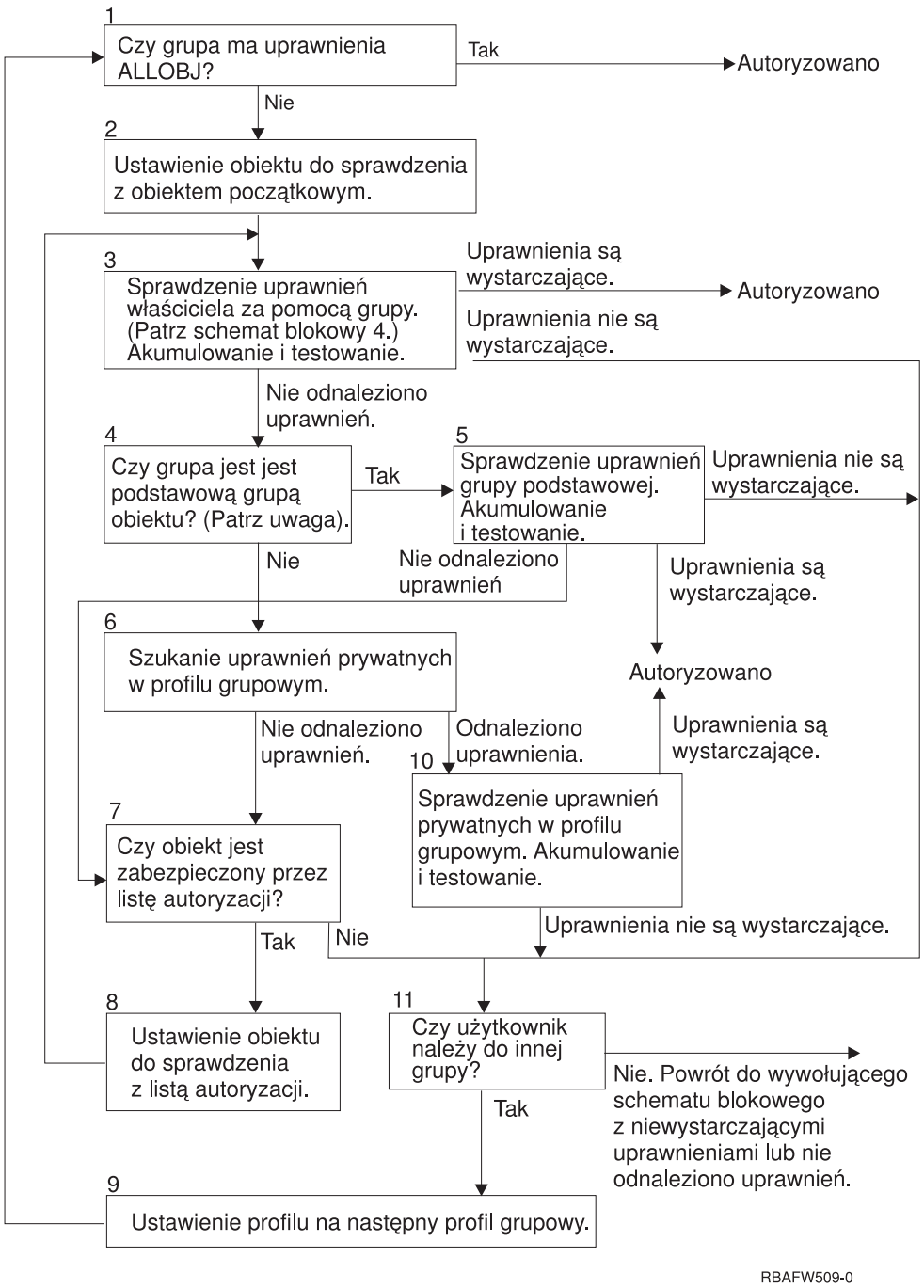
Możliwa jest kumulacja uprawnień z kilku grup użytkownika w celu znalezienia wystarczających uprawnień dla obiektu, do którego użytkownik próbuje uzyskać dostęp. Na przykład użytkownik WAGNERB potrzebuje uprawnień *CHANGE do zbioru CRLIM. Uprawnienia *CHANGE obejmują uprawnienia *OBJOPR, *READ, *ADD, *UPD, *DLT i *EXECUTE. Tabela 122 pokazuje uprawnienia do zbioru CRLIM:

Tabela 122. 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 Rys. 16 na stronie 185 pokazuje kolejne czynności w procesie sprawdzania uprawnień grupowych.



Rysunek 16. Schemat blokowy 6: Sprawdzanie uprawnień grupowych

Uwaga: Jeśli użytkownik wpisał się 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 czynności 2.
2. Jeśli grupa nie ma uprawnień *ALLOBJ, system ustawia sprawdzany obiekt na obiekt początkowy.

3. Po ustawieniu obiektu na obiekt początkowy, system sprawdza uprawnienia właściciela. (Patrz Schemat blokowy 4) Jeśli uprawnienia są wystarczające, to grupa zostaje uznana za autoryzowaną. W przeciwnym razie proces sprawdzania uprawnień przechodzi do czynności 11. Jeśli uprawnienia grupy nie zostały odnalezione, sprawdzanie uprawnień przechodzi do czynności 4.
4. Jeśli uprawnienia właściciela nie zostaną odnalezione, system sprawdza, czy grupa jest grupą podstawową obiektu.

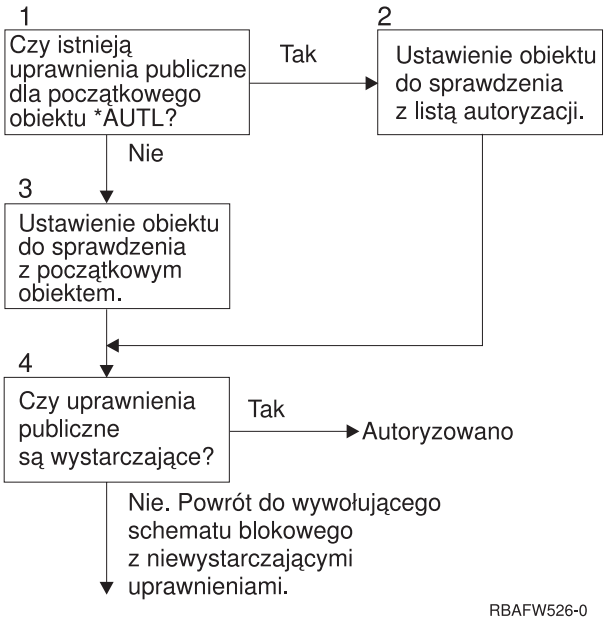
   Uwaga: Jeśli użytkownik wpisał się za pomocą profilu, który jest grupą podstawową dla obiektu, nie może uzyskać uprawnień do obiektu za pośrednictwem grupy podstawowej.

   Jeśli grupa jest grupa podstawową obiektu, wtedy proces sprawdzania uprawnień przechodzi do czynności 5. Jeśli grupa nie jest grupą podstawową obiektu, proces przechodzi do czynności 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 nie zostały odnalezione, sprawdzanie uprawnień przechodzi do czynności 7. Jeśli uprawnienia grupy podstawowej nie są wystarczające, wtedy sprawdzanie uprawnień przechodzi do czynności 11.
6. Jeśli grupa nie jest grupą podstawową obiektu, system sprawdza uprawnienia prywatne w profilu grupowym. Jeśli uprawnienia zostaną odnalezione, proces sprawdzania uprawnień przechodzi do czynności 10. W przeciwnym razie proces przechodzi do czynności 7.
7. Jeśli uprawnienia nie zostaną odnalezione dla uprawnień prywatnych profilu grupy, system sprawdza, czy obiekt jest zabezpieczony przez listę autoryzacji. Jeśli obiekt jest zabezpieczony przez listę autoryzacji, to proces sprawdzania uprawnień przechodzi do czynności 8. W przeciwnym razie proces przechodzi do czynności 11.
8. Jeśli obiekt jest chroniony przez listę autoryzacji, system ustawia obiekt na listę autoryzacji, a proces sprawdzania uprawnień powraca do czynności 3.
9. Jeśli użytkownik należy do innego profilu grupowego, system ustawia ten profil jako następny profil grupowy i powraca do czynności 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. W przeciwnym razie proces sprawdzania uprawnień przechodzi do czynności 11.
11. Jeśli uprawnienia nie zostały odnalezione lub są niewystarczające, system sprawdza, czy użytkownicy powiązani są z innym profilem grupowym. Jeśli użytkownik należy do innego profilu grupowego, system przechodzi do czynności 9. Jeśli użytkownik nie należy do innego profilu grupowego, system wraca do wywołującego schematu blokowego z niewystarczającymi uprawnieniami lub z brakiem uprawnień.

Schemat blokowy 7: Sprawdzanie uprawnień publicznych

Podczas sprawdzania uprawnień publicznych system musi określić, czy do obiektu lub listy autoryzacji mają być użyte uprawnienia publiczne.

Na schemacie blokowym 7 jest przedstawiony następujący proces:



Rysunek 17. 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 czynności 2. Jeśli uprawnienia do tego obiektu nie są uprawnieniami *AUTL, system przechodzi do czynności 3.
2. Jeśli uprawnienia publiczne do obiektu początkowego to uprawnienia *AUTL, system ustawia sprawdzany obiekt na listę autoryzacji i przechodzi do czynności 4.
3. Jeśli nie są to uprawnienia *AUTL, system ustawia sprawdzany obiekt na początkowy i przechodzi do czynności 4.
4. Jeśli sprawdzany obiekt został ustawiony na równoważny z listą autoryzacji lub obiektem początkowym, system sprawdza, czy uprawnienia publiczne są wystarczające. Jeśli tak jest, użytkownik jest autoryzowany do obiektu. W przeciwnym razie system wraca do wywołującego schematu blokowego z niewystarczającymi uprawnieniami.

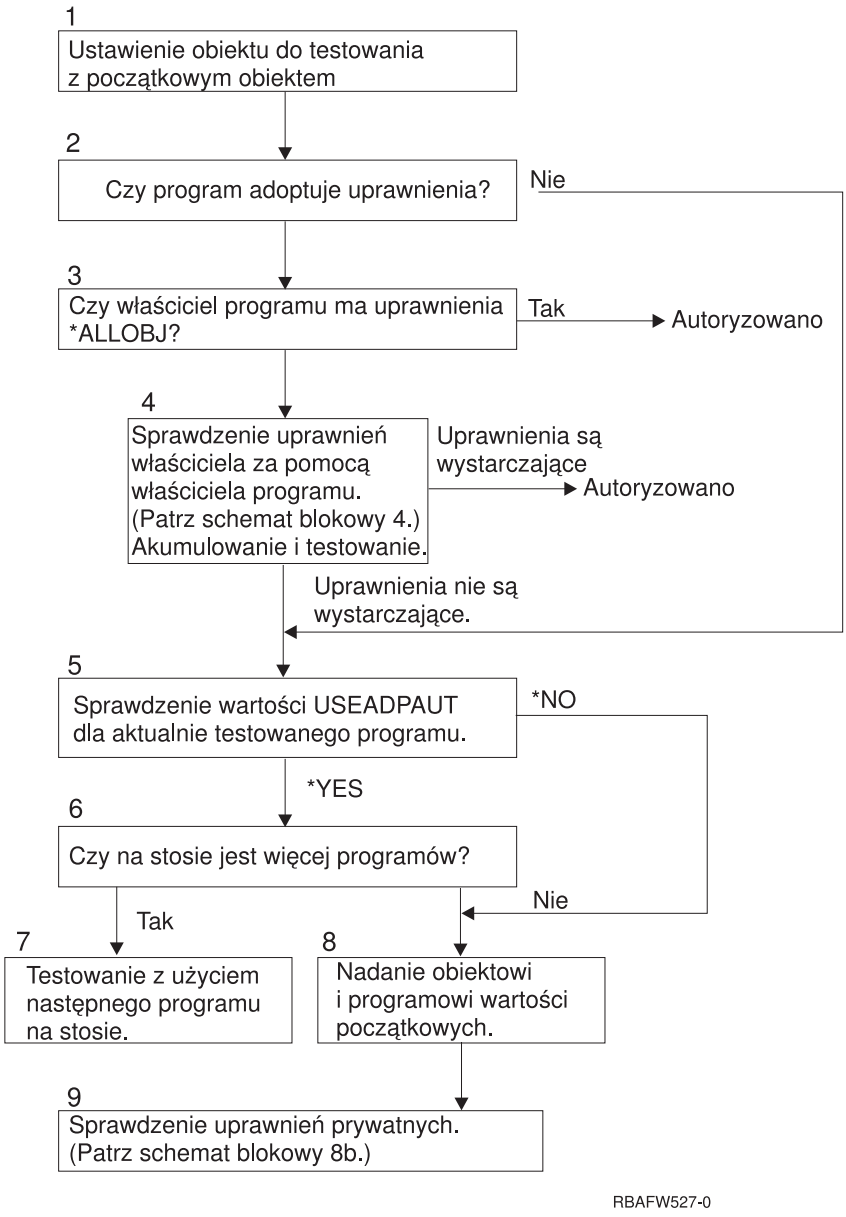
Schemat blokowy 8: Jak są sprawdzane uprawnienia adoptowane

Jeśli podczas sprawdzania uprawnień użytkownika uprawnienia będą niewystarczające, system sprawdza uprawnienia adoptowane.

System może korzystać z uprawnień adoptowanych z programu początkowego wywołanego przez użytkownika lub z wcześniejszych programów ze stosu wywołań. 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. Powtarzane to 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. 18 na stronie 188 i Rys. 19 na stronie 190 pokazują proces sprawdzania uprawnień adoptowanych.



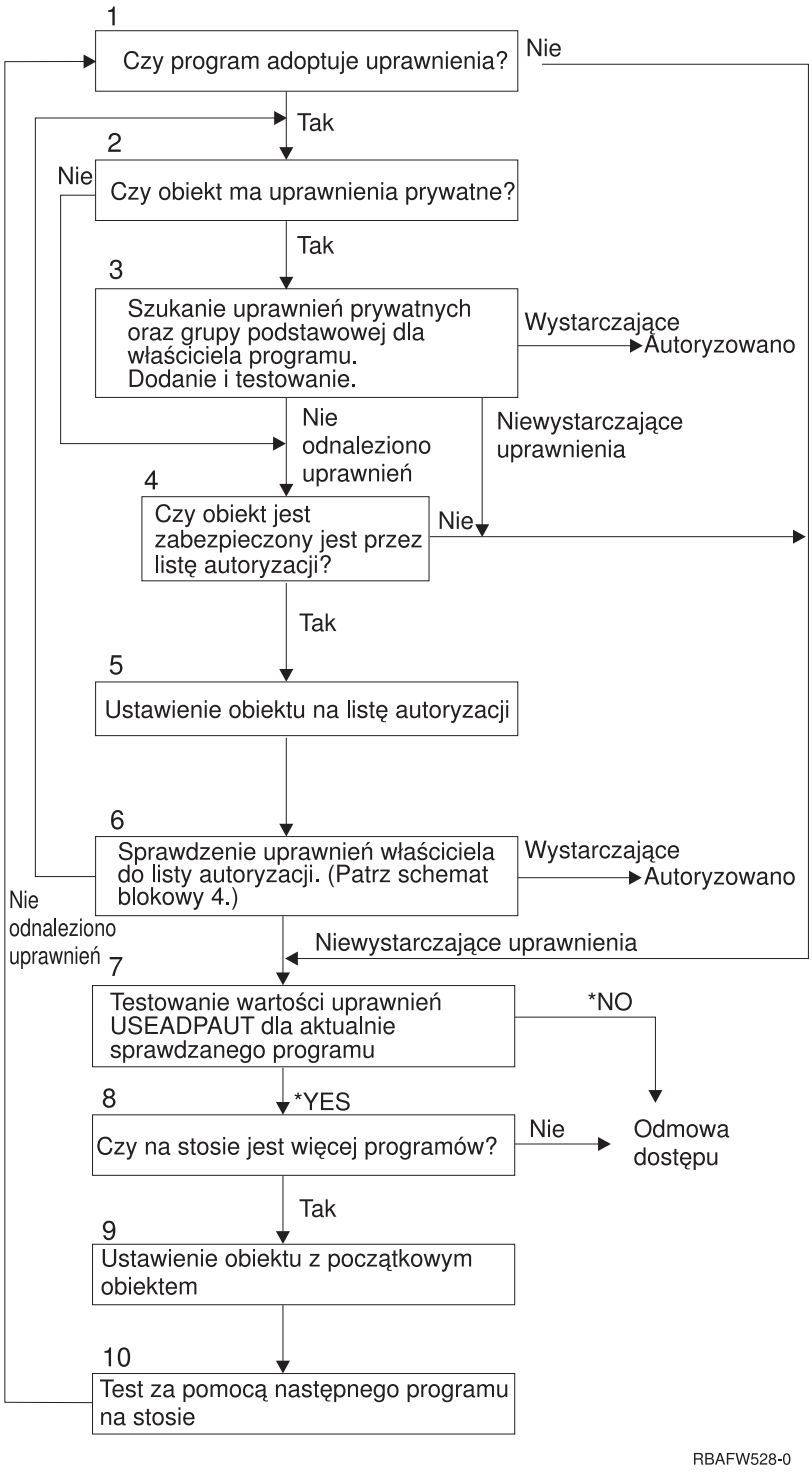
*Rysunek 18. Schemat blokowy 8A: Sprawdzanie uprawnień adoptowanych użytkownika *ALLOBJ i właściciela*

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 czynności 2.
2. System określa, czy program adoptuje uprawnienia. Jeśli program adoptuje uprawnienia, proces sprawdzania uprawnień przechodzi do czynności 3. Jeśli program nie adoptuje uprawnień i uprawnienia są niewystarczające, proces sprawdzania uprawnień przechodzi do czynności 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 czynności 4.
4. Jeśli właściciel programu nie ma uprawnień *ALLOBJ, system sprawdza i testuje uprawnienia właściciela. Jeśli są wystarczające, użytkownik zostaje autoryzowany. W przeciwnym razie proces sprawdzania uprawnień przechodzi do czynności 5.

5. System sprawdza wartość USEADPAUT dla aktualnie testowanego programu. Jeśli wartość ustawiona jest na *NO, proces sprawdzania uprawnień przechodzi do czynności 8. Jeśli wartość ustawiona jest na *YES, proces sprawdzania uprawnień przechodzi do czynności 6.
6. Jeśli wartość USEADPAUT jest równa *YES, system określa, czy na stosie oczekuje więcej programów. Jeśli tak, proces sprawdzania uprawnień przechodzi do czynności 7. Jeśli nie, proces przechodzi do czynności 8.
7. Test za pomocą następnego programu ze stosu i powrót do czynności 2.
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 czynności 9.
9. System sprawdza uprawnienia prywatne. Ten proces jest opisany w sekcji Schemat blokowy 8B: Sprawdzanie uprawnień adoptowanych za pomocą uprawnień prywatnych.



Rysunek 19. 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 czynności 2. Jeśli nie, przechodzi do czynności 7.
2. System określa, czy obiekt ma uprawnienia prywatne. Jeśli tak, przechodzi do czynności 3. Jeśli nie, przechodzi do czynności 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 czynności 7. Jeśli nie odnaleziono żadnych uprawnień, przechodzi do czynności 4.
4. System sprawdza, czy obiekt jest chroniony przez listę autoryzacji. Jeśli tak, przechodzi do czynności 5. Jeśli nie, przechodzi do czynności 7.
5. System ustawia obiekt na listę autoryzacji i przechodzi do czynności 6.
6. System sprawdza uprawnienia właściciela do listy autoryzacji. (Patrz Schemat blokowy 4). Jeśli nie zostaną odnalezione żadne uprawnienia, wraca do czynności 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 czynności 8. Jeśli jest równa *NO, żądanie dostępu jest odrzucane.
8. System sprawdza, czy na stosie znajduje się więcej programów. Jeśli tak, przechodzi do czynności 9. Jeśli nie, żądanie dostępu jest odrzucane.
9. System ustawia obiekt na obiekt początkowy i przechodzi do czynności 10.
10. Test za pomocą następnego programu ze stosu i powrót do czynności 1.

Pojęcia pokrewne

"Ignorowanie uprawnień adoptowanych" na stronie 240
Technika użycia uprawnień adoptowanych w projekcie menu wymaga, aby przed uruchomieniem zapytań użytkownik powrócił do menu początkowego. Jeśli ma być zapewniona wygoda uruchamiania zapytań z menu aplikacji, a także z menu początkowego, można tak ustawić program QRYSTART, aby ignorował uprawnienia adoptowane.

Przykłady sprawdzania uprawnień

W sekcji przedstawiono kilka przykładów sprawdzania uprawnień.

Te przykłady demonstrują kroki podejmowane przez system w celu ustalenia, czy użytkownik może uzyskać dostęp do żądanego obiektu. Przykłady te ilustrują sposób działania procesu sprawdzania uprawnień oraz możliwe problemy z wydajnością systemu z nim związane.

Rys. 20 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 powtarzana 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 chroniony listą autoryzacji. . . . . . . . . . . . . :   *NONE

                       Uprawnienia
Użytkownik  Grupa      do obiektu
OWNCP                  *ALL
DPTSM                  *CHANGE
DPTMG                  *CHANGE
WILSONJ                *USE
*PUBLIC                *USE
```

Rysunek 20. Uprawnienia do zbioru PRICES

Przypadek 1: Używanie prywatnych uprawnień grupowych

W tym przypadku jest pokazany sposób korzystania z 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.)

Wynik:

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

W tym przypadku zademonstrowano sposób użycia 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. 21 na stronie 193 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 chroniony przez listę autoryzacji. . . . . . . . . . . :   *NONE

                       Obiekt
Użytkownik  Grupa      do obiektu
OWNAR                  *ALL
DPTAR                  *CHANGE
*PUBLIC                *USE
```

Rysunek 21. Uprawnienia do zbioru CREDIT

Aby określić, czy użytkownik ANDERSJ może uzyskać dostęp do zbioru CREDIT z wykorzystaniem uprawnień *CHANGE, system wykonuje następujące czynności:

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. Użytkownik DPTAR nie jest właścicielem zbioru CREDIT. Powrót do schematu blokowego 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.

Wynik:

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.

Pojęcia pokrewne

“Uwagi dotyczące grup podstawowych obiektów” na stronie 247
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.

Przypadek 3: Używanie uprawnień publicznych

Ten przypadek opisuje kroki związane z używaniem 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:

Schemat blokowy 1, krok 1.

1. Schemat blokowy 2, krok 1. Zbiór CREDIT nie ma uprawnień prywatnych. Uprawnienia profilu DPTAR są uprawnieniami grupy podstawowej, a nie uprawnieniami prywatnymi.
2. Schemat blokowy 2, kroki 2 i 3. Uprawnienia właściciela (OWNAR) są wystarczające.
3. Schemat blokowy 2, kroki 4 i 5. Uprawnienia grupy podstawowej (DPTAR) są wystarczające.
4. 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 wyszukiwania uprawnień prywatnych

Ten przypadek opisuje sposób użycia uprawnień publicznych bez wyszukiwania 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:

Przykład ten ilustruje zysk wydajności w przypadku uniknięcia zdefiniowania dla obiektu uprawnień prywatnych mniejszych 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

Ten przypadek pokazuje korzystny wpływ na wydajność używania 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 191.

- Jeśli przypadek 1 zmienić tak, aby profil grupowy DPTSM był właścicielem zbioru PRICES i posiadał dla niego uprawnienia *ALL, charakterystyka wydajności w obu przypadkach byłaby taka sama. Jednak posiadanie profilu grupowego będącego właścicielem obiektów aplikacji może oznaczać 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 DPTSM jest pierwszą grupą dla profilu SMITHG (określone w parametrze GRPPRF profilu użytkownika SMITHG), to charakterystyka wydajności jest taka sama jak w przypadku 5.

Przypadek 6: Użytkownik i uprawnienia grupowe

Poniższy przypadek udowadnia, że system może odmówić użytkownikowi dostępu do obiektu, mimo że grupa użytkownika ma wystarczające uprawnienia.

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. Niewystarczające uprawnienia, powrót do schematu 1.
3. Schemat blokowy 1, krok 6.
   a. Schemat blokowy 8A, krok 1. Sprawdzany obiekt = CONTRACTS/PRICES *FILE.
   b. Schemat blokowy 8A, krok 2. Program CPPGM01 nie adoptuje uprawnienia.
   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 uprawnienia.
      2) Schemat blokowy, krok 7. Parametr *USEADPAUT dla programu CPPGM01 ma wartość *NO. Dostęp jest odmawiany.

Analiza:

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. Jeśli jednak użytkownik WILSONJ miał uprawnienia *EXCLUDE (mniejsze niż publiczne), istnieje możliwość utraty zysku wydajności przedstawionego 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

W tym przypadku jest zademonstrowana przewaga, jaką zapewnia pod względem wydajności korzystanie z uprawnień publicznych w stosunku do korzystania z uprawnień prywatnych.

Informacje o uprawnieniach dla zbioru ITEM wyglądają następująco:

```
                          Wyśw. uprawnień dla obiektu

Obiekt . . . . . :   ITEM      Właściciel . . . . . :   OWNIC
  Biblioteka . . . :   ITEMLIB         Grupa podstawowa . . :   *NONE
Typ obiektu  . . . :   *FILE           Urządzenie ASP . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji .. . . . . :   *NONE

                       Obiekt
Użytkownik  Grupa      do obiektu
OWNIC                  *ALL
*PUBLIC                *USE
```

Rysunek 22. 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:

Schemat blokowy 1, krok 1.

1. Schemat blokowy 2, kroki 1, 2 i 3. Uprawnienia właściciela OWNIC są wystarczające.
2. Schemat blokowy 2, krok 4. Zbiór ITEM nie ma grupy podstawowej.
3. 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 przypadku przedstawiono korzyści wynikające z używania uprawnień adoptowanych 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 oraz 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. Zautoryzowano. 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.

Przypadek 9: Używanie listy autoryzacji

W tym przypadku zademonstrowano korzyści płynące z używania list autoryzacji.

Zbiór ARWKR01 z biblioteki CUSTLIB jest chroniony przez listę autoryzacji ARLST1. Rys. 23 i Rys. 24 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

                       Obiekt
Użytkownik  Grupa      do obiektu
OWNCP                  *ALL
*PUBLIC                *USE
```

Rysunek 23. 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 24. 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) 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.

Jeśli AMESJ byłby podzbiorem profilu grupowego, spowoduje to dodanie kilku kroków do tego przykładu, ale nie spowoduje dodatkowego wyszukiwania uprawnień prywatnych tak długo, jak dla zbioru ARWRK01 nie ma zdefiniowanych uprawnień prywatnych. Problemy z wydajnością mogą wystąpić, gdy używana jest kombinacja uprawnień prywatnych, list autoryzacji i profili grupowych, tak jak w “Przypadek 11: Łączenie metod autoryzacji” na stronie 200.

Przypadek 10: Używanie wielu grup

Zamieszczono tu przykład użycia 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. 25 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 chroniony przez listę autoryzacji. . . . . . . . . . . :   *NONE

                       Obiekt
Użytkownik  Grupa      do obiektu
OWNAR                  *ALL
DPTAR                  *CHANGE
DPTSM                  *USE
*PUBLIC                *EXCLUDE
```

Rysunek 25. 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 schematu blokowego 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 autoryzacji

W tym przypadku przedstawiono niepoprawny projekt uprawnień.

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. 26 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

                       Obiekt
Użytkownik  Grupa      do obiektu
OWNAR                  *ALL
DPTSM                  *USE
WILSONJ                *EXCLUDE
*PUBLIC                *USE
```

Rysunek 26. Uprawnienia do zbioru CRLIMWRK

Zbiór CRLIMWRK jest chroniony przez listę autoryzacji CRLST1. Rys. 27 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      do obiektów listą
OWNAR                  *ALL        X
DPTAR                  *ALL
*PUBLIC                *EXCLUDE
```

Rysunek 27. 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 wyszukiwanie 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 wyszukiwanie 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 schematu blokowego 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 wyszukiwanie uprawnień prywatnych**). Profil DPTSM ma uprawnienia *USE do zbioru CRLIMWRK, które nie są wystarczające.

e. Schemat blokowy 6, kontynuowany 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 schematu blokowego 6 bez odnalezienia uprawnień.

i. Schemat blokowy 6, krok 4. DPT702 nie jest podstawową grupą dla zbioru CRLIMWRK.

j. Schemat blokowy 6, krok 6 (**czwarte wyszukiwanie 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 wyszukiwanie 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 schematu blokowego 6 bez odnalezienia uprawnień.

q. Schemat blokowy 6, kroki 4 i 6. (**szóste wyszukiwanie 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.

Wynik:

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 wyszukiwane są 6 razy, co może spowodować problemy 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 sekwencji profili grupowych użytkownika WAGNERB spowoduje zmianę charakterystyki wydajności tego przykładu. Załóżmy, że DPTAR jest pierwszym profilem grupowym (GRPPRF) użytkownika WAGNERB. System wyszukuje uprawnienia prywatne 3 razy przed odnalezieniem uprawnień grupy podstawowej DPTAR na liście autoryzacji.

- 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

System tworzy pamięć podręczną uprawnień dla użytkowników w celu udostępnienia elastyczności i rozszerzonej wydajności.

Od wersji 3, wydania 7, system tworzy pamięć podręczną uprawnień dla użytkownika w momencie, gdy ten po raz pierwszy uzyskuje dostęp do obiektu. 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. Bezpieczeństwo i zarządzanie pracą

W sekcji omówiono zagadnienia związane z zarządzaniem pracą w systemie.

W niniejszej sekcji opisano poniżej przedstawione zagadnienia.

Informacje pokrewne

Zarządzanie pracą

Inicjowanie zadania

Podczas uruchamiania zadania system sprawdza uprawnienia do niektórych obiektów.

Gdy w systemie uruchamiane jest zadanie, przypisywane są do niego obiekty, takie jak kolejka wyjściowa, opis zadania oraz biblioteki z listy bibliotek. Uprawnienia do niektórych z tych obiektów są sprawdzane, zanim zadanie zostanie uruchomione, zaś do innych obiektów po jego uruchomieniu. Niewystarczające uprawnienia mogą spowodować błędy prowadzące do przerwania zadania.

Obiekty będące częściami struktury zadań dla zadania mogą być określone w opisie zadania, profilu użytkownika i w komendzie Wprowadzenie zadania (Submit Job - SBMJOB), w przypadku zadania wsadowego.

Uruchamianie zadania interaktywnego

W temacie znajduje się opis działań związanych z bezpieczeństwem podejmowanych 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. Szczegółowe informacje zawiera sekcja “Stacje robocze” na stronie 207.
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 jest przeprowadzane dla programu procesora QCMD, biblioteki programu i wszystkich używanych obiektów, tak jak opisano w czynności 1.
   b. Sprawdzane są uprawnienia użytkownika do programu obsługi klawisza ATTN. Jeśli uprawnienia są niewystarczające, do użytkownika jest wysyłany komunikat zapisywany również jako 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 jest wysyłany komunikat zapisywany również jako 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 jest wysyłany komunikat zapisywany również jako pozycja w protokole zadania. Zadanie zostaje zakończone.

Uruchamianie zadania wsadowego

W temacie przedstawiono opis działań związanych z bezpieczeństwem podejmowanych w momencie 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 bezpieczeństwa 40 lub 50, 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 i zadania wsadowe

Użytkownik może zmienić parametry zadania wsadowego, gdy jest ono uruchomione z uprawnieniem adoptowanym.

Po uruchomieniu nowego zadania tworzony jest dla niego nowy stos wywołań. Uprawnienie adoptowane nie zadziała, dopóki na stos wywołań nie zostanie dodany pierwszy program. Uprawnienia adoptowane nie mogą zostać wykorzystane do uzyskania dostępu do jakichkolwiek obiektów, takich jak kolejka wyjściowa lub opis zadania, które

dodawane są do struktury zadania przed jego przekierowaniem. 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 oczekującego na uruchomienie. Uprawnienia wymagane do zmiany parametrów zadania opisano w sekcji Komendy zadań.

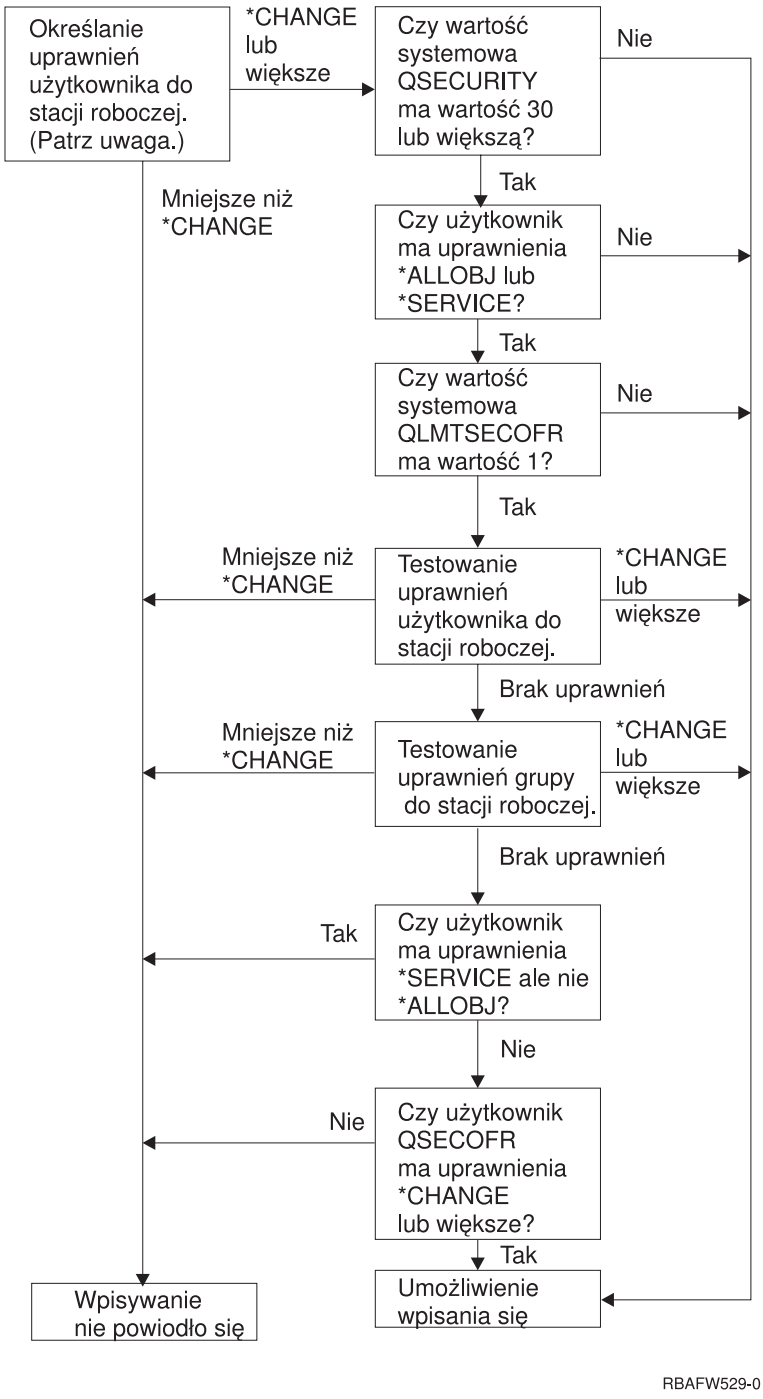
Stacje robocze

System sprawdza uprawnienia do stacji roboczej w momencie wpisywania się użytkownika.

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 osoby odpowiedzialnej za bezpieczeństwo) określa, czy użytkownicy z uprawnieniami specjalnymi *ALLOBJ lub *SERVICE muszą być autoryzowani do opisów urządzeń.

Rys. 28 na stronie 208 pokazuje logikę określania, czy użytkownik może wpisać się do urządzenia:



Rysunek 28. 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 znaleźć można przy użyciu następujących uprawnień:

- 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 jest przeprowadzane przed umieszczeniem programów na stosie wywołań 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 się zakończy się błędem. Jeśli uprawnienia są równe lub większe niż *CHANGE, system sprawdza, czy poziom ochrony w systemie to 30 lub więcej. Jeśli nie jest, użytkownik może wpisać się.

Jeśli poziom uprawnień to 30 lub więcej, system sprawdza, czy użytkownik posiada 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 grupa użytkownika 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 specjalne *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 osoby odpowiedzialnej za bezpieczeństwo (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 opisów urządzeń

Określenie prawa własności do opisów urządzeń umożliwia sterowanie uprawnieniami do urządzeń.

Domyślne uprawnienia publiczne dla komend CRTDEVxxx to *CHANGE. Urządzenia tworzone są w bibliotece QSYS, dostarczanej z wartością parametru CRTAUT ustawioną na *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.

Osoba odpowiedzialna za bezpieczeństwo (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 osobę odpowiedzialną za bezpieczeństwo, to jest ona 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 ograniczania wpisywania się osoby odpowiedzialnej za bezpieczeństwo 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.

Jeśli administrator systemu zmienia zbiór ekranowy wpisania się, musi pamiętać, aby podczas dodawania tekstu do tego zbioru nie zmieniać nazw pól ani długości buforów zbioru ekranowego. Zmiana nazw pól lub długości buforów może doprowadzić do błędów podczas wpisywania się.

Zmiana wyświetlanego ekranu wpisywania się

Użytkownik może zmienić kod źródłowy dla zbioru ekranowego wpisywania się, aby zmienić wyświetlany ekran.

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.

Źródło zbioru ekranowego ekranu wpisania

Aby utworzyć własny ekran wpisania, należy skopiować odpowiedni plik źródłowy.

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** przy każdej instalacji systemu operacyjnego i5/OS. 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.

Zmiana zbioru ekranowego wpisywania się

W tym temacie opisane są czynności, jakie należy wykonać w celu zmiany zbioru ekranowego wpisywania się.

Aby zmienić format ekranu wpisywania się, wykonaj następujące czynności:

1. Utwórz zmieniony zbiór ekranu wpisywania się.

   Pole ukryte UBUFFER w zbiorze ekranowym można zmienić, aby zarządzać mniejszymi polami. Pole UBUFFER ma 128 bajtów długości i jest ostatnim polem w zbiorze ekranowym. 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, aby zawierało dowolną wymaganą liczbę mniejszych pól, o ile 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 do aplikacji.
- 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 buforu wejściowego lub wyjściowego. Jeśli kolejność lub wielkość buforów zostanie zmieniona mogą wystąpić poważne błędy.
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, wykonaj następujące czynności:
   a. Użyj komendy Zmiana opisu podsystemu (Change Subsystem Description - CHGSBSD).
   b. Należy podać nowy zbiór ekranowy w parametrze SGNDSPF.
   c. Przed dokonaniem próby zmiany podsystemu sterującego należy użyć wersji testowej podsystemu, aby sprawdzić, czy ekran jest poprawny.
6. Przetestuj zmianę.
7. Zmień inne opisy podsystemów.

Uwagi:

1. Długość buforu dla zbioru ekranowego musi wynosić 318. 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. Prawa autorskie nie mogą zostać usunięte.

Opisy podsystemów

Opisy podsystemów pełnią różne funkcje w systemie.

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.

Pojęcia pokrewne

“Wpisywanie się bez identyfikatora użytkownika oraz hasła” na stronie 17
Ustawiony poziom bezpieczeństwa określa sposób kontrolowania przez system czynności wpisywania się bez identyfikatora użytkownika oraz hasła.

Sterowanie sposobem wejścia zadań do systemu

Za pomocą opisów podsystemu można sterować sposobem, w jaki zadania wchodzą do systemu.

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 poziomach ochrony 30 i wyższych, system protokołuje pozycję (typu AF, podtyp S) w kronice kontroli, jeśli dojdzie do próby domyślnego wpisania się i aktywna jest funkcja kontroli. Na poziomach ochrony 40 i wyższych, system nie zezwala na domyślne wpisywanie się nawet w przypadkach, gdy istnieje kombinacja pozycji stacji roboczej i opisu zadania, która na nie zezwala. Więcej informacji na ten temat zawiera sekcja “Wpisywanie się bez identyfikatora użytkownika oraz hasła” na stronie 17.

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 ryzyko naruszenia bezpieczeństwa. 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 220 omawia atrybuty sieciowe, które są ważne dla ochrony.

Opisy zadań

Opis zadania to wartościowe narzędzie bezpieczeństwa 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 “Sterowanie sposobem wejścia zadań do systemu” na stronie 211 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

Można określić uprawnienia w celu sterowania dostępem do kolejki komunikatów operatora systemu

Menu Asysta Operacyjna (ASSIST) systemu i5/OS 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. Administrator może uniemożliwić użytkownikom odpowiadanie na komunikaty w kolejce komunikatów QSYSOPR (operator systemu). 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 Komendy komunikatów). 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.

Ważne: 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 123 podsumowuje części listy bibliotek oraz ich budowanie podczas zadania. Przedstawione poniżej sekcje omawiają ryzyko oraz sposoby zabezpieczania list bibliotek.

Tabela 123. Części listy bibliotek. Lista bibliotek przeszukiwana jest w następującej kolejności:

Część	Zasada budowania
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.

Tabela 123. Części listy bibliotek (kontynuacja). Lista bibliotek przeszukiwana jest w następującej kolejności:

Część	Zasada budowania
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.

Pojęcia pokrewne

"Bezpieczeństwo biblioteki i listy bibliotek" na stronie 140
Gdy do listy bibliotek użytkownika dodawana jest biblioteka, uprawnienia, które użytkownik ma do biblioteki, przechowywane są razem z informacjami listy bibliotek.

"Planowanie bibliotek" na stronie 232
Biblioteka jest podobna do katalogu, w którym można przechowywać obiekty. Na sposób grupowania informacji aplikacji w biblioteki oraz na zarządzanie bibliotekami wpływ ma wiele czynników.

Ryzyko związane z bezpieczeństwem w przypadku list bibliotek

Niniejszy temat zawiera konkretne przykłady możliwych naruszeń bezpieczeństwa związanych z listami bibliotek oraz sposoby ich uniknięcia.

Listy bibliotek stanowią potencjalne ryzyko naruszenia bezpieczeństwa. Jeśli użytkownik może zmieniać sekwencję bibliotek na liście bibliotek, lub dodawać do niej nowe biblioteki, to możliwe jest, że będzie on miał możliwość wykonywania funkcji łamiących wymagania systemowe.

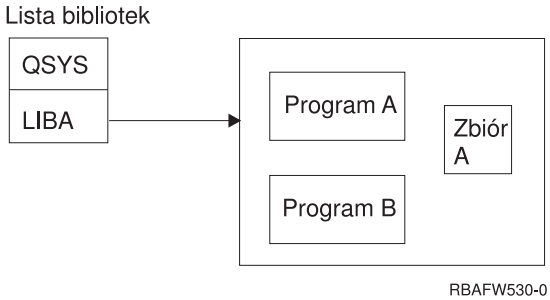
Sekcja "Bezpieczeństwo biblioteki i listy bibliotek" na stronie 140 udostępnia niektóre ogólne informacje dotyczące zagadnień związanych z listami bibliotek.

W sekcji znajdują się dwa przykłady zmiany listy bibliotek, które mogą spowodować złamanie wymogów bezpieczeństwa.

Zmiana w funkcji

w tym przykładzie przedstawiono możliwe ryzyko związane ze zmianą w funkcji podczas wywoływania programu w bibliotece.

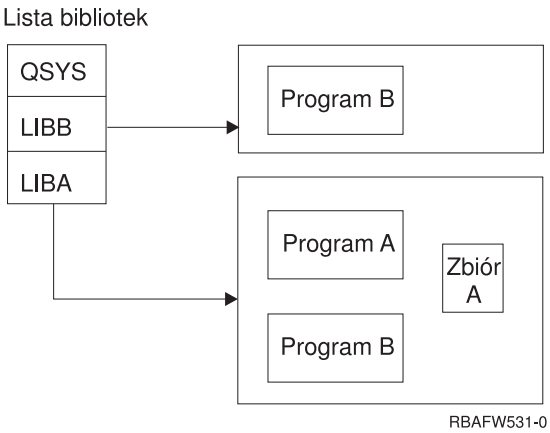
Rys. 29 pokazuje bibliotekę aplikacji. Program A wywołuje Program B, który znajduje się w bibliotece LIBA. Program B aktualizuje Zbiór A. Program B wywoływany jest bez nazwy kwalifikowanej, tak więc w celu jego odnalezienia przeszukiwana jest lista bibliotek.



Rysunek 29. Lista bibliotek–środowisko oczekiwane

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 30. Lista bibliotek–środowisko aktualne

Dostęp do informacji bez uprawnień

Przykład przedstawia potencjalne ryzyko dostępu bez uprawnień do informacji znajdujących się w bibliotece.

Przyjmijmy, że Program A z Rys. 29 na stronie 214 adoptuje uprawnienia użytkownika UŻYTKOWNIK_1, który ma uprawnienia *ALL do zbioru Zbiór A. Załóżmy też, że Program B jest wywoływany przez Program A (uprawnienia adoptowane wciąż działają). Doświadczony użytkownik może utworzyć zastępczy Program B, który po prostu wywoła procesor komend. Użytkownik uzyska wiersz komend i całkowity dostęp do zbioru A.

Zalecenia dotyczące części systemowej listy bibliotek

Podano tu zalecenia dotyczące systemowej części 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 “Zmiana listy bibliotek systemowych” na stronie 234.

Zalecenia dotyczące biblioteki produktu

W tym temacie podano zalecenia dotyczące ochrony biblioteki produktu.

Część biblioteki produktu listy bibliotek przeszukiwana jest przed częścią użytkownika. Doświadczony użytkownik może utworzyć komendę lub menu umieszczające bibliotekę produktu na liście 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 dotyczące biblioteki bieżącej

W tym temacie podano zalecenia dotyczące zapewniania bezpieczeństwa systemu podczas korzystania z 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 “Sterowanie listą bibliotek użytkownika” na stronie 234.

Zalecenia dotyczące części listy bibliotek odnoszącej się do użytkownika

W tym temacie podano zalecenia dotyczące sterowania tą częścią listy bibliotek, która odnosi się do użytkowników.

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.

Oto niektóre możliwości kontroli części użytkownika listy bibliotek w celu upewnienia się, że nieautoryzowane biblioteki z programami i zbiorami zastępczymi nie będą wykorzystywane 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 235 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 listy bibliotek dotyczącej użytkowników. 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 danej aplikacji. Gdy aplikacja zakończy swoje działanie, należy przywrócić ustawienie początkowe listy bibliotek. Przykład użycia tej techniki zawiera sekcja “Sterowanie listą bibliotek użytkownika” na stronie 234.

Drukowanie

Można kontrolować bezpieczeństwo kolejek wyjściowych w systemie.

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. W temacie Advanced Function Presentation znajdują się przykłady kierowania danych wyjściowych do konkretnej kolejki wyjściowej.

Zabezpieczanie zbiorów buforowych

Można określić kilka parametrów w celu kontroli bezpieczeństwa zbioru buforowego.

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. Istnieje możliwość manipulacji zbiorami buforowymi samemu, niezależnie od sposobu, w jaki zdefiniowane są uprawnienia dla 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).

Ważne: 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 Wyświetlanie danych (Display Data - DSPDTA) kolejki wyjściowej

Określenie parametru Wyświetlanie danych (DSPDTA) pozwoli na ochronę zawartości zbioru buforowego.

Parametr DSPDTA określa uprawnienie, które jest wymagane do wykonania następujących czynności na zbiorach buforowych należących do innych użytkowników.

- 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).

Dozwolone wartości dla DSPDTA	
***NO**	Użytkownik nie może wyświetlać, wysyłać ani kopiować zbiorów buforowych należących do innych użytkowników, chyba że posiada on jedno z następujących uprawnień: • 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 Uprawnienia do sprawdzania (Authority to Check - AUTCHK) umożliwia sterowanie uprawnieniami użytkownika do zmiany lub usuwania zbioru buforowego z systemu.

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 Sterowane przez operatora (Operator Control - 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.

Możliwe wartości parametru OPRCTL	
***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

Ta sekcja zawiera informacje uzupełniające dotyczące parametrów kolejki wyjściowej i uprawnień wymaganych do wykonywania funkcji zarządzania drukowaniem.

Tabela 124 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 513.

Uprawnienia oraz parametry kolejki wyjściowej dla wszystkich komend związanych ze zbiorami buforowymi zostały opisane w sekcji “Komendy zbioru buforowego” na stronie 497. Komendy kolejki wyjściowej zostały opisane w sekcji “Komendy kolejek wyjściowych” na stronie 469.

Ważne: Użytkownik posiadający uprawnienia specjalne *SPLCTL (kontrola buforu) nie podlega ograniczeniom uprawnień związanym z kolejkami wyjściowymi. Uprawnienia specjalne *SPLCTL umożliwiają użytkownikowi wykonywanie wszystkich operacji na wszystkich kolejkach wyjściowych. Podczas przydzielania uprawnień specjalnych *SPLCTL dowolnemu użytkownikowi należy kierować się ostrożnością.

Tabela 124. Uprawnienia wymagane do wykonywania funkcji drukowania

Funkcja drukowania	**Parametry kolejki wyjściowej**			**Uprawnienie kolejki wyjściowej**	**Uprawnienia specjalne**
	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 (DSPSPLF, CPYSPLF, SNDNETSPLF, SNDTCPSP[2])	*YES			*READ	Brak
	*NO	*DTAAUT		*READ, *ADD, *DLT	Brak
	*NO	*OWNER		Właściciel [3]	Brak
	*YES		*YES		*JOBCTL
	*NO		*YES		*JOBCTL
	*OWNER				
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 (CHGOUTQ, CLROUTQ, HLDOUTQ, RLSOUTQ[2])		*DTAAUT		*READ, *ADD, *DLT	Brak
		*OWNER		Właściciel [3]	Brak
			*YES		*JOBCTL
Start programu piszącego dla kolejki (STRPRTWTR, STRRMTWTR[2])		*DTAAUT		*CHANGE	Brak
			*YES		*JOBCTL

Tabela 124. Uprawnienia wymagane do wykonywania funkcji drukowania (kontynuacja)

Funkcja drukowania	Parametry kolejki wyjściowej			Uprawnienie kolejki wyjściowej	Uprawnienia specjalne
	DSPDTA	AUTCHK	OPRCTL		
[1] Jest to uprawnienie wymagane do kierowania wydruków do kolejki wyjściowej.					
[2] Należy skorzystać z tych komend lub ich równoważnych opcji z ekranu.					
[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

Niniejsze przykłady pokazują sposób ustawiania parametrów bezpieczeństwa kolejek wyjściowych, w celu spełnienia różnorodnych potrzeb.

- 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),
- Żądanie dostępu klienta (PCSACC)
- Żądanie dostępu 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.

Informacje pokrewne

SNA Distribution Services

Atrybut sieciowy Żądanie dostępu klienta (Client Request Access - PCSACC)

Atrybut sieciowy PCSACC określa sposób przetwarzania przez program licencjonowany System i 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 znajdujących się na platformie System i, ale nie kontroluje, czy komputer osobisty może korzystać z funkcji emulowania stacji roboczej.

Uwaga: Atrybut sieciowy PCSACC kontroluje jedynie klientów DOS i OS/2. Ten atrybut nie ma wpływu na innych klientów System i Access.

Możliwe wartości parametru PCSACC:	
***REJECT**	Program System i Access odrzuca każde żądanie z komputera osobistego dotyczące dostępu do obiektów na platformie System i. Do aplikacji PC wysyłany jest komunikat o błędzie.
***OBJAUT**	Programy System i Access w systemie sprawdzają zwykłe uprawnienia do obiektu dla każdego obiektu zażądanego przez program komputera 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.

Możliwe wartości parametru PCSACC:	
kwalifikowana- nazwa- programu	Program System i 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 System i 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.

Czynniki ryzyka i zalecenia

Instrukcje podane w tym temacie dotyczą ochrony zbiorów w systemie.

Zwykłe zabezpieczenia okazać się niewystarczające w sytuacji, gdy w systemie zainstalowano program System i Access. Jeśli np. użytkownik ma uprawnienia *USE do zbioru, a atrybut sieciowy PCSACC ma wartość *OBJAUT, to użytkownik może skorzystać z programu System i Access i programu na komputerze PC, aby przenieść cały ten zbiór na komputer PC. Następnie może skopiować dane na dyskietkę lub taśmę i usunąć je lokalnie.

Istnieje kilka metod ochrony przed kopiowaniem zbioru przez użytkownika systemu System i z uprawnieniem *USE do tego zbioru:

- ustawienie parametru LMTCPB(*YES) w profilu użytkownika,
- ograniczanie uprawnień do komend, które kopiują zbiory,
- ograniczenie uprawnień do komend używanych przez program System i 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.

Powyższe metody są nieskuteczne w przypadku użytkownika komputera PC posługującego się programem licencjonowanym System i Access. Jedynym odpowiednim środkiem ochrony jest używanie programu obsługi wyjścia sprawdzającego wszystkie żądania.

Program System i Access przekazuje do programu użytkownika obsługi wyjścia wywoływanego przez atrybut sieciowy PCSACC informacje o następujących typach dostępu:

- przesyłanie zbioru,
- drukowanie wirtualne,
- komunikat,
- folder współużytkowany.

Informacje pokrewne

Programowanie: iSeries Access

Atrybut sieciowy Żądanie dostępu DDM (DDM Request Access - DDMACC)

Atrybut sieciowy Żądanie dostępu DDM (DDM Request Access - DDMACC) określa sposób, w jaki procesy systemowe żądają dostępu do danych od innych systemów przy użyciu funkcji zarządzania danymi rozproszonymi (DDM) lub funkcji rozproszonej relacyjnej bazy danych.

Dozwolone wartości 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.

Dozwolone wartości DDMACC:	
***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.

Informacje pokrewne

Uwagi dotyczące parametru DDMACC

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. Z tego powodu typowy programista może utworzyć kopię taśmową najbardziej wartościowych programów.

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

Ograniczając operacje składowania i odtwarzania można zapewnić systemowi ochronę.

Użytkownik może kontrolować możliwość składowania i odtwarzania obiektów na kilka sposobów:

- przez ograniczenie dostępu do urządzeń składowania i odtwarzania, takich jak jednostki taśm i jednostki optyczne,
- 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

W temacie przedstawiono przykład ograniczenia komend składowania i odtwarzania.

Aby ograniczyć komendy składowania i odzyskiwania w systemie, należy wykonać następujące czynności:

1. Aby utworzyć listę autoryzacji, dzięki której można przydzielać uprawnienia dla komend operatorom systemu, należy wpisać poniższy przykład:

   ```
   CRTAUTL AUTL(SRLIST) TEXT('Lista składowania i odtwarzania')
   AUT(*EXCLUDE)
   ```

2. Aby wykorzystać listę autoryzacji w celu zabezpieczenia komend składowania, należy wpisać następujący przykład:

```
GRTOBJAUT OBJ(SAV*) OBJTYPE(*CMD) AUTL(SRLIST)
```

3. Aby upewnić się, że uprawnienia *PUBLIC pochodzą z listy autoryzacji, należy wpisać następujący przykład:

```
GRTOBJAUT OBJ(SAV*) OBJTYPE(*CMD) USER(*PUBLIC)
   AUT(*AUTL)
```

4. Aby wykorzystać listę autoryzacji w celu zabezpieczenia komend odtwarzania, należy wpisać następujący przykład:

```
GRTOBJAUT OBJ(RST*) OBJTYPE(*CMD) AUTL(SRLIST)
```

5. Aby upewnić się, że uprawnienia *PUBLIC pochodzą z listy autoryzacji, należy wpisać następujący przykład:

```
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: Warto rozważyć możliwość przydzielenia operatorom systemu wyłącznie uprawnień dla komend składowania. W takim przypadku należy zabezpieczyć komendy składowania i odtwarzania za pomocą oddzielnych list autoryzacji.

7. Aby ograniczyć funkcje API składowania i odtwarzania i zabezpieczyć je za pomocą listy autoryzacji, należy wprowadzić 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)
GRTOBJAUT OBJ(QSRRSTO) OBJTYPE(*PGM) AUTL(SRLIST)
GRTOBJAUT OBJ(QSRRSTO) OBJTYPE(*PGM) USER(*PUBLIC)
   AUT(*AUTL)
```

Strojenie wydajności

Monitorowanie oraz strojenie wydajności nie należy do obowiązków osoby odpowiedzialnej za bezpieczeństwo. Jednak osoba odpowiedzialna za bezpieczeństwo powinna 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 zadaniami) 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 zezwolić użytkownikom na wyświetlanie informacji o wydajności za pomocą komendy WRKSYSSTS, nie dając im jednocześnie możliwości na zmianę tych informacji, należy wykonać następujące czynności:

```
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, użytkownik może chociaż uruchomić niektóre raporty lub kompilacje programów w trybie wsadowym. Zadanie uruchomione w trybie wsadowym często wpływa na wydajność systemu mniej niż takie samo zadanie uruchomione interaktywnie.

Na przykład, aby ograniczyć komendę uruchamiającą RPTA programu w trybie wsadowym, 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 bezpieczeństwa

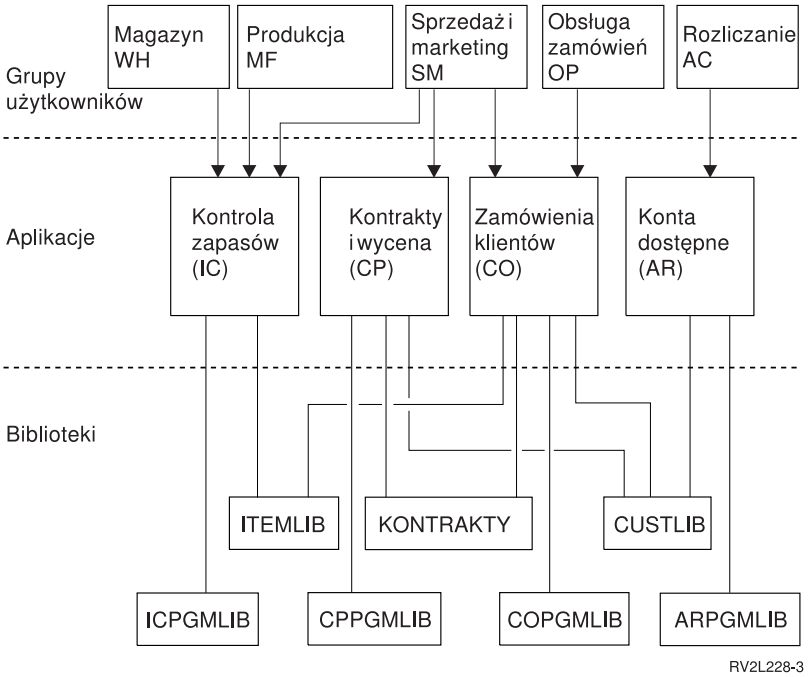
Niniejsza sekcja zawiera wskazówki, które pomagają włączyć bezpieczeństwo do całości projektów tworzonych przez programistów aplikacji i system managerów. Znajdują się tu również przykłady technik, które będą pomocne w osiąganiu celów bezpieczeństwa w administrowanym systemie.

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.

Niektóre przykłady w niniejszej sekcji zawierają programy przykładowe. 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.

Publikacja Planowanie i konfigurowanie bezpieczeństwa systemu Centrum informacyjnego jest przeznaczona dla administratorów bezpieczeństwa. Zawiera formularze, przykłady oraz wskazówki dotyczące planowania ochrony dla aplikacji, które już zostały napisane. Osoby odpowiedzialne za projektowanie aplikacji zachęcane są do przejrzenia szczegółowych informacji, formularzy i przykładówszczegółowych informacji zawartych w temacie Planowanie i konfiguracja bezpieczeństwa systemu.Mogą one pomóc spojrzeć na aplikację z perspektywy administratora ochrony oraz zrozumieć, jakie informacje należy udostępnić.

Temat Centrum informacyjnego pt. Planowanie i konfiguracja bezpieczeństwa systemu korzysta z zestawu przykładowych aplikacji dla fikcyjnego przedsiębiorstwa o nazwie Fabryka Zabawek JKL. Ta sekcja rozważa zagadnienia projektowe dla tego samego zestawu aplikacji przykładowych.Rys. 31 opisuje relacje pomiędzy grupami użytkowników, aplikacjami oraz bibliotekami Fabryki Zabawek JKL:



Rysunek 31. Aplikacje przykładowe

Opis rysunku

Obrazek ten ukazuje, w jaki sposób pięć zestawów grup użytkowników uzyskuje dostęp do aplikacji i bibliotek w systemie firmy JKL. Grupy użytkowników to: Magazyn, Produkcja, Sprzedaż i marketing, Obsługa zamówień oraz Księgowość. Niniejsze grupy użytkowników posiadają różne dostępy do różnych aplikacji, opisanych w liście.

- Grupy użytkowników Magazyn, Produkcja oraz Sprzedaż i marketing posiadają dostęp do aplikacji sterowania inwentarzem.
- Grupa użytkowników Sprzedaży i marketingu ma także dostęp do aplikacji Kontrakty i wycena oraz Zamówienia klientów.
- Grupa użytkowników Obsługa zamówień również ma dostęp do aplikacji Zamówienia klientów.
- Grupa użytkowników Księgowość ma dostęp wyłącznie do aplikacji Należności.

Informacje pokrewne

Scenariusze dla serwera HTTP

Ogólne zalecenia dotyczące projektowania ochrony

Utrzymywanie projektu ochrony tak prostego jak to tylko możliwe, ułatwia zarządzanie i kontrolę ochrony. Zwiększa także wydajność aplikacji oraz tworzenia kopii zapasowych.

Oto lista ogólnych zaleceń przy projektowaniu 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 korzystania z produktu takiego jak System i Access lub posiadania linii komunikacyjnych podłączonych do systemu nie należy polegać na ograniczaniu możliwości w profilu użytkownika i kontroli dostępu do menu. Należy użyć bezpieczeństwo zasobów, aby chronić wszystkie obiekty, które mają być niedostępne za pośrednictwem tych interfejsów.
- 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.

Pojęcia pokrewne

Rozdział 5, “Bezpieczeństwo zasobów”, na stronie 135
Ten rozdział zawiera opisy poszczególnych elementów bezpieczeństwa zasobów oraz opis ich działania. Wyjaśnia także, jak używać komend CL oraz ekranów do konfigurowania ochrony zasobów.

Planowanie zmian poziomu haseł

Zmiana poziomu haseł powinna być odpowiednio zaplanowana. Jeśli nie zaplanowano odpowiednio zmiany poziomu haseł, działania na innych systemach mogą nie powieść się, zaś użytkownicy mogą nie być w stanie wpisać się do systemu.

Przed zmianą wartości systemowej QPWDLVL, należy upewnić się, że dane bezpieczeństwa zostały zapisane za pomocą komendy SAVSECDTA lub SAVSYS. Jeśli dostępna jest aktualna kopia zapasowa, można zresetować hasła dla wszystkich profili użytkowników nawet, gdyby był konieczny powrót do niższego poziomu haseł.

Produkty wykorzystywane w systemie i na systemach klientów, z którymi system współpracuje, mogą nie pracować poprawnie z ustawieniami 2 i 3 wartości systemowej poziomu haseł (QPWDLVL). Każdy produkt lub klient, który wysyła hasła z ekranu wpisywania się do systemu w postaci zaszyfrowanej, a nie jawnego tekstu, musi zostać zaktualizowany, aby mógł pracować z regułami szyfrowania haseł dla QPWDLVL 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 algorytmu dla poziomu QPWDLVL 2 lub 3, nawet jeśli konkretne znaki są poprawne, nie będą akceptowane. Dotyczy to także dostępu do platformy System i z równorzędnej platformy System i z użyciem szyfrowania w celu uwierzytelnienia systemów.

Na problem składa się fakt, że niektóre produkty, których problem ten dotyczy (takie jak IBM Toolbox for Java) dostarczane są 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.

Dzięki temu i innym scenariuszom łatwo zauważyć, dlaczego przed ustawieniem wartości systemowej QPWDLVL ważne jest dokładne planowanie.

Uwagi dotyczące zmiany wartości QPWDLVL z 0 na 1

Poziom hasła 1 umożliwia systemowi, który nie musi komunikować się z produktem System i Support for Windows Network Neighborhood (NetServer), wyeliminowanie haseł produktu NetServer. 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.

Kwestie dotyczące zmiany QPWDLVL z 0 lub 1 na 2

Poziom hasła 2 wprowadza hasła z rozróżnianiem wielkich i małych liter, o długości do 128 znaków (zwane również frazami haseł), i zapewnia największe możliwości powrotu do QPWDLVL 0 lub 1.

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 QPWDLVL na 2 administrator systemu powinien znaleźć wszystkie profile użytkowników bez hasła użytecznego na poziome hasła 2, za pomocą komendy PRTUSRPRF TYPE(*PWDLVL). W zależności od odnalezionych profili administrator może wykorzystać jeden z poniższych mechanizmów, pozwalających na dodanie hasła poziomu 2 i 3 do profilu.

- Zmienić hasło profilu za pomocą komendy CHGUSRPRF lub CHGPWD, albo za pomocą funkcji API QSYCHGPW. Spowoduje to zmianę przez system hasła możliwego do użycia na poziomach hasła 0 i 1. System tworzy również dwa równoważne hasła rozróżniające wielkość znaków, których użyć można na poziomie hasła 2 i 3. Tworzone są wersje haseł w całości składające się z wielkich i małych znaków do użycia na poziomie hasła 2 lub 3.

  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 prawidłowe, a użytkownik nie posiada hasła możliwego do użycia na poziomach hasła 2 i 3, system tworzy dwa równoważne, rozróżniające wielkość znaków hasła, których można użyć na poziomach hasła 2 i 3. Tworzone są wersje haseł w całości składające się z wielkich i małych znaków do użycia na poziomie hasła 2 lub 3.

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 spełnia poniższe warunki, system sprawdza poprawność użytkownika pod względem hasła poziomu 0, a następnie tworzy dwa hasła poziomu 2 (zgodnie z wcześniejszym opisem) dla profilu użytkownika.

- Profil użytkownika nie ma hasła nadającego się do użytku na poziomie 2 lub 3.
- Profil użytkownika ma hasło nadające się do użytku na poziomie 0 lub 1.
- Użytkownik wpisuje się poprzez produkt, który wysyła hasła jawnym tekstem.

Dalsze próby wpisania się będą sprawdzane z użyciem haseł poziomu 2.

Klienty korzystające z podstawiania haseł nie będą pracować poprawnie z QPWDLVL 2, jeśli nie nie zostały zaktualizowane do nowej metody podstawiania hasła (frazy hasła). Administrator powinien sprawdzić, czy wymagane jest korzystanie z klienta, który nie został zaktualizowany do nowej metody podstawiania haseł.

Klienty korzystające z podstawiania haseł to:

- TELNET
- System iDostęp (Access)
- System i Host Servers
- QFileSrv.400
- obsługa System i NetServer Print
- DDM
- DRDA
- SNA LU6.2

Przed zmianą poziomu haseł na QPWDLVL 2 zaleca się zeskładowanie danych bezpieczeństwa. Ułatwi to późniejsze przejście do poziomu QPWDLVL 0 lub 1, jeśli będzie to konieczne.

| Należy unikać zmiany wartości systemowych haseł, takich jak QPWDMINLEN, QPWDMAXLEN i QPWDRULES,
| przed przetestowaneim QPWDLVL 2. Dzięki temu w razie potrzeby będzie łatwiej powrócić do QPWLVL 1 lub 2.
| Wartość systemowa QPWDVLDPGM musi określić *REGFAC lub *NONE, zanim system zezwoli na zmianę
| QPWDLVL na 2. W przypadku korzystania z programu sprawdzającego poprawność haseł warto napisać nowy taki
| program, który można zarejestrować do punktu wyjścia QIBM_QSY_VLD_PASSWRD za pomocą komendy
| ADDEXITPGM.

Hasła NetServer są wciąż obsługiwane na poziomie QPWDLVL 2, więc dowolne funkcje/usługi wymagające hasła NetServer powinny wciąż poprawnie działać.

Gdy system jest gotowy do pracy z QPWDLVL 2, można zmienić wartości systemowe haseł tak, aby korzystały z dłuższych haseł. Należy jednak pamiętać, że dłuższe hasła przynoszą następujące efekty:

- Jeśli podane zostanie hasło dłuższe niż 10 znaków, hasła na poziomach 0 i 1 zostaną usunięte. Ten profil użytkownika nie będzie w stanie się wpisać do systemu, jeśli system powróci do poziomu 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 haseł dotyczą tylko nowej wartości poziomu hasła 2 i nie dotyczą haseł poziomu 0 i 1 wygenerowanych przez system, ani też wartości haseł NetServer (jeśli zostały utworzone).

Kwestie dotyczące zmiany QPWDLVL z 2 na 3

Jeśli system od pewnego czasu działa na poziomie QPWDLVL 2, można rozważyć przejście 2 na QPWDLVL 3, co pozwoli na maksymalizację poziomu zabezpieczenia hasłem.

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 znaleźć profile użytkowników bez przypisanych haseł poziomu 2 lub 3 za pomocą komend DSPAUTUSR lub PRTUSRPRF.

Zmiana wartości systemowej QPWDLVL na niższy poziom hasła

Mimo iż powrót do niższej wartości QPWDLVL jest możliwy, z założenia jest on utrudniony. W zasadzie należy przyjąć, że zwiększenie wartości QPWDLVL jest nieodwracalne. Mogą jednak wystąpić przypadki, w których konieczne będzie przywrócenie niższej wartości QPWDLVL.

Uwagi dotyczące zmiany wartości QPWDLVL z 3 na 2

Zmiana ta jest względnie łatwa. Po ustawieniu wartości QPWDLVL na 2, administrator musi określić, czy któreś z profili użytkowników muszą zawierać hasła NetServer lub hasła poziomu 0 lub 1 oraz, w razie potrzeby, zmienić hasła tych profili na dopuszczalną wartość.

Ponadto, konieczna może być zmiana wartości systemowych haseł na wartości zgodne z NetServer i hasła poziomu 0 lub 1, jeżeli takie są wymagane.

Uwagi dotyczące zmiany wartości 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 QPWDLVL z 2 na 1

Przed ustawieniem wartości QPWDLVL na 1 należy użyć komendy DSPAUTUSR lub PRTUSRPRF TYPE(*PWDINFO) w celu zlokalizowania profili użytkowników nie posiadających haseł poziomu 0 lub 1. Jeśli profil użytkownika wymaga hasła po zmianie wartości QPWDLVL, należy sprawdzić, czy dla profilu utworzone zostanie hasło poziomu 0 i 1 za pomocą jednej z następujących metod:

- 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 spełnione są następujące warunki:
  - Długość hasła wynosi co najwyżej 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 od znaku podkreślenia.

  Na przykład zmiana hasła na RainyDay spowoduje wygenerowanie hasła RAINYDAY dla poziomów 0 i 1. Jednak zmiana wartości hasła na Rainy Days in April może spowodować usunięcie hasła poziomu 0 i 1 (ponieważ hasło jest za długie i zawiera odstępy).

  Jeśli hasło poziomu 0 lub 1 nie może zostać utworzony, nie jest wyświetlany żaden komunikat ani wskaźnik,
- 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 QPWDLVL z 2 na 0

Uwagi te są takie same jak w przypadku zmiany wartości QPWDLVL z 2 na 1, z tą różnicą, że hasła NetServer są zachowane podczas wprowadzania zmiany.

Uwagi dotyczące zmiany wartości QPWDLVL z 1 na 0

Po zmianie wartości QPWDLVL na 0, należy użyć komendy DSPAUTUSR lub PRTUSRPRF w celu zlokalizowania profili użytkowników nie posiadających 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 można zmienić poziom QPWDLVL na 0.

Planowanie bibliotek

Biblioteka jest podobna do katalogu, w którym można przechowywać obiekty. Na sposób grupowania informacji aplikacji w biblioteki oraz na zarządzanie bibliotekami wpływ ma wiele czynników.

Ochrona biblioteki jest efektywna pod warunkiem przestrzegania następujących reguł:

- 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.

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.

Uprawnienia *USE do biblioteki umożliwiają użytkownikowi znajdowanie 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.

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.

Oto dwa przykłady wykorzystania ochrony bibliotek dla aplikacji firmy JKL Toy Company. (Rys. 31 na stronie 227 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 zapytania SQL. Biblioteki zawierające 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.

Pojęcia pokrewne

“Bezpieczeństwo biblioteki” na stronie 139
Zabezpieczenia biblioteki mogą służyć do ochrony informacji.

Odsyłacze pokrewne

“Listy bibliotek” na stronie 213
Lista bibliotek dla zadania wskazuje, które biblioteki mają być przeszukiwane, oraz kolejność, w jakiej mają być przeszukiwane.

Informacje pokrewne

Scenariusze dla serwera HTTP

Planowanie aplikacji pod kątem zapobiegania powstawaniu dużych profili

Ponieważ duże profile mają niekorzystny wpływ na wydajność i bezpieczeństwo systemu, należy tak planować aplikacje, aby unikać ich powstawania.

Ze względu na możliwy wpływ na wydajność i ochronę, należy wykonać następujące czynności w celu zapobiegnięcia przepełnieniu 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 będące własnością profili użytkowników IBM mogą również mieć wpływ na wydajność komend takich jak 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. W profilu właściciela obiektu listy autoryzacji spowodują utworzenie jednej pozycji uprawnień do obiektu dla każdego użytkownika, któremu przyznano uprawnienia do listy autoryzacji.

Listy bibliotek

Lista bibliotek dla zadania zapewnia elastyczność, chociaż niesie ze sobą również ryzyko naruszenia bezpieczeństwa. 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.

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.

Wymagania innych aplikacji mogą uniemożliwić wykorzystanie nazw kwalifikowanych. Jeśli aplikacja korzysta z list bibliotek, ryzyko naruszenia ochrony można zmniejszyć, stosując techniki opisane w następnej sekcji.

Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki określone w sekcji Rozdział 10, “Licencja na kod oraz Informacje dotyczące kodu”, na stronie 317.

Sterowanie listą bibliotek użytkownika

W celu lepszej ochrony, warto jest upewnić się przed uruchomieniem zadania, że część listy bibliotek należąca do użytkowników posiada odpowiednie pozycje w oczekiwanej kolejności. Jedną z metod jest użycie programu CL do zeskładowania listy bibliotek użytkownika, zastąpienie jej listą wymaganą, a następnie odtworzenie listy po zakończeniu działania aplikacji.

Poniżej przedstawiono program wykonujący tę czynność:

Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki zapisane w sekcji Rozdział 10, “Licencja na kod oraz Informacje dotyczące kodu”, na stronie 317.

```
          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 32. Program zastępujący i odtwarzający listę bibliotek

Uwagi:

1. Niezależnie od tego, jak program zakończy swoje działanie (normalnie lub niepoprawnie), lista bibliotek jest przywracana do wersji sprzed wywołania programu. Dzieje się tak dlatego, obsługa błędów zawiera odtwarzanie listy bibliotek.
2. Ponieważ komenda CHGLIBL wymaga listy nazw bibliotek, nie może być uruchomiona bezpośrednio. Dlatego komenda RTVJOBA wczytuje biblioteki używane do utworzenia komendy CHGLIBL jako zmienną. Zmienna przekazywana jest jako parametr do funkcji QCMDEXC.
3. Jeśli nastąpi wyjście do niekontrolowanej funkcji (np. program użytkownika, menu pozwalające na wprowadzanie komend lub ekran wprowadzania komend) w czasie trwania pracy programu, program powinien w czasie powrotu zastąpić listę bibliotek w celu zapewnienia odpowiedniej kontroli.

Zmiana listy bibliotek systemowych

W celu zabezpieczenia systemu może również zaistnieć potrzeba zmiany części systemowej listy bibliotek.

Jeśli aplikacja musi dodać pozycje do systemowej części listy bibliotek, można użyć programu CL podobnego do tego przedstawionego na Rys. 32, z następującymi zmianami:

- Zamiast komendy RTVJOBA aby pobrać wartość systemową QSYSLIBL, należy użyć komendy Odtworzenie wartości systemowej (Retrieve System Values - RTVSYSVAL).

- 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 domyślnie ma ustawione uprawnienia publiczne na wartość *EXCLUDE. Aby wykorzystać tę komendę w programie, należy wykonać jedną z następujących 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 bezpieczeństwa 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:

- Wszelkie funkcje aplikacji, które dodają obiekty do 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. 33 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 33. Format opisywania bezpieczeństwa 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 zapewnia wszystkie wymagane połączenia pomiędzy menu, tak, aby użytkownik nie musiał odwoływać się do wiersza poleceń w celu wywołania jednego z nich.
- 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 237,
- należy rozważyć kontrolowanie dostępu do menu żądania systemowego (Request) lub niektórych opcji tego menu;
- 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.

Na przykład 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 34. Przykładowe menu zapytania

Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki określone w sekcji Rozdział 10, “Licencja na kod oraz Informacje dotyczące kodu”, na stronie 317.

Odsyłacze pokrewne

“Ograniczenie możliwości” na stronie 85
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 narzędziem zabezpieczającym przed eksperymentowaniem przez użytkowników w systemie.

Informacje pokrewne

Scenariusze dla serwera HTTP

Opisywanie bezpieczeństwa menu

Projektanci aplikacji powinni przedstawić administratorom bezpieczeństwa informacje na temat menu. Dzięki tym informacjom administrator bezpieczeństwa może zadecydować o tym, kto powinien mieć dostęp do menu oraz jakie uprawnienia są potrzebne.

Poniżej znajdują się przykładowe informacje, których potrzebuje administrator bezpieczeństwa.

- 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. 35 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 dla obiektów: Użytkownik musi posiadać uprawnienia *USE dla programu QRYSTART. QRYUSR musi posiadać uprawnienia *USE dla bibliotek zawierających
zbiory, do których wysyłane jest zapytanie. Użytkownik, QRYUSR, lub wszyscy muszą posiadać uprawnienia *USE dla zbiorów, do których wysyłane jest zapytanie.

Rysunek 35. Format opisywania bezpieczeństwa menu

Używanie uprawnień adoptowanych w projekcie menu

Dostępność narzędzia do wspomagania podejmowania decyzji, takiego jak Query/400, stanowi wyzwanie przy projektowaniu ochrony. 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.

Na przykład chcemy zapewnić, aby użytkownicy mogli wyświetlać informacje w zbiorach za pomocą narzędzia zapytań, ale zbiory mają być modyfikowane tylko przez przetestowane programy użytkowe.

Uwaga: Sekcja “Obiekty adoptujące uprawnienia właściciela” na stronie 153 opisuje sposób działania uprawnień adoptowanych. Sekcja “Schemat blokowy 8: Jak są sprawdzane uprawnienia adoptowane” na stronie 187 opisuje proces wyszukiwania przez system uprawnień adoptowanych.

Rys. 36 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 36. 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. Oto przykład programu sterowania zasobami (ICSTART).

Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki zapisane w sekcji Rozdział 10, “Licencja na kod oraz Informacje dotyczące kodu”, na stronie 317.

```
PGM
ADDLIBLE ITEMLIB
ADDLIBLE ICPGMLIB
GO ICMENU
RMVLIBLE ITEMLIB
RMVLIBLE ICPGMLIB
ENDPGM
```

Rysunek 37. Przykładowy początkowy program użytkowy

Program uruchamiający program Query (QRYSTART) adoptuje uprawnienia profilu (QRYUSR) udostępnianego w celu umożliwienia dostępu do zbiorów za pomocą zapytań. Rys. 38 pokazuje program QRYSTART:

```
PGM
ADDLIBLE ITEMLIB
ADDLIBLE CUSTLIB
STRQRY
RMVLIBLE ITEMLIB
RMVLIBLE CUSTLIB
ENDPGM
```

Rysunek 38. Przykładowy program do tworzenia zapytań z uprawnieniami adoptowanymi

System menu korzysta z trzech typów profili użytkowników, które opisuje Tabela 125. Natomiast Tabela 126 opisuje obiekty używane przez system menu.

Tabela 125. 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 126. 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

Tabela 126. Obiekty używane przez system menu (kontynuacja)

Nazwa obiektu	Właściciel	Uprawnienia publiczne	Uprawnienia prywatne	Informacje dodatkowe
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		
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 wywołań. 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 197,
- 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 upewnić się, że menu nie daje dostępu do wiersza poleceń ani nie zezwala na niechciane funkcje usuwania i aktualizacji.
- 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.

Pojęcia pokrewne

“Planowanie ochrony zbiorów” na stronie 243
Informacje zawarte w zbiorach bazy danych są najczęściej najważniejszymi zasobami systemu. Ochrona zasobów umożliwia kontrolowanie, kto może przeglądać, zmieniać i usuwać informacje ze zbiorów.

Ignorowanie uprawnień adoptowanych

Technika użycia uprawnień adoptowanych w projekcie menu wymaga, aby przed uruchomieniem zapytań użytkownik powrócił do menu początkowego. Jeśli ma być zapewniona wygoda uruchamiania zapytań z menu aplikacji, a także z menu początkowego, można tak ustawić program QRYSTART, aby ignorował uprawnienia adoptowane.

Rys. 39 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 39. Przykładowe menu aplikacji z zapytaniem.

Informacje o uprawnieniach dla programu QRYSTART są takie same, jak to pokazuje Tabela 126 na stronie 238. Program tworzony jest z parametrem użycia uprawnień adoptowanych (USEADPAUT) ustawionym na *NO, aby ignorować uprawnienia adoptowane poprzednich programów ze stosu.

Poniżej znajdują się porównania stosów wywołań przy wyborze zapytanie z MENU1 przez użytkownika USERA (patrz Rys. 36 na stronie 237) oraz z ICMENU:

Stos wywołań dla zapytania wybranego z menu MENU1

- MENU1 (brak uprawnień adoptowanych)
- QRYSTART (uprawnienia adoptowane od QRYUSR)

Stos wywołań dla zapytania wybranego 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 USERA uruchamianie zapytania z menu ICMENU bez możliwości zmiany lub usuwania zbiorów. Dzieje się tak ponieważ uprawnienia właściciela OWNIC nie są używane przez program QRYSTART.

Kiedy użytkownik USERA 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. 34 na stronie 236) 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 wywołań.

Pojęcia pokrewne

“Programy ignorujące uprawnienie adoptowane” na stronie 156
Podanie parametru użycia uprawnień adoptowanych (USEADPAUT) umożliwia określenie, czy program będzie używał uprawnień adoptowanych.

Odsyłacze pokrewne

“Schemat blokowy 8: Jak są sprawdzane uprawnienia adoptowane” na stronie 187
Jeśli podczas sprawdzania uprawnień użytkownika uprawnienia będą niewystarczające, system sprawdza uprawnienia adoptowane.

Informacje pokrewne

Scenariusze dla serwera HTTP

Menu żądania systemowego

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. Może to stanowić ryzyko naruszenia bezpieczeństwa, ponieważ uprawnienia publiczne do menu żądania systemowego w dostarczanym systemie są ustawione na *USE.

Najprostszy sposób na uniemożliwienie użytkownikom uzyskania dostępu do tego menu to 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. Komendy kwalifikowane są nazwą biblioteki z komunikatu CPX2373. Wartości w komunikacie CPX2373 dla każdej komendy, to *NLVLIBL lub *SYSTEM. Ktoś mógłby wykorzystać komendę Przesłonięcie zbioru komunikatów (Override Message File - OVRMSGF) w celu zmiany komend wykorzystywanych przez menu Żądań systemowych.

Przy każdym naciśnięciu klawisza Żądania systemowego, system automatycznie zmienia bieżący profil użytkownika dla zadania na początkowy profil użytkownika tego zadania. Dzieje się tak, aby nie dawać użytkownikowi dodatkowych uprawnień w menu Żądań systemowych lub w programie wyjściowym Żądań przedsystemowych. Po zakończeniu funkcji Żądania systemowego, bieżący profil użytkownika dla zadania ustawiany jest na wartość, którą posiadał przed naciśnięciem klawisza Żądania systemowego.

Ograniczając uprawnienia do pewnych komend można zapobiec wybieraniu przez użytkowników niektórych opcji z menu żądania systemowego. Tabela 127 pokazuje komendy związane z opcjami menu:

Tabela 127. 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)
5	Wysłanie komunikatu (Send Message - SNDMSG)
6	Wyświetlenie komunikatów (Display Message - DSPMSG)
7	Wyświetlenie użytkownika stacji roboczej (Display Workstation User - DSPWSUSR)

Tabela 127. Opcje i komendy dla menu żądania systemowego (kontynuacja)

Opcja	Komenda
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.)
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. 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

Fabryczna konfiguracja systemu pod względem możliwości korzystania z komend odpowiada wymaganiom dotyczącym bezpieczeństwa większości instalacji. Niektóre komendy mogą być uruchamiane tylko przez osobę odpowiedzialną za bezpieczeństwo. Inne wymagają uprawnień specjalnych, takich jak *SAVSYS. Większość komend może być używana przez wszystkich użytkowników systemu. Uprawnienia do komend można zmienić w zależności od indywidualnych wymagań dotyczących bezpieczeństwa.

Na przykład, administrator może chcieć uniemożliwić większości użytkowników w systemie pracę z komunikacją. 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

uprawnienie *USE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 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. Administrator może również chcieć ograniczyć dostęp do całej biblioteki. Jeśli w systemie używana jest jedna lub więcej wersji programu licencjonowanego i5/OS 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.

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. Choć 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. W celu okresowego przeglądania próbek pozycje kroniki można użyć komendy Wyświetlenie kroniki (Display Journal - DSPJRN).

Odsyłacze pokrewne

“Używanie uprawnień adoptowanych w projekcie menu” na stronie 237
Dostępność narzędzia do wspomagania podejmowania decyzji, takiego jak Query/400, stanowi wyzwanie przy projektowaniu ochrony. 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.

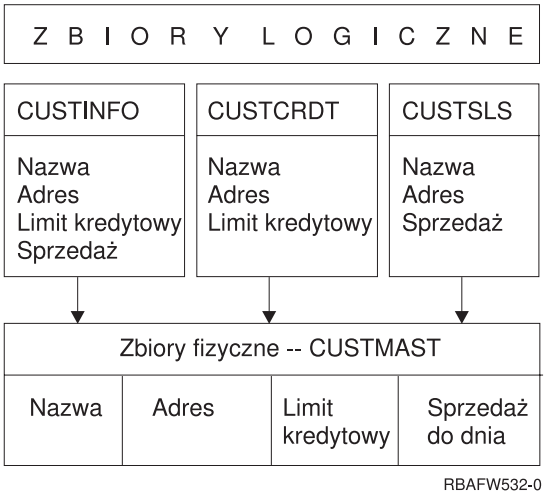
Ochrona zbiorów logicznych

Ochrona zasobów w systemie wspiera opcję zabezpieczania zbioru na poziomie pól. Do zabezpieczania pól lub rekordów w zbiorze można także użyć zbiorów logicznych.

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 dostępowi 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. 40 na stronie 244 przedstawia przykład zbioru fizycznego oraz trzech różnych związanych z nim zbiorów logicznych.



Rysunek 40. 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 128. 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:

```
                          Wyśw. uprawnień dla obiektu

Obiekt . . . . . :   CUSTINFO      Właściciel  . . . . . :   OWNAR
  Biblioteka . . . . . : CUSTLIB       Grupa główna        . . . :   *NONE
Typ obiektu . . . . :   *FILE          Urządzenie ASP  . . . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji .. . . . . :   *NONE

                        Obiekt
Użytkownik  Grupa       do obiektu
*PUBLIC                 *USE
```

```
                          Wyśw. uprawnień dla obiektu

Obiekt . . . . . :   CUSTCRDT      Właściciel . . . . . :   OWNAR
  Biblioteka . . . . :   CUSTLIB       Grupa podstawowa . . :   DPTAR
Typ obiektu . . . . :   *FILE          Urządzenie ASP  . . . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji .. . . . . :   *NONE

                        Obiekt
Użytkownik  Grupa       do obiektu
DPTAR                   *CHANGE
*PUBLIC                 *USE
```

```
                          Wyśw. uprawnień dla obiektu

Obiekt . . . . . :   CUSTSLS      Właściciel  . . . . . :   OWNSM
  Biblioteka . . . . :   CUSTLIB       Grupa podstawowa . . :   DPTSM
Typ obiektu . . . . :   *FILE          Urządzenie ASP  . . . . . :   *SYSBAS

Obiekt jest chroniony przez listę autoryzacji .. . . . . :   *NONE

                        Obiekt
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 192.

Począwszy od wersji V3R1 programu licencjonowanego i5/OS można podawać uprawnienia do danych dla zbiorów logicznych. Jeśli zbiór logiczny z wersji systemu wcześniejszej niż V3R1 zostanie odtworzony w systemie w wersji V3R1 lub nowszej, system przekształci zbiory logiczne podczas ich otwierania po raz pierwszy. System udziela wszystkich uprawnień 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.

Informacje pokrewne

DB2 Universal Database for iSeries

Przesłanianie zbiorów

Komendy przesłaniania umożliwiają użycie przez program innego zbioru o tym samym formacie.

Przyjmijmy na przykład, że program w aplikacji Kontrakty i wycena w przedsiębiorstwie JKL Toy Company przed zmianą cen zapisuje informacje o cenach w zbiorze roboczym. Użytkownik posiadający dostęp do wiersza poleceń, chcący przechwycić poufne informacje, może skorzystać z komendy przesłaniania, aby zmusić program do zapisania danych w innym zbiorze w bibliotece kontrolowanej przez użytkownika.

Aby mieć pewność że program przetwarza odpowiednie zbiory, można przed uruchomieniem programu wykonać komendy przesłaniania z parametrem SECURE(*YES). Gdyby został użyty parametr SECURE(*NO), te zbiory nie będą zabezpieczone przed przesłanianiem przez inne zbiory. Ich wartości mogą zostać przesłonięte przez efekty dowolnych komend przesłaniania, które były wcześniej wywoływane.

Bezpieczeństwo zbiorów a język SQL

Należy zwrócić szczególną uwagę podczas używania programu CL adoptującego uprawnienia w celu uruchomienia SQL lub menedżera zapytań. Oba te programy umożliwiają użytkownikom podanie nazwy zbioru. W ten sposób użytkownik może uzyskać dostęp do dowolnego zbioru, do którego adoptowany profil ma uprawnienia.

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.

Planowanie profili grupowych

Profil grupowy jest przydatnym narzędziem, gdy kilku użytkowników ma podobne wymagania ochrony. Profile można tworzyć od razu jako profile grupowe albo zmienić na profil grupowy już istniejący profil. Używając profili grupowych można wydajniej zarządzać uprawnieniami oraz zmniejszyć liczbę pojedynczych uprawnień prywatnych dla obiektów.

Zbiory grup są szczególnie przydatne, kiedy 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.

Profil grupowy jest po prostu szczególnym typem profilu użytkownika. W przypadku spełnienia poniższych warunków staje się on profilem grupowym:

- 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.

Pojęcia pokrewne

"Profile grupowe" na stronie 4
Profil grupowy jest szczególnym typem profilu użytkownika. Można go używać do definiowania uprawnień dla grupy użytkowników, zamiast przyznawania uprawnień każdemu użytkownikowi z osobna.

Uwagi dotyczące grup podstawowych 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.

Zadania pokrewne

"Przypadek 2: Używanie uprawnień grupy podstawowej" na stronie 192
W tym przypadku zademonstrowano sposób użycia uprawnień grupy podstawowej.

Uwagi dotyczące wielu profili grupowych

Używając profili grupowych, można efektywniej zarządzać uprawnieniami oraz zmniejszyć liczbę pojedynczych uprawnień prywatnych do obiektów. Niepoprawne użycie profili grupowych może negatywnie wpłynąć na wydajność sprawdzania uprawnień. Ta sekcja zawiera pewne sugestie dotyczące korzystania z wielu profili grupowych.

Użytkownik może być członkiem do 16 grup: pierwszej grupy (parametr GRPPRF w profilu użytkownika) i 15 grup dodatkowych (parametr SUPGRPPRF).

Poniżej znajdują się porady przydatne w sytuacjach, w których wykorzystywanych jest kilka 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 "Jak system sprawdza uprawnienia" na stronie 174. Należy zapoznać się dokładnie z wykorzystywaniem wielu grup w połączeniu z innymi technikami ochrony, takimi jak listy autoryzacji, w celu poznania wpływu tych technik na wydajność systemu.

Akumulowanie uprawnień specjalnych dla członków profili grupowych

Uprawnienia specjalne dla członków wielu grup są łączone.

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: Jeśli członek grupy jest właścicielem programu, program adoptuje tylko uprawnienia właściciela. Uprawnienia grupy właściciela 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.

Jest możliwa sytuacja, w której pewien użytkownik ma wszystkie uprawnienia wymagane przez grupę użytkowników i kusi, aby zamienić profil użytkownika na profil grupowy. Jednak wykorzystanie pojedynczego profilu jako profilu grupowego może spowodować problemy w przyszłości:

- 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 okaże się, że po zakończeniu pracy aplikacji użytkownik posiada uprawnienia, które powinny należeć do grupy użytkowników, należy wykonać następujące czynności:

1. Utwórz profil grupowy.
2. Użyj komendy GRTUSRAUT, aby nadać uprawnienia użytkownika profilowi grupowemu.
3. Usuń uprawnienia prywatne użytkownika, ponieważ nie są już potrzebne. Użyj komendy RVKOBJAUT lub EDTOBJAUT.

Porównanie profili grupowych i list autoryzacji

Profile grupowe są używane do uproszczenia zarządzania profilami użytkowników, które mają podobne wymagania bezpieczeństwa. Listy autoryzacji używane są do zabezpieczania obiektów o podobnych wymaganiach bezpieczeństwa.

Tabela 129 opisuje charakterystyki obu metod.

Tabela 129. 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	Tak [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. Prywatne uprawnienia grupowe są składowane, jeśli w komendzie składowania podano PVTAUT(*YES).

Dla listy autoryzacji elementu ″Uprawnienia mogą zostać określone przy tworzeniu obiektu″:

- Aby przypisać listę autoryzacji obiektowi opartemu na bibliotece, należy określić AUT (*LIBCRTAUT) dla komendy CRTxxxx i CRTAUT (nazwa_listy_autoryzacji) dla biblioteki. Niektóre obiekty, takie jak listy sprawdzania, nie mogą korzystać z wartości *LIBCRTAUT dla komendy CRT.

- Aby przypisać listę autoryzacji obiektowi opartemu na katalogu, należy określić wartość *INDIR dla parametrów DTAAUT i OBJAUT komendy MKDIR. Dzięki temu, lista autoryzacji zabezpieczać będzie zarówno katalog nadrzędny jak i nowo powstały. System nie zezwala na określenie arbitralnej listy autoryzacyjnej podczas tworzenia obiektu.

Planowanie ochrony dla programistów

Programiści stanowią problem dla osoby odpowiedzialnej za bezpieczeństwo. Ich wiedza umożliwia im obejście procedur ochrony, które nie zostały uważnie zaprojektowane.

Programiści mogą obejść mechanizmy bezpieczeństwa w celu uzyskania dostępu do danych, których potrzebują do testów. 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; jeśli muszą mieć uprawnienia specjalne, należy nadawać im tylko te, które są wymagane do wykonywania zadań lub czynności 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 wszystkie 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 147,
- 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 może mieć niekontrolowany dostęp do nich w środowisku produkcyjnym; Profil będący właścicielem aplikacji może być profilem użytkownika odpowiedzialnego za aplikację, lub profilem utworzonym specjalnie jako właściciel tej aplikacji.

Zarządzanie zbiorami źródłowymi

Zabezpieczenie informacji w systemie wymaga dokładnego zaplanowania ochrony zbiorów źródłowych.

Zbiory źródłowe są bardzo ważne dla integralności systemu. Mogą być również cennym zasobem firmy, jeśli utworzyła ona lub nabyła aplikacje niestandardowe. Zbiory źródłowe powinny być chronione, tak jak inne ważne zbiory w systemie. Należy rozważyć umieszczenie zbiorów źródłowych w oddzielnej bibliotece i kontrolowanie tego, kto może je aktualizować i przenosić do środowiska produkcyjnego.

Gdy w systemie tworzony jest zbiór źródłowy, domyślne uprawnienia publiczne mają wartość *CHANGE. Umożliwia to 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, aby mogli dodawać nowe podzbiory. Uprawnienia publiczne powinny być zredukowane do *USE lub *EXCLUDE, chyba że zbiory źródłowe znajdują się w chronionej bibliotece.

Ochrona plików klas Java i plików jar w zintegrowanym systemie plików

Aby uruchomić program Java, użytkownik musi mieć uprawnienie Odczyt (*R) dla każdego zbioru klasy Java i zbioru jar oraz uprawnienie Wykonywanie (*X) dla każdego katalogu w ścieżce do zbiorów klas Java i zbiorów jar. Jeśli użytkownik korzysta ze zbiorów klas Java i zbiorów jar w zintegrowanym systemie plików, konieczne jest zabezpieczenie ich za pomocą normalnych uprawnień obiektów.

Aby zabezpieczyć zbiory Java, należy użyć komendy CHGAUT w celu ochrony katalogów w ścieżce i zbiorów z atrybutami uprawnień obiektów. Użytkownik może potrzebować uprawnień odczytu (*R) dla zbiorów klas Java i zbiorów jar, aby uruchomić program Java. Mogą otrzymać te uprawnienia z uprawnień publicznych zbioru lub z uprawnień prywatnych. Lista autoryzacji może okazać się pomocna przy konfiguracji uprawnień dla grupy użytkowników. Nie należy dawać nikomu uprawnień zapisu (*W) dla zbioru, chyba że mogą oni go zmieniać.

Parametr Poziomu ochrony ścieżki (CHKPATH) komendy RUNJVA umożliwia sprawdzenie, czy działająca aplikacja Java korzysta z odpowiednich zbiorów ze ścieżki CLASSPATH. Za pomocą wartości CHKPATH(*SECURE) można zapobiec wykonaniu programu Java, jeśli dla każdego katalogu w ścieżce CLASSPATH, który ma publiczne uprawnienie zapisu, został wysłany komunikat ostrzegawczy.

Planowanie ochrony dla programistów systemowych lub menedżerów

W celu ochrony zbiorów w systemie można ograniczyć uprawnienia udzielane programistom systemowym lub menedżerom.

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.

Jeśli na przykład chcesz, aby Sue i Fred byli dwiema osobami, które mogą tworzyć i zmieniać profile użytkowników bez udzielania im uprawnień specjalnych, możesz to osiągnąć, wykonując następujące kroki:

1. Napisz komendę lub program, który stanowi element frontowy komendy CRT/CHGUSRPRF.
2. Niech ta komenda lub program adoptuje profil, który może wykonywać operacje tworzenia i zmieniania.
3. Autoryzuj Sue i Freda do korzystania z tego programu.

Wtedy Sue i Fred będą mogli wykonywać zadanie tylko przez aplikację.

Korzystanie z list sprawdzania

Obiekty listy sprawdzania dają aplikacjom możliwość bezpiecznego składowania informacji uwierzytelniających użytkowników.

Na przykład w programie Internet Connection Server (ICS) listy sprawdzania są wykorzystywane do utworzenia pojęcia użytkownika Internetu. Serwer ICS może wykonać podstawowe uwierzytelnienie przed otworzeniem strony WWW. 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 System i oraz hasła.

Użytkownik Internetu może uzyskać (lub też nie) dostęp do systemu z serwera WWW. Jednak nie ma on żadnych uprawnień do zasobów systemu System i lub uprawnień do wpisywania się i uruchamiania zadań. Dla użytkowników Internetu nie jest nigdy tworzony profil użytkownika systemu System i.

Do tworzenia lub usuwania list sprawdzania można użyć komend 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.

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. Ponieważ lista sprawdzania jest zaszyfrowana, ta metoda jest bezpieczniejsza niż weryfikowanie hasła użytkownika przez samą aplikację.

Informacje uwierzytelniania można składować w postaci odszyfrowywalnej. Jeśli użytkownik ma odpowiednią ochronę, informacje te mogą zostać odszyfrowane i zwrócone do użytkownika.

Odsyłacze pokrewne

"Zachowanie ochrony serwera (QRETSVRSEC)" na stronie 32
Wartość systemowa Zachowywanie bezpieczeństwa serwera (Retain Server Security - QRETSVRSEC) określa, czy możliwe do odszyfrowania informacje o uwierzytelnianiu powiązane z profilem użytkownika lub pozycjami listy sprawdzania (*VLDL) można zachowywać w systemie hosta. Nie obejmuje to hasła profilu użytkownika systemu System i.

Informacje pokrewne

Aplikacyjne interfejsy programistyczne (API)

Ograniczanie dostępu do funkcji programu

Ograniczenie dostępu do funkcji programu umożliwia zdefiniowanie użytkowników mających dostęp do aplikacji, jej części lub funkcji wewnątrz 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. Funkcja przechodzi przez następujące procesy w celu weryfikacji.

- 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.

Funkcja ograniczenia dostępu do funkcji programu umożliwia wykonywanie następujących zadań przez funkcje API: Aby skorzystać z tej funkcji wewnątrz aplikacji, dostawca tej aplikacji musi zarejestrować funkcje podczas jej instalacji. Zarejestrowana funkcja odpowiada blokowi kodu realizującemu określone funkcje w aplikacji. Gdy użytkownik uruchamia aplikację, przed wywołaniem bloku kodu aplikacja wywołuje funkcję API sprawdzania użycia, aby sprawdzić, czy użytkownik ma uprawnienie do korzystania z funkcji, która jest związana z blokiem kodu. 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. Administrator może zarządzać dostępem do funkcji w programie za pomocą komendy Praca z informacjami o wykorzystaniu funkcji (Work with Function Usage Information - WRKFCNUSG) lub użyć w tym celu funkcji Administrowanie aplikacjami w programie System i Navigator.

Informacje pokrewne

Administrowanie aplikacjami

Rozdział 8. Składowanie i odtwarzanie informacji o bezpieczeństwie

Składowanie informacji o bezpieczeństwie jest tak samo ważne, jak składowanie danych. W niektórych sytuacjach, konieczne może być odzyskanie profili użytkowników, uprawnień obiektów i danych systemowych. Jeśli informacje ochrony nie zostały zapisane, konieczne będzie ręczne odbudowanie profili użytkowników i uprawnień obiektów. Taka operacja może być czasochłonna oraz prowadzić do błędów i ryzyka naruszenia ochrony.

Ten temat zawiera informacje z następujących obszarów:

- 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.

Planowanie odpowiednich procedur składowania i odtwarzania informacji o ochronie wymaga zrozumienia, jak te informacje są przechowywane, składowanie oraz odtwarzane.

Tabela 130 przedstawia komendy służące do zapisywania i odtwarzania informacji o bezpieczeństwie. Przedstawione poniżej sekcje prezentują szczegółowe omówienie składowania i odtwarzania informacji o ochronie.

Tabela 130. W jaki sposób są składowane i odtwarzane informacje o ochronie.

	Komendy użyte do zapisywania i odtwarzania					
Zapisywana lub odtwarzana informacja o bezpieczeństwie	**SAVSECDTA SAVSYS**	**SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG**	**RSTUSRPRF**	**RSTOBJ RSTLIB RSTDLO RSTCFG**	**RSTAUT**	**RSTDFROBJ**
Profile użytkowników	X		X			
Prawo własności[1]		X		X		X
Grupa podstawowa[1]		X		X		X
Uprawnienia publiczne[1]		X		X		X
Uprawnienie prywatne[3]	X	X	X	X	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	
Listy sprawdzania		X		X		
Pozycje uwierzytelniania serwera	X		X			

Tabela 130. W jaki sposób są składowane i odtwarzane informacje o ochronie. (kontynuacja)

Zapisywana lub odtwarzana informacja o bezpieczeństwie	Komendy użyte do zapisywania i odtwarzania					
	SAVSECDTA SAVSYS	**SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG**	**RSTUSRPRF**	**RSTOBJ RSTLIB RSTDLO RSTCFG**	**RSTAUT**	**RSTDFROBJ**
[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.						
[3] Komenda SAVSECDTA zapisuje uprawnienie prywatne dla wszystkich obiektów. Komenda RSTUSRPRF odtwarza informacje o uprawnieniach niezbędnych do odtworzenia uprawnień prywatnych. Uprawnienia prywatne odtwarza się za pomocą komendy RSTAUT. Uprawnienia prywatne do poszczególnych obiektów można zapisać za pomocą komend SAV, SAVLIB, SAVOBJ i SAVCHGOBJ. Uprawnienia prywatne do poszczególnych obiektów, zapisane za pomocą komend zapisujących (SAVE), można odtwarzać za pomocą komend RST, RSTLIB i RSTOBJ.						

Informacje pokrewne

Składowanie i odtwarzanie

Składowanie i odtwarzanie - plik PDF

Sposób przechowywania informacji o bezpieczeństwie

Zaplanowanie odpowiednich procedur tworzenia i odtwarzania kopii zapasowych informacji o bezpieczeństwie wymaga znajomości sposobu przechowywania i zapisywania tych informacji.

Informacje o ochronie przechowywane są z obiektami, profilami użytkowników i listami autoryzacji:

Informacje o uprawnieniach zapisywane 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 zapisywane 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 uwierzytelniające serwer*:
  - Pozycje dotyczące uwierzytelniania serwera.

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.

Pojęcia pokrewne

"Informacje dodatkowe powiązane z profilem użytkownika" na stronie 117
W tym temacie omówione zostały uprawnienia prywatne, informacje o posiadanych obiektach oraz informacje o obiektach grupy podstawowej powiązanych z profilem użytkownika.

Zapisywanie Informacji o bezpieczeństwie

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
- Uprawnienia prywatne dla obiektu, jeśli w komendzie SAVxxx podano atrybut PVTAUT(*YES).

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).

- Inne informacje o aplikacji powiązane z profilem użytkownika. Na przykład:
  - Pozycje dotyczące uwierzytelniania serwera.
  - Pozycje dotyczące informacji o aplikacji użytkownika, dodawane za pomocą funkcji API Aktualizacja informacji o aplikacji użytkownika (Update User Application Information - QsyUpdateUserApplicationInfo)

Tabela uprawnień składowana z profilem użytkownika:

- Jeden rekord na każde uprawnienie prywatne profilu użytkownika, w tym na ustawienia użycia zarejestrowanych funkcji.

Informacje o rejestracji funkcji, składowane z obiektem QUSEXRGOBJ:

- Informacje o zarejestrowaniu funkcji mogą być zeskładowane podczas składowania obiektu QUSEXRGOBJ *EXITRG w bibliotece QUSRSYS.

Odtwarzanie Informacji o bezpieczeństwie

Odzyskiwanie systemu często wymaga odtworzenia danych i związanych z nimi informacji o ochronie.

Typowa sekwencja odzyskiwania wymaga:

1. Odtworzenia profili użytkowników i list autoryzacji (RSTUSRPRF USRPRF(*ALL)).
2. Odtwarzanie obiektów (RSTCFG, RSTLIB, RSTOBJ, RSTDLO lub RST).
3. Odtworzenia uprawnień prywatnych do obiektów (RSTAUT).

Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki zapisane w sekcji Rozdział 10, “Licencja na kod oraz Informacje dotyczące kodu”, na stronie 317.

Informacje pokrewne

Składowanie i odtwarzanie

Odtwarzanie profili użytkowników

W odtwarzanym profilu użytkownika mogą pojawić się pewne zmiany.

Obowiązują następujące reguły

- Jeśli profile odtwarzane są pojedynczo (nie podano parametru RSTUSRPRF USRPRF(*ALL)), parametr SECDTA(*PWDGRP) nie jest wymagany, a odtwarzany profil nie istnieje w systemie, następujące pola są zmieniane na wartość *NONE:
  - 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).

Ważne:

1. Profile użytkownika zapisywane z systemu o innym poziomie hasła (wartość systemowa QPWDLVL) niż system, na którym są one odzyskiwane, mogą posiadać nieprawidłowe na systemie odzyskiwania. Na przykład, mogły zostać profile zapisane na systemie o poziomie hasła 2, zaś hasło użytkownika to ″Moje hasło″. Takie hasło nie będzie poprawne w systemie z poziomem hasła 0 lub 1.
2. Warto zapisać hasło osoby odpowiedzialnej za bezpieczeństwo (QSECOFR) przypisane do poszczególnych wersji zapisywanych informacji o bezpieczeństwie. Dzięki temu zawsze będzie można wpisać się do systemu w razie potrzeby przeprowadzenia operacji pełnego odtwarzania.

Do zresetowania hasła dla profilu QSECOFR można wykorzystać narzędzia DST.

- 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).
- Jeśli system znajduje się na poziomie bezpieczeństwa 30 lub wyższym, to w wymienionych poniżej sytuacjach z odtwarzanych profili użytkowników usuwane są uprawnienia specjalne *ALLOBJ:
  - 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.

  Ważne: 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:
  - profil użytkownika QSYS (system)
  - profil użytkownika QSECOFR (osoba odpowiedzialna za bezpieczeństwo)
  - QLPAUTO (automatyczna instalacja programu licencjonowanego), profil użytkownika
  - profil użytkownika QLPINSTALL (instalowanie programu licencjonowanego)

  Informacje pokrewne

  Resetowanie hasła profilu użytkownika QSECOFR

Odtwarzanie obiektów

Podczas odtwarzania obiektu system korzysta z informacji o uprawnieniach zeskładowanych razem z obiektem. W tym temacie opisano reguły przetwarzania informacji o uprawnieniach podczas odtwarzania obiektów.

Ochrony odtworzonego obiektu dotyczą:

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, zaś właściciel systemu jest inny niż właściciel nośnika, obiekt nie zostanie odtworzony, chyba że określony zostanie parametr ALWOBJDIF(*ALL) lub ALWOBJDIF(*OWNER). W takim przypadku obiekt jest odtwarzany i używany jest właściciel w nowym systemie.
- Dodatkowe uwagi dotyczące odtwarzania programów zawiera sekcja “Odtwarzanie programów” na stronie 260.

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 zapisanego 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 określony zostanie parametr ALWOBJDIF(*ALL) lub ALWOBJDIF(*AUTL), obiekt zostanie odtworzony. Obiekt zostaje powiązany z listą autoryzacji, skojarzoną z istniejącym obiektem.
- Jeśli odtwarzany jest dokument lub folder, który już istnieje w systemie, to 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 określony zostanie parametr ALWOBJDIF(*ALL) lub ALWOBJDIF(*AUTL), obiekt zostanie powiązany z listą autoryzacj i.
  – jeśli podano If ALWOBJDIF(*NONE) obiekt nie jest powiązywany z listą autoryzacji, a jego uprawnienia publiczne ustawiane są na *EXCLUDE.

Uprawnienie prywatne:

- Uprawnienie prywatne jest zapisywane wraz z profilami użytkownika. Jeśli w komendzie SAVxxx podano atrybut PVTAUT(*YES), to uprawnienie prywatne będzie zapisywane również razem z obiektami.
- Jeśli profile użytkowników mają uprawnienia prywatne dla odtwarzanego obiektu, uprawnienia te zazwyczaj nie zostaną zmienione. Odtwarzanie niektórych rodzajów programów może spowodować odwołanie niektórych uprawnień prywatnych.
- Gdy obiekt zostanie usunięty z systemu, to przestaje istnieć również uprawnienie prywatne do tego obiektu. Gdy obiekt jest usuwany, wszystkie uprawnienia prywatne do obiektu są usuwane z profili użytkowników. Jeśli obiekt zostanie później odtworzony ze składowanej wersji, to uprawnienia prywatne zostaną odtworzone tylko wtedy, jeśli przy zapisywaniu obiektu podano atrybut PVTAUT(*YES).
- Jeśli uprawnienia prywatne nie zostały zapisane wraz z obiektem, a trzeba je odtworzyć, należy użyć komendy 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, to wartość kontrolowania obiektu nie jest zmieniana. Wartość OBJAUD zeskładowanej wersji obiektu nie jest odtwarzana.
- Jeśli odtwarzana biblioteka lub katalog nie istnieje w systemie, to odtworzona zostanie wartość Tworzenia kontroli obiektu lub katalogu (Create object or directory auditing - CRTOBJAUD) dla odtwarzanej biblioteki lub katalogu.
- Jeśli odtwarzana biblioteka lub katalog istnieje i ma zostać zastąpiona, wartość CRTOBJAUD dla biblioteki lub katalogu nie zostanie odtworzona. Wykorzystana zostanie istniejąca wartość CRTOBJAUD.

Magazyn uprawnień:
- Jeśli przy odtwarzaniu zbioru okaże się, że istnieje magazyn uprawnień dla tego zbioru oraz biblioteki, do której zbiór jest odtwarzany, to zbiór zostanie połączony z tym magazynem uprawnień.
- Informacje o uprawnieniach związane z magazynem uprawnień zastępują uprawnienia publiczne oraz informacje o właścicielu zeskładowane ze zbiorem.

Obiekt z domeny użytkownika:

System ogranicza obiekty z domeny użytkownika (*USRSPC, *USRIDX i *USRQ) do bibliotek określonych w wartości systemowej QALWUSRDMN. Jeśli biblioteka przenoszona jest z wartości systemowej QALWUSRDMN po zeskładowaniu obiektu z domeny użytkownika typu *USRSPC, *USRIDX lub *USRQ, podczas odtwarzania obiektu system zmienia go na domenę systemową.

Informacje o rejestrowaniu 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 korzystające z 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.

Pojęcia pokrewne

“Odtwarzanie programów” na stronie 260
Odtwarzanie w systemie programów, które zostały pobrane z nieznanego źródła, stanowi ryzyko naruszenia ochrony. Ten temat zawiera informacje o czynnikach, które należy uwzględnić podczas odtwarzania programów.

“Odtwarzanie list autoryzacji” na stronie 261
Nie istnieje żadna metoda odtworzenia pojedynczej listy. Podczas odtwarzania listy autoryzacji uprawnienia i prawo własności ustawiane jest tak samo, jak dla innych odtwarzanych obiektów.

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) odtwarza uprawnienia prywatne profilu użytkownika, korzystając z informacji z tabeli uprawnień. Dla każdego uprawnienia prywatnego z tabeli uprawnień uruchamiana jest operacja nadawania uprawnień. Jeśli odtwarza się uprawnienia dla wielu profili, a w tabelach uprawnień istnieje wiele uprawnień prywatnych, proces ten może okazać się długotrwały.

Komendy RSTUSRPRF and RSTAUT można uruchamiać dla pojedynczego profilu, listy profili, ogólnej nazwy profili lub dla wszystkich profili. System przegląda nośnik składowania lub zbiór składowania utworzony przez komendę SAVSECDTA, komendę SAVSYS lub funkcję API QSRSAVO w poszukiwaniu profili, które mają zostać odtworzone.

Jeśli uprawnienia prywatne są składowane razem z obiektami, to można odtwarzać je wraz z obiektami. Jest to zalecana metoda, gdy składuje się i odtwarza względnie małą liczbę obiektów, a nie cały system.

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. Ten temat zawiera informacje o czynnikach, które należy uwzględnić podczas odtwarzania programów.

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.

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 (Force conversion on restore - QFRCCVNRST).

Uwaga: Programy zawierają informacje, które umożliwiają ponowne utworzenie programu podczas operacji 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.

Odtwarzanie programów adoptujących uprawnienia właściciela:

Gdy odtwarzany jest program adoptujący uprawnienia właściciela, prawo własności oraz uprawnienia do programu mogą zostać zmienione. Stosowane są następujące zasady:

- 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.

Pojęcia pokrewne

“Odtwarzanie obiektów” na stronie 257
Podczas odtwarzania obiektu system korzysta z informacji o uprawnieniach zeskładowanych razem z obiektem. W tym temacie opisano reguły przetwarzania informacji o uprawnieniach podczas odtwarzania obiektów.

Odsyłacze pokrewne

“Wartości systemowe odtwarzania związane z ochroną” na stronie 42
W temacie omówiono wartości systemowe odtwarzania związane z bezpieczeństwem w systemie operacyjnym i5/OS.

Odtwarzanie programów licencjonowanych

Ten temat zawiera instrukcje odtwarzania programów licencjonowanych w systemie.

Komenda Odtworzenie programu licencjonowanego (Restore Licensed Programs - RSTLICPGM) służy do instalowania w systemie programów dostarczonych przez firmę IBM. Można jej użyć także do zainstalowania programów producentów innych niż IBM, które zostały utworzone w programie licencjonowanym IBM System Manager for i5/OS.

W nowym systemie komendy RSTLICPGM mogą używać tylko 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. Zamiast uruchamiać komendę RSTLICPGM bezpośrednio z konta użytkownika z uprawnieniem *ALLOBJ, można użyć programu, który adoptuje uprawnienie specjalne *ALLOBJ.

Oto przykład tej techniki. Program, który będzie instalowany za pomocą komendy RSTLICPGM, nosi nazwę CPAPP (Umowy i ceny).

1. Utwórz profil użytkownika z uprawnieniami wystarczającymi do pomyślnego zainstalowania aplikacji. Nie nadawaj temu profilowi uprawnień specjalnych *ALLOBJ. W tym przykładzie profil użytkownika nosi nazwę OWNCP.
2. Napisz program do instalowania aplikacji. W tym przykładzie program ten nosi nazwę CPINST:

   Uwaga: Korzystając z przykładów kodu, użytkownik wyraża zgodę na warunki zapisane w sekcji Rozdział 10, “Licencja na kod oraz Informacje dotyczące kodu”, na stronie 317.

   ```
   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

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. Uprawnienia prywatne użytkowników do listy odtwarza się za pomocą komendy RSTAUT.

Listy autoryzacji składowane są za pomocą SAVSECDTA lub komendy SAVSYS. Odtwarzane są przez komendę:
`RSTUSRPRF USRPRF(*ALL)`

Odtwarzanie uszkodzonej listy autoryzacji

Jeśli dojdzie do uszkodzenia listy autoryzacji, która zabezpiecza obiekt, to dostęp do tego obiektu będą mieli tylko użytkownicy o uprawnieniu specjalnym *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.

Pojęcia pokrewne

“Odtwarzanie obiektów” na stronie 257
Podczas odtwarzania obiektu system korzysta z informacji o uprawnieniach zeskładowanych razem z obiektem. W tym temacie opisano reguły przetwarzania informacji o uprawnieniach podczas odtwarzania obiektów.

Odtwarzanie listy autoryzacji

Instrukcje podane w tym temacie umożliwiają odtworzenie listy autoryzacji.

Jeśli znane są uprawnienia użytkowników do listy autoryzacji, to można odtworzyć tę listę, wykonując następujące czynności:

1. Usuń listę autoryzacji.
2. Ponownie utwórz listę autoryzacji.
3. Dodaj do niej wszystkich znanych użytkowników.

Jeśli nie są znane uprawnienia wszystkich użytkowników, to listę autoryzacji można odtworzyć z ostatnio zapisanych taśm SAVSYS lub SAVECDTA. 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.

Procedura ta odtwarza wartości profilu użytkownika z nośnika. Więcej informacji na temat odtwarzania wartości profili użytkowników z nośników zapisu można znaleźć w sekcji “Odtwarzanie profili użytkowników” na stronie 256.

Odtwarzanie powiązań między obiektami a listą autoryzacji

Instrukcje podane w tym temacie umożliwiają odtworzenie powiązań między obiektami a listą autoryzacji.

Po usunięciu uszkodzonej listy autoryzacji, należy dodać zabezpieczane przez nią obiekty do nowej listy autoryzacji. Wykonaj następujące czynności:

1. Za pomocą komendy Odzyskiwanie pamięci (Reclaim Storage - RCLSTG) odszukaj obiekty powiązane z uszkodzoną listą autoryzacji. Komenda Odzyskiwanie pamięci (Reclaim storage) przypisuje do listy autoryzacji QRCLAUTL obiekty, które były związane ze zniszczoną listą.
2. Za pomocą komendy Wyświetlenie obiektów listy autoryzacji (Display Authorization List Objects - DSPAUTLOBJ) wyświetl obiekty powiązane z listą autoryzacji QRCLAUTL.
3. Za pomocą komendy Nadanie uprawnień dla obiektu (Grant Object Authority - GRTOBJAUT) zabezpiecz każdy obiekt za pomocą prawidłowej listy autoryzacji:

```
GRTOBJAUT OBJ(nazwa_biblioteki/nazwa_obiektu) +
          OBJTYPE(typ_obiektu) +
          AUTL(nazwa_listy autoryzacji)
```

Jeśli z listą autoryzacji QRCLAUTL powiązana jest duża liczba obiektów, to należy użyć komendy DSPAUTLOBJ z parametrem OUTPUT(*OUTFILE), aby utworzyć zbiór bazy danych. Można napisać program CL, który uruchomi komendę GRTOBJAUT dla każdego obiektu w zbiorze.

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.

Uprawnienie 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.

Kontrolowanie operacji składowania i odtwarzania

Jeśli wartość kontroli działania (wartość systemowa QAUDLVL lub wartość AUDLVL w profilu użytkownika) zawiera atrybut *SAVRST, to przy każdej operacji odtwarzania powstaje rekord kontroli bezpieczeństwa. Jeśli używana jest komenda odtwarzająca dużą liczbę obiektów, taka jak RSTLIB, rekord kontroli zapisywany jest dla każdego odtwarzanego obiektu. Może to powodować problemy wynikające z rozmiaru dziennika dla kroniki kontroli, zwłaszcza jeśli odtwarza się kilka bibliotek.

Komenda RSTCFG nie powoduje generowania rekordu kontroli dla każdego z odtworzonych obiektów. 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. Kontrola bezpieczeństwa na platformie System i

W tej sekcji opisano techniki kontroli efektywności zabezpieczeń 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 tej sekcji dotyczą wszystkich tych sytuacji. Dobór kontrolowanych elementów oraz częstotliwość kontrolowania zależą od wielkości organizacji i potrzeb związanych z ochroną. Celem tej sekcji jest omówienie następujących kwestii: jakie informacje są dostępne, jak je uzyskać i dlaczego są potrzebne, a nie udzielenie wskazówek dotyczących częstotliwości kontroli.

Ta sekcja 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 bezpieczeństwa obejmuje używanie komend w środowisku systemu System i oraz dostęp do informacji o systemie znajdujących się w protokołach i kronikach. Administrator może zdecydować się na utworzenie specjalnego profilu dla osoby odpowiedzialnej za kontrolę ochrony systemu. Profil ten, aby mógł zmieniać charakterystykę kontroli w systemie, wymaga uprawnienia specjalnego *AUDIT. Niektóre z zadań kontroli zalecanych w tej wymagają profilu użytkownika z uprawnieniami specjalnymi *ALLOBJ i *SECADM. Należy upewnić się, że hasło profilu kontrolera zostanie ustawione na *NONE po zakończeniu okresu kontroli.

Pojęcia pokrewne

“Kronika kontroli bezpieczeństwa” na stronie 6
Za pomocą kronik kontroli bezpieczeństwa można sprawdzać skuteczność zabezpieczeń systemu.

Lista kontrolna dla osób odpowiedzialnych za bezpieczeństwo systemu i kontrolerów

Lista kontrolna może być używana do planowania i kontroli bezpieczeństwa systemu.

Planując bezpieczeństwo systemu, należy wybrać te tematy z kolekcji, które najlepiej spełniają wymagania dotyczące bezpieczeństwa. Podczas kontrolowania bezpieczeństwa systemu należy użyć listy do oceny przeprowadzanej kontroli oraz określenia, czy konieczne są dodatkowe kontrole.

Każda lista służy jako przegląd informacji zawartych w tej kolekcji tematów. Listy zawierają krótkie opisy wykonania każdej pozycji i sposób sprawdzenia, że pozycja została wykonana, ze wskazaniem, jakich pozycji należy szukać w kronice QAUDJRN. Szczegóły dotyczące pozycji można znaleźć w tej kolekcji tematów.

Ochrona fizyczna

Lista kontrolna ochrony fizycznej ułatwia planowanie lub kontrolę ochrony fizycznej systemu.

Uwaga: Pełne omówienie fizycznej ochrony produktu System i zawiera sekcja Planowanie i konfigurowanie bezpieczeństwa systemu.

Lista kontrolna planowania ochrony fizycznej systemu jest następująca:

__ • 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. Klucze są wyjęte i przechowywane są osobno w dobrze zabezpieczonym miejscu. Więcej informacji na temat stacyjki zawiera sekcja Planowanie ochrony fizycznej jednostki systemowej.

__ • 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 jest równa 1. Aby sprawdzić, czy użytkownik QSECOFR ma uprawnienia *CHANGE, należy użyć komendy DSPOBJAUT dla urządzeń.

Wartości systemowe

Skonfigurowanie funkcji kontroli dla wartości systemowych pomaga w śledzeniu wartości zmienianych w systemie.

- 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.
- Użytkownik może użyć komendy Wyświetlenie atrybutów bezpieczeństwa (Display Security Attributes - DSPSECA) w celu zweryfikowania oczekujących wartości QSECURITY (poziom bezpieczeństwa) i QPWDLVL (poziom hasła) oraz bieżących ustawień systemu związanych z bezpieczeństwem (czy wartości te mogą być zmieniane).
- Przeglądaj okresowo decyzje dotyczące wartości systemowych. Jest to istotne zwłaszcza podczas zmian środowiska systemu, takich jak instalowanie nowych aplikacji lub sieci komunikacyjnych.

Profile użytkowników IBM

Zadania kontroli profili użytkowników IBM można wykonać, sprawdzając ich hasła.

- Hasło dla profilu użytkownika QSECOFR zostało zmienione.

  Hasło domyślne tego profilu ma wartość QSECOFR, aby można było zainstalować system. Hasło musi zostać zmienione przy pierwszym wpisaniu do systemu, a następnie zmieniane co jakiś czas po instalacji.

  Należy sprawdzić, czy hasło zostało zmienione, sprawdzając listę DSPAUTUSR pod kątem daty zmiany hasła QSECOFR oraz próbując wpisać się za pomocą hasła domyślnego.
- Hasła IBM dla narzędzi DST zostały zmienione.

Identyfikatory użytkowników dla narzędzi serwisowych nie są wyświetlane na liście DSPAUTUSR. Aby sprawdzić, czy identyfikatory użytkowników i hasła zostały zmienione, należy uruchomić DST i spróbować zalogować się używając wartości domyślnych.

- Za wyjątkiem profilu QSECOFR, nie należy wpisywać się do systemu używając profili użytkowników dostarczonych przez IBM.

  Te profile użytkowników IBM zaprojektowane zostały do posiadania obiektów lub uruchamiania funkcji systemowych. Należy użyć listy DSPAUTUSR aby sprawdzić, czy profile użytkowników dostarczone przez IBM, znajdujące się w Dodatek B, "Profile użytkowników IBM", na stronie 329, za wyjątkiem profilu QSECOFR, mają hasło ustawione na *NONE.

Pojęcia pokrewne

"Profile użytkowników IBM" na stronie 131
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 dostarczanych przez IBM.

"Praca z identyfikatorami użytkowników narzędzi serwisowych" na stronie 132
Istnienie kilka ulepszeń i dodatków do narzędzi serwisowych, ułatwiających ich używanie i zrozumienie.

Odsyłacze pokrewne

Dodatek B, "Profile użytkowników IBM", na stronie 329
Ta sekcja 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.

Kontrola hasła

Mechanizmy kontroli hasła umożliwiają kontrolowanie bezpieczeństwa systemu.

- 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.

Jeśli poziom haseł w systemie ma wartość inną niż 3, to gdy użytkownicy zmieniają swoje hasło, system próbuje utworzyć równoważne hasło, którego można będzie użyć na innych poziomach haseł. Aby sprawdzić, które profile użytkowników mają hasła, których można używać na różnych poziomach haseł, należy użyć komendy PRTUSRPRF TYPE(*PWDLVL).

Uwaga: Równoważne hasło jest najlepszą próbą utworzenia hasła możliwego do użycia na innych poziomach haseł, ale po zmianie poziomu haseł może ono nie przejść przez wszystkie reguły tworzenia hasła. Na przykład, jeśli na poziomie haseł 2 określono hasło BbAaA3x, system utworzy równoważne hasło BBAAA3X do użycia na

poziomach haseł 0 i 1. Dzieje się tak nawet wówczas, gdy wartość systemowa QPWDLMTCHR zawiera jako jeden ze znaków ograniczonych wartość 'A' (QPWDLMTCHR nie działa na poziomie hasła 2) lub wartość QPWDLMTREP określa, że sąsiadujące znaki nie mogą być takie same (ponieważ hasła sprawdzane są z rozróżnianiem wielkich i małych liter na poziomie 2, zaś bez rozróżniania na poziomach 0 i 1).

Profile użytkowników i profile grupowe

Aby skontrolować efektywność zabezpieczeń w systemie, można sprawdzić profile użytkowników i profile grupowe oraz ich uprawnienia.

- Każdy użytkownik ma przypisany unikalny profil użytkownika.

  Ustaw wartość systemową QLMTDEVSSN na 1. Ograniczanie każdego użytkownika do jednej sesji urządzenia w danym momencie nie zapobiega współużytkowaniu profili użytkowników, ale je ogranicza.
- Profile użytkowników z uprawnieniami specjalnymi *ALLOBJ są ograniczone i nie są używane jako profile grupowe.

  Użyj komendy DSPUSRPRF, aby sprawdzić uprawnienia specjalne profili użytkowników oraz określić, które profile są profilami grupowymi. Temat "Drukowanie wybranych profili użytkowników" na stronie 312 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 312.
- 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 249.
- 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 312.
- 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 zapewnić natychmiastowe usunięcie profili użytkowników po odejściu pracowników, przejrzyj pozycje dotyczące usunięcia obiektu w kronice kontroli.
- Menedżerowie regularnie sprawdzają uprawnienia użytkowników do systemu.

  Aby wyświetlić informacje o autoryzacjach użytkowników, użyj 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 312.

Kontrola autoryzacji

Sterowanie autoryzacją umożliwia kontrolę bezpieczeństwa informacji przechowywanych w systemie.

Następująca lista kontrolna może pomóc w kontroli bezpieczeństwa przez sterowanie autoryzacją.

- 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 opisu zadania, należy użyć komendy Wyświetlenie uprawnień obiektu (Display Object Authority - 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 213.
- 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 313.

- Interfejsy API zostały zabezpieczone.
- W celu uniknięcia problemów związanych z wydajnością, używane są dobre techniki ochrony.

Dostęp bez uprawnień

Listy niniejszej wraz z kroniką kontroli należy użyć w celu kontroli prób dostępu do informacji 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 komunikatów QSYSMSG, która jest monitorowana.
- Kronika kontroli kontrolowana jest pod kątem powtórzonych prób użytkownika. (Błędy autoryzacji powodują zapisanie w kronice kontroli pozycji typu AF.)
- Programy nie są w stanie uzyskiwać dostępu do obiektów za pomocą nieobsługiwanych interfejsów. (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 należy upewnić się, że żadne opisy podsystemów nie mają pozycji stacji roboczej, w której użyto opisu zadania z podaną nazwą profilu użytkownika.

Nieautoryzowane programy

Komenda Sprawdzenie integralności obiektu (Check Object Integrity - CHKOBJITG) umożliwia kontrolę nieautoryzowanych zmian wprowadzanych w programach w systemie.

- 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 pod kątem zmodyfikowanych obiektów” na stronie 314.

Komunikacja

Ta lista kontrolna może być użyta zarówno do planowania, jak i do kontroli mechanizmów wymaganych dla różnych typów komunikacji w systemie.

- Użyj procedur oddzwaniania, aby zabezpieczyć komunikację telefoniczną.
- Użyj szyfrowania ważnych danych.
- Kontroluj zdalne wpisywanie się. Wartość systemowa QRMTSIGN ustawiona jest na *FRCSIGNON lub używany jest program sprawdzania tranzytu.
- Użyj atrybutów sieciowych JOBACN, PCSACC oraz DDMACC do kontroli praw dostępu do danych w innych systemach, w tym do komputerów osobistych. Atrybut sieciowy JOBACN powinien mieć wartość *FILE.

Korzystanie z kroniki kontroli bezpieczeństwa

Kronika kontroli ochrony jest podstawowym źródłem informacji o kontroli dotyczących systemu. W niniejszej sekcji opisano sposób planowania i konfigurowania kontroli bezpieczeństwa oraz zarządzania nią, a także jakie informacje są zapisywane i w jaki sposób je przeglądać.

Kontroler bezpieczeństwa w organizacji lub poza nią może użyć funkcji kontroli udostępnianej przez system, aby zebrać informacje dotyczące zdarzeń związanych z bezpieczeństwem, 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 bezpieczeństwa” opisuje sposób wykonania tego zadania.

W momencie, gdy dojdzie do wydarzenia związanego z ochroną, które może być kontrolowane, system sprawdza, czy wybrane zdarzenie zostało wybrane do kontroli. 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 analizy danych można użyć jakiejś aplikacji lub narzędzia do zapytań.

Odsyłacze pokrewne

Dodatek F, “Układ pozycji kroniki kontroli”, na stronie 581
Ta sekcja 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.

Dodatek E, “Operacje na obiektach i kontrola”, na stronie 515
W tej kolekcji tematów opisano operacje, które można wykonywać na obiektach systemu oraz zamieszczono informacje o kontrolowaniu tych operacji.

Planowanie kontroli bezpieczeństwa

Funkcja kontroli bezpieczeństwa jest opcjonalna. Skonfigurowanie kontroli bezpieczeństwa wymaga wykonania pewnych określonych czynności.

Aby zaplanować użycie kontroli bezpieczeństwa w systemie, należy:

- określić, jakie zdarzenia związane z ochroną mają być zapisywane dla wszystkich użytkowników systemu; kontrola zdarzeń dotyczących bezpieczeństwa 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 działań

Wartość systemowa QAUDCTL (sterowanie kontrolą), wartość systemowa QAUDLVL (poziom kontroli), wartość systemowa QAUDLVL2 (rozszerzenie poziomu kontroli) oraz parametr AUDLVL (kontrola działania) w profilach użytkownika współpracują ze sobą w celu sterowania kontrolą działania:

Funkcje wartości systemowych są następujące:

- 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.

Zdarzenia, które zostaną wybrane do protokołowania, zależą od celów zabezpieczeń i potencjalnego ryzyka. Sekcja "Kontrola działań" na stronie 115 opisuje możliwe wartości poziomu kontroli oraz sposób ich użycia. Informuje także, czy są to wartości systemowe, parametry profilu użytkownika, czy oba jednocześnie.

Odsyłacze pokrewne

"Poziom kontroli (QAUDLVL)" na stronie 68
Wartość systemowa Poziom kontroli (Auditing Level - QAUDLVL) łącznie z wartością systemową QAUDLVL2 określa, które zdarzenia związane z bezpieczeństwem systemu są protokołowane w kronice kontroli bezpieczeństwa (QAUDJRN) dla wszystkich użytkowników systemu.

"Rozszerzenie poziomu kontroli (QAUDLVL2)" na stronie 70
Wartość systemowa Rozszerzenie poziomu kontroli (Auditing Level Extension - QAUDLVL2) jest wymagana, gdy potrzebnych jest więcej niż szesnaście wartości kontroli.

"Kontrola działań" na stronie 115
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.

Wartości związane z kontrolą działania:

W tej tabeli przedstawiono możliwe wartości dostępne dla wartości systemowych QAUDLVL i QAUDLVL2 oraz dla komendy CHGUSRAUD podczas kontrolowania działania systemu.

Tabela 131. Wartości związane z kontrolą 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.
*ATNEVT	Tak	Nie	**Zdarzenia uwagi**: System dodaje pozycje kroniki dla zdarzeń wymagających dalszego wglądu. Dzięki tym informacjom, użytkownik może ocenić możliwy wpływ zdarzenia uwagi na pracę systemu.

Tabela 131. Wartości związane z kontrolą działania (kontynuacja)

Możliwa wartość	Dostępna dla wartości systemowych QAUDLVL i QAUDLVL2	Dostępna dla komendy CHGUSRAUD	Opis
*AUTFAIL	Tak	Tak	**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. Parametr *CMD może zostać użyty do zapisania działań konkretnego użytkownika, np. osoby odpowiedzialnej za bezpieczeństwo.
*CREATE	Tak	Tak	**Tworzenie obiektów**: system zapisuje pozycję kroniki, gdy tworzony jest nowy lub zastępujący obiekt. Parametr *CREATE służy do monitorowania tworzenia i rekompilacji programów.
*DELETE	Tak	Tak	**Usuwanie obiektów**: system zapisuje pozycję kroniki, gdy usuwany jest obiekt.
*JOBBAS	Tak	Tak	**Funkcje podstawowe zadania**: protokołowane są działania wpływające na zadanie, takie jak uruchamianie lub zatrzymywanie zadania, wstrzymywanie, zwalnianie, anulowanie lub zmiana zadania.
*JOBCHGUSR	Tak	Tak	**Zmiany u użytkownika zadania**: protokołowane są zmiany aktywnego profilu użytkownika wątku lub profili grupowych.
*JOBDTA	Tak	Tak	**Działania związane z zadaniem**: protokołowane są działania wpływające na zadanie, takie jak uruchamianie lub zatrzymywanie zadania, wstrzymywanie, zwalnianie, anulowanie, zmiana zadania, zmiany aktywnego profilu użytkownika wątku lub profili grupowych. Parametr *JOBDTA służy do monitorowania użytkowników uruchamiających zadania w trybie wsadowym. Wartość *JOBDTA jest złożona z dwóch wartości, *JOBBAS oraz *JOBCHGUSR, które umożliwiają lepsze dostosowanie kontroli.
*NETBAS	Tak	Tak	**Podstawowe funkcje sieci**: działania dla reguł IP, połączenia przez gniazda, filtru przeszukiwania katalogów APPN, filtr zakończenia APPN.

Tabela 131. Wartości związane z kontrolą działania (kontynuacja)

Możliwa wartość	Dostępna dla wartości systemowych QAUDLVL i QAUDLVL2	Dostępna dla komendy CHGUSRAUD	Opis
*NETCLU	Tak	Tak	**Działania klastra lub grupy zasobów klastra**: pozycja kroniki kontroli jest zapisywana, gdy wystąpi co najmniej jedno z następujących zdarzeń: • 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	Tak	**Kontrola komunikacji sieciowej**: naruszenia ochrony wykryte przez obsługę filtru APPN protokołowane są w kronice kontroli bezpieczeństwa podczas kontroli filtru wyszukiwania katalogowego i filtru zakończenia. Parametr *NETCMN składa się z kilku wartości umożliwiających lepsze dostosowanie kontroli. Następujące wartości składają się na wartość *NETCMN: *NETBAS *NETCLU *NETFAIL *NETSCK.
*NETFAIL	Tak	Tak	**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	Tak	**Zadania gniazda**: pozycja kroniki kontroli zapisywana jest, gdy wystąpi co najmniej jedno z następujących zdarzeń: • 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. Parametr *OBJMGT może zostać użyty do wykrycia kopiowania poufnych informacji poprzez przeniesienia obiektu do innej biblioteki.

Tabela 131. Wartości związane z kontrolą 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. Parametr *OPTICAL może zostać użyty 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. Parametr *PGMADP może zostać użyty do sprawdzenia czy i gdzie nowa aplikacja korzysta z uprawnień adoptowanych.
*PGMFAIL	Tak	Tak	**Awarie programu**: system zapisuje pozycję kroniki, gdy program powoduje błąd integralności. Parametr *PGMFAIL może zostać użyty jako pomoc przy przenoszeniu na wyższy poziom ochrony lub podczas testowania nowej aplikacji.
*PRTDTA	Tak	Tak	**Funkcje drukowania**: protokołowane jest drukowanie zbioru buforowego, drukowanie bezpośrednio z programu lub wysyłanie zbioru buforowego do zdalnej drukarki. Parametr *PRTDTA może zostać użyty w celu wykrycia drukowanych informacji poufnych.
*SAVRST	Tak	Tak	**Działania odtwarzania**: Parametr *SAVRST może zostać użyty w celu wykrycia prób odtwarzania nieupoważnionych obiektów.
*SECCFG	Tak	Tak	**Konfiguracja bezpieczeństwa**: pozycja kroniki kontroli zapisywana jest, gdy wystąpi co najmniej jedno z następujących zdarzeń: • 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 osoby odpowiedzialnej za bezpieczeństwo narzędzi serwisowych na wartość domyślną.
*SECDIRSRV	Tak	Tak	**Funkcje usług katalogowych**: pozycja kroniki kontroli zapisywana jest, gdy wystąpi co najmniej jedno z następujących zdarzeń: • w kontroli, uprawnieniach, hasłach i prawie własności wprowadzane są zmiany, • następuje pomyślne konsolidowanie i odłączanie. • Zmiany wprowadzane są do strategii ochrony katalogów (np. strategia haseł)

Tabela 131. Wartości związane z kontrolą działania (kontynuacja)

Możliwa wartość	Dostępna dla wartości systemowych QAUDLVL i QAUDLVL2	Dostępna dla komendy CHGUSRAUD	Opis
*SECIPC	Tak	Tak	**Komunikacja między procesami**: pozycja kroniki kontroli zapisywana jest, gdy wystąpi co najmniej jedno z następujących zdarzeń: • wprowadzanie zmian w prawach własności lub uprawnieniach obiektu IPC, • tworzenie, usuwanie lub pobieranie obiektu IPC, • podłączanie pamięci współużytkowanej.
*SECNAS	Tak	Tak	**Działania usługi uwierzytelniania sieciowego**: pozycja kroniki kontroli zapisywana jest, gdy wystąpi co najmniej jedno z następujących zdarzeń: • nieprawidłowy 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 zestawu symboli graficznych: wygasłe referencje, błąd sumy kontrolnej lub wiązania kanału, • w przypadku odpakowania lub weryfikacji zestawu symboli graficznych wystąpią: wygasły kontekst, deszyfrowanie/dekodowanie, błąd sumy kontrolnej lub błąd kolejności.
*SECRUN	Tak	Tak	**Funkcje środowiska wykonawczego ochrony**: Zmiany w prawach własności obiektów, uprawnieniach i grupach podstawowych zapisywane są w kronice kontroli.
*SECSCKD	Tak	Tak	**Deskryptory gniazda**: pozycja kroniki kontroli zapisywana jest, gdy wystąpi co najmniej jedno z następujących zdarzeń: • deskryptor gniazda nadany zostanie innemu zadaniu, • odebrany zostanie deskryptor gniazda, • deskryptor gniazda jest nie do użycia.

Tabela 131. Wartości związane z kontrolą działania (kontynuacja)

Możliwa wartość	Dostępna dla wartości systemowych QAUDLVL i QAUDLVL2	Dostępna dla komendy CHGUSRAUD	Opis
*SECVFY	Tak	Tak	**Funkcje sprawdzania**: pozycja kroniki kontroli jest zapisywana, gdy wystąpi co najmniej jedno z następujących zdarzeń: • 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.
*SECVLDL.	Tak	Tak	**Operacje listy sprawdzania**: pozycja kroniki kontroli jest zapisywana, gdy wystąpi co najmniej jedno z następujących zdarzeń: • pozycja listy sprawdzania zostanie dodana, zmieniona, usunięta lub odnaleziona, • weryfikacja pozycji listy sprawdzania powiedzie się lub nie powiedzie.
*SECURITY	Tak	Tak	**Zadania bezpieczeństwa**: protokołowane są zdarzenia dotyczące bezpieczeństwa, takie jak zmiana profilu użytkownika lub wartości systemowej. Parametr *SECURITY może zostać użyty do śledzenia wszystkich działań dotyczących bezpieczeństwa. Parametr *SECURITY składa się z kilku wartości umożliwiających lepsze dostosowanie kontroli. Następujące wartości składają się na wartość *SECURITY: *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). Parametr *SERVICE może zostać użyty do wykrywania prób ominięcia 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. Parametr *SPLFDTA może zostać użyty do wykrycia prób wydruku lub wysłania poufnych danych.

Tabela 131. Wartości związane z kontrolą działania (kontynuacja)

Możliwa wartość	Dostępna dla wartości systemowych QAUDLVL i QAUDLVL2	Dostępna dla komendy CHGUSRAUD	Opis
*SYSMGT	Tak	Tak	**Zadania zarządzania systemem**: system zapisuje pozycję kroniki dla czynności zarządzania systemem, jak zmienianie listy odpowiedzi lub harmonogramu wł./wył. Parametr *SYSMGT może zostać użyty do wykrycia prób wykorzystania funkcji zarządzania systemem w celu ominięcia sterowania ochroną.

Pozycje kroniki dotyczące kontroli bezpieczeństwa:

Temat ten udostępnia dodatkowe informacje dotyczące 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,
- Zbiór wyjściowy bazy danych modeli może zostać użyty w celu zdefiniowania rekordu podczas tworzenia zbioru wyjściowego za pomocą komendy DSPJRN. pełny układ dla modelowych zbiorów wyjściowych bazy danych zawiera Dodatek F, “Układ pozycji kroniki kontroli”, na stronie 581,
- 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 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
Kontrola działania:				
*ATNEVT	IM	QASYIMJ5	P	Wykryto możliwe naruszenie systemu. Należy sprawdzić, czy rzeczywiście jest to włamanie, czy akcja oczekiwane bądź dozwolone działanie.

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
*AUTFAIL	AF	QASYAFJE/J4/J5	A	Próba dostępu do obiektu lub wykonania działania, do którego użytkownik nie był uprawniony.
			B	Instrukcja ograniczona
			C	Niepowodzenie sprawdzania poprawności
			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 działania programu wyjściowego.
			I	Systemowe dziedziczenie Java nie jest dozwolone
			J	Próba wprowadzenia lub ustalenia harmonogramu dla zadania z opisu zadania, w którym podano profil użytkownika. Użytkownik wprowadzający nie miał uprawnień *USE.
			K	Podjęto próbę wykonania czynności, do której użytkownik nie posiada odpowiednich uprawnień specjalnych.
			N	Token profilu nie jest tokenem do regeneracji.
			O	Błąd uprawnień do obiektu optycznego
			P	Podjęto próbę użycia uchwytu profilu, który nie jest poprawny dla funkcji API QWTSETP.
			R	Błąd ochrony sprzętu
			S	Próba domyślnego wpisania się do systemu.
			T	Brak uprawnień dla portu TCP/IP.
			U	Żądanie uprawnień użytkownika nie było poprawne.
			V	Niepoprawny token profilu dla operacji generowania nowego tokenu profilu.
			W	Niepoprawny token profilu do wymiany.
			X	Błąd systemu, patrz opis pozycji kroniki AF (błąd uprawnień)
			Y	Brak uprawnień do bieżącego pola JUID podczas wykonywania operacji usuwania zawartości pola JUID.

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
			Z	Brak uprawnień do bieżącego pola JUID podczas wykonywania operacji ustawiania pola JUID.
	CV	QASYCVJ4/J5	E	Połączenie nieoczekiwanie przerwane.
			R	Odrzucono połączenie.
	DI	QASYDIJ4/J5	AF	Błędy uprawnień.
			PW	Błędy haseł.
	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.
			C	Błąd CHKPWD.
			D	Podano niepoprawny identyfikator użytkownika narzędzi serwisowych.
			E	Podano niepoprawne hasło użytkownika narzędzi serwisowych.
			P	Wprowadzono niepoprawne hasło.
			Q	Próba wpisania się (uwierzytelnienia użytkownika) nie powiodła się, ponieważ profil użytkownika został wyłączony.
			R	Próba wpisania się (uwierzytelnienia użytkownika) nie powiodła się, ponieważ upłynął termin ważności hasła.
			S	Niepoprawne hasło deszyfrowania SQL.
			U	Niepoprawna nazwa użytkownika.
			X	Użytkownik narzędzi serwisowych jest wyłączony.
			Y	Użytkownik narzędzi serwisowych nie jest poprawny.
			Z	Niepoprawne hasło narzędzi serwisowych.
	VC	QASYVCJE/J4/J5	R	Połączenie zostało odrzucone z powodu niepoprawnego hasła.
	VO	QASYVOJ4/J5	U	Weryfikacja pozycji listy sprawdzania nie powiodła się.
	VN	QASYVNJE/J4/J5	R	Próba zalogowania sieciowego została odrzucona, z powodu nieważnego konta, błędnej godziny, niepoprawnego identyfikatora użytkownika lub błędnego hasła.
	VP	QASYVPJE/J4/J5	P	Użyto niepoprawnego hasła sieciowego.
	X1	QASYX1J5	F	Delegacja znacznika tożsamości nie powiodła się.

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
			U	Pobieranie użytkownika ze znacznika tożsamości nie powiodło się.
	XD	QASYXDJ5	G	Nazwy grup (powiązanych z pozycją DI)
*CMD [1]	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 [2]	CO	QASYCOJE/J4/J5	N	Tworzenie nowego obiektu, z wyjątkiem tworzenia obiektów w bibliotece QTEMP.
			R	Wymiana istniejącego obiektu.
	DI	QASYDIJ4/J5	CO	Obiekt utworzony.
	XD	QASYXDJ5	G	Nazwy grup (powiązanych z pozycją DI)
*DELETE [2]	DO	QASYDOJE/J4/J5	A	Obiekt usunięty.
			C	Oczekująca operacja kasowania zatwierdzona.
			D	Oczekująca operacja utworzenia wycofana.
			P	Oczekująca operacja usunięcia.
			R	Oczekująca operacja usunięcia wycofana.
	DI	QASYDIJ4/J5	DO	Obiekt usunięty.
	XD	QASYXDJ5	G	Nazwy grup (powiązanych z pozycją DI)
*JOBBAS	JS	QASYJSJ5	A	Użyto komendy ENDJOBABN
			B	Wprowadzono zadanie.
			C	Zmieniono zadanie.
			E	Zakończono zadanie.
			H	Wstrzymano zadanie.
			I	Odłączono zadanie.
			N	Użyto komendy ENDJOB
			P	Do zadania prestartu dołączono żądanie uruchomienia programu.
			Q	Zmieniono atrybuty zapytania.
			R	Zwolniono wstrzymane zadanie.
			S	Uruchomiono zadanie.
			U	Komenda CHGUSRTRC.
*JOBCHGUSR	JS	QASYJSJ5	M	Zmiana profilu lub profilu grupowego.

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
			T	Zmiana profilu lub profilu grupowego za pomocą tokenu profilu.
*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	Asynchroniczny proces sygnału i5/OS.
			P	Asynchroniczny sygnał środowiska PASE (Private Address Space Environment)został przetworzony.
	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	Połączenie odrzucone.
	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.

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
	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 kontroli klastra.
			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 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.
	SK	QASYSKJ4/J5	A	Akceptowanie
			C	Połączenie
			D	Przypisano adres DHCP
			F	Filtrowana poczta
			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

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
			D	Przypisano adres DHCP
			F	Filtrowana poczta
			R	Odrzucenie poczty
			U	Odmówiono adresu DHCP
*OBJMGT [2]	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	Kopia zapasowa zbioru lub katalogu
			S	Składowanie zawieszonego zbioru optycznego
			M	Przeniesienie pliku
	O3	QASY03JE/J4/J5	I	Inicjowanie woluminu
			B	Kopia zapasowa 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 wywołań.

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
			E	Program, który adoptuje uprawnienia właściciela, zakończył działanie. Kiedy program opuszcza stos wywołań, zapisywana jest pozycja zakończenia. Jeśli ten sam program wystąpi na stosie wywołań więcej niż jeden raz, pozycja zakończenia jest zapisywana, gdy najwyższe (ostatnie) wystąpienie programu opuści stos.
			A	Podczas aktywowania programu użyto uprawnienia adoptowanego.
*PGMFAIL	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 sprzętowej pamięci masowej.
			R	Próba zaktualizowania obiektu, który został zdefiniowany jako tylko do odczytu. (Rozszerzona ochrona sprzętowa pamięci masowej protokołowana jest tylko na poziomie ochrony 40 i wyższym)
*PRTDTA	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 [2]	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. [3]
	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. [3]
	RP	QASYRPJE/J4/J5	A	Odtworzony został program, który adoptuje uprawnienia właściciela.

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
	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 zmieniono kontrolę obiektu.
			U	Za pomocą komendy CHGUSRAUD zmieniono kontrolę użytkownika.
*SECCFG	AD	QASYADJE/J4/J5	D	Za pomocą komendy CHGDLOAUD zmieniono kontrolę biblioteki DLO.
			O	Za pomocą komendy CHGOBJAUD lub CHGAUD zmieniono kontrolę obiektu.
			S	Atrybut skanowania został zmieniony za pomocą komendy CHGATR, funkcji API Qp0lSetAttr albo podczas tworzenia obiektu.
			U	Za pomocą komendy CHGUSRAUD zmieniono kontrolę 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.

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
			C	Zmiana.
			D	Usunięcie.
			I	Inicjowanie przestrzeni zmiennej środowiskowej.
	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.
			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.
			E	Zmiana na opcję
			F	Zmiana na ogólnosystemowy atrybut kroniki
	VA	QASYVAJE/J4/J5	S	Lista kontroli dostępu została pomyślnie zmieniona.
			F	Zmiana listy kontroli dostępu nie powiodła się.
			V	Poprawna weryfikacja pozycji listy sprawdzania.
	VU	QASYVUJE/J4/J5	G	Rekord grupy został zmieniony.
			M	Zmieniono informacje globalne profilu użytkownika.
			U	Rekord użytkownika został zmieniony.
*SECDIRSRV	DI	QASYDIJE/J4/J5	AD	Zmiana kontroli.
			BN	Konsolidacja powiodła się
			CA	Zmiana uprawnień
			CP	Zmiana hasła

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
			OW	Zmiana prawa własności
			PO	Zmiana strategii
			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
			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.

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
	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 zostanie utworzony, jeśli nie soztał utworzony dla bieżącego zadania.)
			R	Pobrano deskryptor.
			U	Nie można użyć deskryptora.
*SECURITY	AD	QASYADJE/J4/J5	D	Za pomocą komendy CHGDLOAUD zmieniono kontrolę biblioteki DLO.
			O	Za pomocą komendy CHGOBJAUD lub CHGAUD zmieniono kontrolę obiektu.
			S	Atrybut skanowania został zmieniony za pomocą komendy CHGATR lub funkcji API Qp01SetAttr
			U	Za pomocą komendy CHGUSRAUD zmieniono kontrolę użytkownika.
	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
			PO	Zmiana strategii

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
			UB	Odłączanie powiodło się
	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.
			I	Inicjowanie przestrzeni zmiennej środowiskowej.
	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 zostanie utworzony, jeśli nie soztał 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.

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
	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	Utworzono uchwyt profilu poprzez API QSYGETPH.
			I	Wszystkie znaczniki profilu zostały unieważnione.
			M	Utworzono maksymalną dopuszczalną liczbę tokenów.
			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.
			E	Zmiana na opcję
			F	Zmiana na ogólnosystemowy atrybut kroniki
	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.

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
			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
			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	Utworzono uchwyt profilu poprzez API QSYGETPH.

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
			I	Wszystkie znaczniki profilu zostały unieważnione.
			M	Utworzono maksymalną dopuszczalną liczbę tokenów.
			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	Poprawna weryfikacja pozycji listy sprawdzania.
*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.
			S	Zbiór buforowy został zapisany.
			T	Zbiór buforowy został odtworzony.
			U	Zbiór buforowy został zmieniony.
			V	Zmianie uległy tylko te atrybuty zbiorów buforowych, które nie dotyczą bezpieczeństwa.
*SYSMGT	DI	QASYDIJ4/J5	CF	Zmiany konfiguracji
			CI	Tworzenie instancji
			DI	Usunięcie instancji
			RM	Zarządzanie replikacją
	SM	QASYSMJE/J4/J5	B	Opcje składowania zostały zmienione za pomocą xxxxxxxxxx.
			C	Opcje automatycznego czyszczenia zostały zmienione za pomocą xxxxxxxxxx.

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
			D	Dokonano zmiany DRDA*.
			F	Zmieniony został system plików HFS.
			N	Przeprowadzona została operacja na pliku sieciowym.
			O	Lista składowania została zmieniona za pomocą xxxxxxxxxx.
			P	Harmonogram włączania i wyłączania został zmieniony za pomocą xxxxxxxxxx.
			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	Zmiana obiektu
	ZC	QASYZCJ4/J5	C	Zmiany obiektu
			U	Aktualizowanie dostępu otwartego do obiektu
	AD	QASYADJEJ4/J5	D	Za pomocą komendy CHGOBJAUD zmieniono kontrolę obiektu.
			O	Za pomocą komendy CHGOBJAUD zmieniono kontrolę obiektu.
			S	Atrybut skanowania został zmieniony za pomocą komendy CHGATR lub funkcji API Qp01SetAttr
			U	Za pomocą komendy CHGUSRAUD zmieniono kontrolę 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.

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
	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[5]
	LD	QASYLDJE/J4/J5	L	Dowiązanie katalogu.
			U	Usunięcie dowiązania katalogu.
	VF	QASYVFJE/J4/J5	A	Plik został zamknięty z powodu odłączenia administracyjnego.
			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 [4]	CD	QASYCDJ4/J5	C	Uruchomiono komendę
	DI	QASYDIJ4/J5	EX	Eksportowanie katalogu LDAP
			ZR	Odczytano obiekt
	GR	QASYGRJ4/J5	F	Działania rejestrowania funkcji[5]
	LD	QASYLDJE/J4/J5	K	Przeszukiwanie katalogu.
	YR	QASYYRJE/J4/J5	R	Obiekt biblioteki dokumentów został odczytany.
	ZR	QASYZRJE/J4/J5	R	Obiekt został odczytany.

Tabela 132. Pozycje kroniki dotyczące kontroli bezpieczeństwa (kontynuacja)

Wartość kontroli działania lub obiektu	Typ pozycji kroniki	Plik zewnętrzny modelu bazy danych	Pozycja szczegółowa	Opis
[1] Ta wartość może być podana tylko dla parametru AUDLVL profilu użytkownika. Nie jest to wartość dla wartości systemowej QAUDLVL.				
[2] 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.				
[3] Informacje na temat możliwych zmian uprawnień w momencie odtworzenia obiektu znajdują się w temacie “Odtwarzanie obiektów” na stronie 257.				
[4] W przypadku ustawienia *ALL pozycje zapisywane są dla opcji *CHANGE i *ALL.				
[5] Kiedy kontrolowany jest obiekt QUSRSYS/QUSEXRGOBJ *EXITRG.				

Planowanie kontroli dostępu do obiektu

System operacyjny i5/OS zapewnia możliwość protokołowania dostępu do obiektu w kronice kontroli bezpieczeństwa, korzystając z wartości systemowych oraz wartości kontrolowania obiektu dla użytkowników i obiektów. Funkcja ta nosi nazwę *kontrolowanie 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 133 pokazuje, w jaki sposób współpracują ze sobą wartości OBJAUD dla obiektu i dla profilu użytkownika.

Tabela 133. Jak współdziałają funkcje kontrolowania obiektu i użytkownika

Wartość parametru OBJAUD dla obiektu	Wartość parametru OBJAUD dla użytkownika		
	***NONE**	***CHANGE**	***ALL**
*NONE	Brak	Brak	Brak
*USRPRF	Brak	Zmiana (Change)	Zmiana i użycie
*CHANGE	Zmiana (Change)	Zmiana (Change)	Zmiana (Change)
*ALL	Zmiana i użycie	Zmiana i użycie	Zmiana i użycie

Kontrolowanie obiektu można być używane do śledzenia wszystkich użytkowników, którzy uzyskują dostęp do krytycznego obiektu w systemie. Można również używać tej funkcji do śledzenia wszystkich obiektów, do których uzyskuje dostęp określony użytkownik. 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 zaplanowana kontrola może spowodować powstanie większej liczby rekordów kontroli, niż użytkownik jest w stanie przeanalizować. Może to mieć poważny wpływa 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 istnieją zbiory krytyczne wykorzystywane przez całą firmę użytkownika, to można sprawdzić, kto uzyskuje dostęp do tych plików i kiedy, za pomocą następującej techniki:
  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)

Podaj wybrane opcje i naciśnij klawisz 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 technik opisanych w sekcji “Analizowanie pozycji kroniki kontroli za pomocą zapytania lub programu” na stronie 306, przeanalizuj pozycje kroniki kontroli.

- Jeśli mają znaczenie informacje o użytkowniku używającym danego zbioru, można zebrać informacje o wszystkich uzyskanych dostępach 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. Sprawdź, czy 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 zapytania lub programu” na stronie 306 przeanalizuj pozycje kroniki kontroli.
- Aby skontrolować wszystkie próby uzyskania dostępu przez wybranego użytkownika, należy wykonać następujące czynności:
  1. Ustawić wartość OBJAUD dla wszystkich obiektów na *USRPRF używając do tego komend CHGOBJAUD oraz CHGAUD:

```
                    Zmiana kontroli obiektu (Change Object Auditing - CHGOBJAUD)

Podaj wybrane opcje i naciśnij klawisz Enter.

Obiekt . . . . . . . . . . . . .   *ALL
  Biblioteka  . . . . . . . . . .  *ALLAVL
Typ obiektu  . . . . . . . . . . *ALL
Urządzenie ASP. . . . . . . . . .   *
Wartość kontroli obiektu . . . . .   *USRPRF
```

     Ważne: W zależności od ilości obiektów w systemie, uruchomienie tej komendy może potrwać 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.

Odsyłacze pokrewne

“Kontrolowanie obiektu” na stronie 114
Wartość kontrolowania obiektu dla profilu użytkownika współpracuje z wartością kontrolowania obiektu dla obiektu, w celu określenia, czy użytkownik ma dostęp do kontrolowanego obiektu.

Wyświetlanie poziomu 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 domyślnej kontroli dla obiektów:

Za pomocą wartości systemowej QCRTOBJAUD i wartości CRTOBJAUD dla bibliotek i katalogów, można skonfigurować 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. Niewłaściwe ich użycie może spowodować powstanie wielu niepożądanych pozycji w kronice kontroli ochrony. Efektywne używanie możliwości kontrolowania obiektu wymaga ostrożnego planowania.

Zapobieganie utracie informacji o kontrolowaniu

Dwie wartości systemowe sterują działaniem systemu w sytuacjach, gdy stan wywołany błędem może spowodować utratę pozycji kroniki kontroli.

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 wyborem jest wartość *SYS.

Niskie poziomy wymuszenia minimalizują możliwość utracenia rekordów kontroli, ale powodują obniżenie wydajności 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 Działanie zakończenia kontroli (Auditing End Action - QAUDENDACN) określa działanie systemu, gdy nie jest możliwe zapisanie pozycji w kronice kontroli.

Wartością domyślną jest *NOTIFY. W razie braku możliwości zapisu pozycji w kronice kontroli i przy ustawionej wartości systemowej QAUDENDACN na wartość *NOTIFY system wykonuje 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 jest w stanie zapisać pozycji kroniki kontroli, a wartość systemowa QAUDENDACN ustawiona jest na *PWRDWNSYS, może dojść do następujących sytuacji:

1. Następuje natychmiastowe wyłączenie systemu (równoważne z wprowadzeniem 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, należy wpisać się do konsoli jako użytkownik z uprawnieniami specjalnymi *ALLOBJ i *AUDIT.

   System uruchamia się w stanie zastrzeżonym z komunikatem wskazującym, że zatrzymanie systemu spowodował błąd kontroli.
3. Wartość systemowa QAUDCTL ustawiona jest na *NONE.
4. 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. Należy usunąć przyczynę problemu i wykonać reset wartości QAUDCTL.

Niekontrolowanie obiektów QTEMP

Użytkownik może zdecydować o niekontrolowaniu obiektów QTEMP, określając wartość *NOQTEMP.

Wartość *NOQTEMP może być podana jako wartość dla wartości systemowej QAUDCTL. Jeśli zostanie użyta wartość *NOQTEMP, należy również określić wartość *OBJAUD lub *AUDLVL dla wartości systemowej QAUDCTL. Jeśli kontrolowanie jest włączone i określono parametr *NOQTEMP, następujące czynności z biblioteki QTEMP nie będą kontrolowane.

- 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 bezpieczeństwa

Przegląd:

za pomocą komendy CHGSECAUD użytkownik może uruchomić kontrolę ochrony systemu dla działań, poprzez upewnienie się, że kronika ochrony istnieje, wartość systemowa QAUDCTL ustawiona jest na wartość *AUDLVL, a wartość QAUDLVL ustawiona jest na domyślne wartości. Domyślne wartości to kontrole działań *AUTFAIL, *CREATE, *DELETE, *SECURITY, oraz *SAVRST.

```
CHGSECAUD QAUDCTL(*AUDLVL) QAUDLVL(*DFTSET)
```

Przeznaczenie:
Konfiguruje system do zbierania zdarzeń ochrony w kronice QAUDJRN.

Sposób używania:

CHGSECAUD
DSPSECAUD

Uprawnienia:

Użytkownik musi mieć uprawnienia specjalne *ALLOBJ i *AUDIT.

Pozycja kroniki:

CO (tworzenie obiektu),
SV (zmiana wartości systemowej),
AD (zmiany kontroli obiektu i użytkownika).

Uwaga:
Komenda CHGSECAUD tworzy kronikę oraz dziennik, jeśli nie istnieją. Następnie ustawia wartości systemowe QAUDCTL, QAUDLVL i QAUDLVL2.

Odsyłacze pokrewne

"Opcje menu Narzędzia bezpieczeństwa" na stronie 735
Menu Narzędzia bezpieczeństwa (Security Tools - SECTOOLS) upraszcza zarządzanie bezpieczeństwem systemu oraz kontrolę nad nim dzięki dużej liczbie udostępnianych opcji i komend.

Konfigurowanie kontroli bezpieczeństwa

Kontrola bezpieczeństwa pozwala zebrać w kronice QAUDJRN informacje o zdarzeniach związanych z bezpieczeństwem.

Przegląd:

Przeznaczenie:
Konfiguruje system do zbierania zdarzeń związanych z bezpieczeństwem w kronice QAUDJRN.

Sposób używania:

CRTJRNRCV
CRTJRN QSYS/QAUDJRN
WRKSYSVAL *SEC
CHGOBJAUD
CHGDLOAUD
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 będzie mogła być zmieniona, musi istnieć kronika QSYS/QAUDJRN, w przeciwnym razie funkcja kontroli systemu nie będzie znała nazwy kroniki i nie jej nie znajdzie.

Aby skonfigurować kontrolę ochrony, należy wykonać następujące czynności. Do wykonania tych czynności niezbędne jest uprawnienie specjalne *AUDIT.

1. Utwórz dziennik w wybranej bibliotece komendą Tworzenie dziennika (Create Journal Receiver - CRTJRNRCV). Ten przykład korzysta z biblioteki JRNLIB.

   ```
   CRTJRNRCV  JRNRCV(JRNLIB/AUDRCV0001) +
              THRESHOLD(100000) AUT(*EXCLUDE)   +
              TEXT('Dziennik kontroli')
   ```

   a. Umieść dziennik w bibliotece, która jest regularnie składowana. Dziennika **nie** należy umieszczać w bibliotece QSYS, nawet jeśli jest to miejsce docelowe kroniki.

   b. 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.

      Korzystanie z tego typu konwencji nazewnictwa jest bardzo pomocne, jeśli system ma zarządzać zmianami dzienników.

   c. 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 użytkownik skorzysta z systemowej funkcji zmiany kroniki, próg dziennika powinien wynosić przynajmniej 100 000 KB. Więcej informacji na temat progu dziennika znajduje się w temacieZarządzanie kroniką.

   d. Aby ograniczyć dostęp do informacji przechowywanych w kronice, dla parametru AUT należy podać wartość *EXCLUDE.

2. Utwórz kronikę QSYS/QAUDJRN komendą Tworzenie kroniki (Create Journal - CRTJRN):

   ```
   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 próg podany podczas tworzenia dziennika, użyj 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 upewnić się, że zostały odpowiednio zeskładowane.

   Więcej informacji dotyczących pracy z kronikami oraz dziennikami zawiera temat Zarządzanie kroniką.

3. Ustaw wartość systemową poziomu kontroli (QAUDLVL) lub wartość systemową rozszerzenia poziomu kontroli (QAUDLVL2) komendą WRKSYSVAL. Wartości systemowe QAUDLVL i QAUDLVL2 określają, jakie działania użytkowników systemu protokołowane są w kronice kontroli. Patrz “Planowanie kontroli działań” na stronie 271.
4. W razie potrzeby ustaw kontrolowanie działań dla poszczególnych użytkowników komendą CHGUSRAUD. Patrz “Planowanie kontroli działań” na stronie 271.
5. W razie potrzeby ustaw kontrolowanie obiektów dla poszczególnych obiektów komendami CHGOBJAUD, CHGAUD i CHGDLOAUD. Patrz “Planowanie kontroli dostępu do obiektu” na stronie 296.
6. W razie potrzeby ustaw kontrolowanie obiektow dla poszczególnych użytkowników komendą CHGUSRAUD.
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 298.
8. Ustaw wartość systemową QAUDFRCLVL, aby kontrolować, jak często w pamięci dyskowej zapisywane są rekordy kontroli. Patrz “Zapobieganie utracie informacji o kontrolowaniu” na stronie 298.
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 nie powiedzie się, wyświetlony zostanie komunikat, a kontrolowanie nie zostanie rozpoczęte.

Zarządzanie kroniką kontroli oraz dziennikami

W systemie dostępny jest mechanizm zarządzania kroniką kontroli i dziennikami. Metody opisane w tej sekcji umożliwiają wykonywanie kontroli bezpieczeństwa w systemie.

Kronika kontroli QSYS/QAUDJRN jest przeznaczona wyłącznie do kontroli bezpieczeństwa. 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).

W systemie stosowana jest specjalna blokada, aby zagwarantować zapisywanie pozycji kontroli w kronice kontroli. 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:

- DLTJRN, komenda
- przenoszenie kroniki,
- odtwarzanie kroniki,
- WRKJRN, komenda

Informacje zapisane w pozycjach kroniki ochrony opisano w sekcji Dodatek F, “Układ pozycji kroniki kontroli”, na stronie 581. 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.

Użytkownik może zażyczyć sobie, aby system 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. Działanie to jest nazywane *systemowym zarządzaniem zmiany kroniki*.

Jeśli dla kroniki QAUDJRN została określona wartość MNGRCV(*USER), po osiągnięciu progu pamięci przez dziennik do kolejki komunikatów progu, określonej dla kroniki, jest wysyłany komunikat. Komunikat informuje, że dziennik osiągnął swój próg. Należy wtedy odłączyć dziennik i podłączyć nowy za pomocą komendy CHGJRN. Zapobiega to powstaniu warunku błędu *pozycja nie została zakronikowana*. Jeśli ten komunikat zostanie wyświetlony, w celu kontynuowania kontroli bezpieczeństwa należy użyć komendy CHGJRN.

Domyślną kolejką komunikatów dla kroniki jest kolejka QSYSOPR. Jeśli kolejka komunikatów QSYSOPR w danej instalacji zawiera większą ilość komunikatów, można powiązać z kroniką QAUDJRN inną kolejkę komunikatów, jak np. 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. Monitorowanie wystąpienia tego komunikatu umożliwia określenie, kiedy należy składować odłączone dzienniki kontroli.

Ważne: Funkcja czyszczenia automatycznego udostępniana przez menu Asysty Operacyjnej nie usuwa zawartości dzienników QAUDJRN. Aby uniknąć problemów związanych z przestrzenią dyskową, należy regularnie odłączać, składować i usuwać dzienniki QAUDJRN.

Sekcja Zarządzanie kroniką zawiera więcej szczegółowych informacji o zarządzaniu kronikami i dziennikami.

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.

Informacje pokrewne

Zarządzanie kronikami

Składowanie i usuwanie dzienników z kronikami kontroli

Bieżący dziennik kroniki kontroli należy regularnie odłączać i przyłączać nowy.

Przegląd:

Przeznaczenie:
Przyłączanie nowego dziennika kroniki kontroli; składowanie i usuwanie poprzedniego dziennika

Sposób używania:
- CHGJRN QSYS/QAUDJRN JRNRCV(*GEN)
- 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 powodować spadek wydajności systemu, a poza tym zajmują cenne miejsce na pamięci dyskowej.

Zalecane jest wdrożenie automatycznego zarządzania dziennikami w systemie. Można to określić przez podanie parametru *Zarządzanie dziennikami* podczas tworzenia kroniki.

Jeśli użytkownik skonfiguruje kontrolowanie działań i obiektów tak, aby protokołowały wiele różnych zdarzeń, możliwe, że konieczne będzie ustawienie wysokiej wartości dla progu dziennika. Jeśli użytkownik zarządza dziennikami ręcznie, możliwe, że konieczna będzie zmiana dzienników kilka razy dziennie. Jeśli protokołowanych jest tylko kilka zdarzeń, to warto ustawić dzienniki tak, aby zgadzały się z harmonogramem kopii zapasowych dla biblioteki zawierającej dziennik.

Do odłączania dziennika i przyłączania nowego służy komenda CHGJRN.

Dzienniki zarządzane przez system:

Aby składować lub usunąć dzienniki, postępuj zgodnie z instrukcjami przedstawionymi poniżej.

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 odpowiadającego im statusu.
3. Aby składować dzienniki, użyj komendy SAVOBJ. Nie należy składować aktualnie podłączonego dziennika.
4. Za pomocą komendy DLTJRNRCV usuń każdy zeskładowany dziennik.

Inną możliwością jest użycie kolejki komunikatów kroniki i monitorowanie jej w oczekiwaniu na komunikat CPF7020, oznaczający, że zmiana kroniki przez system zakończyła się sukcesem.

Informacje pokrewne

Składowanie i odtwarzanie

Dzienniki zarządzane przez użytkowników:

Aby samodzielnie odłączyć, składować lub usunąć dzienniki, wykonaj opisane poniżej czynności.

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. Przy próbie usunięcia dziennika bez jego składowania zostanie wyświetlony komunikat ostrzegawczy.

Zatrzymywanie funkcji kontroli

Użytkownik może chcieć korzystać z funkcji kontroli od czasu do czasu, zamiast bez przerwy. Na przykład można jej używać podczas testowania nowej aplikacji. Lub podczas wykonywania kwartalnej kontroli ochrony.

Aby zatrzymać funkcję kontroli, należy wykonać następujące czynności:

1. Użyj komendy WRKSYSVAL, aby zmienić wartość systemową QAUDCTL na *NONE. Zatrzyma to protokołowanie przez system zdarzeń ochrony.
2. Odłącz bieżący dziennik komendą CHGJRN.
3. Zeskładuj i usuń odłączony dziennik komendami SAVOBJ i DLTJRNRCV.
4. Kronikę QAUDJRN można usunąć po ustawieniu wartości QAUDCTL na *NONE. Jeśli planujesz przywrócić w przyszłości kontrolę bezpieczeństwa, pozostaw kronikę QAUDJRN w systemie.

   Jeśli kronika QAUDJRN jest skonfigurowana z wartością MNGRCV(*SYSTEM), system będzie odłączał dziennik i przyłączał nowy przy każdym wykonaniu IPL gdy kontrola bezpieczeństwa jest aktywna. Te dzienniki należy usunąć. Zapisanie ich przed usunięciem nie jest konieczne, ponieważ nie zawierają one wpisów kontroli.

Analizowanie pozycji kroniki kontroli

Po skonfigurowaniu funkcji kontroli bezpieczeństwa użytkownik może skorzystać z kilku metod w celu analizy zaprotokołowanych zdarzeń.

- Wyświetlanie wybranych pozycji na stacji roboczej użytkownika za pomocą komendy Wyświetlenie kroniki (Display Journal - DSPJRN).
- Kopiowanie wybranych pozycji do zbiorów wyjściowych za pomocą komendy Kopiowanie pozycji kroniki kontroli (Copy Audit Journal Entries - CPYAUDJRNE) lub komendy DSPJR, a następnie analiza pozycji za pomocą narzędzia zapytań lub programu do analizowania pozycji.
- Użycie komendy Wyświetlenie pozycji kroniki kontroli (Use the Display Audit Journal Entries - DSPAUDJRNE).

  Uwaga: Firma IBM nie dostarcza już rozszerzeń dla komendy DSPAUDJRNE. Nie jest w stanie przetworzyć wszystkich typów rekordów kontroli ochrony i nie wyświetla wszystkich pól dla rekordów, które obsługuje.
- Używanie komendy Pobranie pozycji kroniki (Receive Journal Entry - RCVJRNE) dla kroniki QAUDJRN w celu pobierania pozycji podczas ich zapisywania do kroniki QAUDJRN.

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 wyświetlić 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 . . . . . :                  Biblioteka . . . . . :
Podzbiór . . . . . :
Niekompletne dane. . :   Nie      Zminimalizowane dane wejściowe : *None
Sekwencja. . . . . :   1198
Kod  . . . . . :   T  - Pozycja zapisu kontrolnego
Typ. . . . . :   CO - Tworzenie obiektu

            Dane specyficzne dla pozycji
Kolumna     *...+....1....+....2....+....3....+....4....+....5
00001      'NISAVLDCK  QSYS      *PGM    CLE                  '
00051      '                                                  '
00101      '                                                  '
00151      '                                                  '
00201      '                                                  '
00251      '                                                  '
00301      '                                                  '

                                                                 Więcej...
Aby kontynuować, naciśnij klawisz Enter.

F3=Wyjdź   F6=Wyświetlenie tylko danych dotyczących pozycji
F10=Wyświetlenie szczegółów pozycji    F12=Anuluj    F24=Inne klawisze
```

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, “Układ pozycji kroniki kontroli”, na stronie 581 zawiera układ dla każdego typu pozycji kroniki QAUDJRN.

Analizowanie pozycji kroniki kontroli za pomocą zapytania lub programu

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 dla QSYS/QAUDJRN, uprawnienia *USE dla dziennika, oraz uprawnienia *ADD dla biblioteki 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)

Podaj wybrane opcje i naciśnij klawisz Enter.
⋮
Wyjście . . . . . . . . . . . . . > *OUTFILE
Format zbioru wyjściowego  . . . *TYPE5
Zbiór wyjściowy do zapisania . . dspjrnout
  Biblioteka . . . . . . . . . . .     mojabiblioteka
Opcje podzbioru wyjściowego:
  Podzbiór wyjściowy . . . . . . *FIRST
  Zastąp. 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. QADSPJR5 (o formacie rekordu QJORDJE5) służy do definiowania tych pól w momencie nadania parametrowi formatu zbioru wyjściowego wartość *TYPE5. Więcej informacji na ten temat zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581.

Więcej informacji na temat innych rekordów i ich formatach zbiorów wyjściowych zawiera Dodatek F, “Układ pozycji kroniki kontroli”, na stronie 581.

Jeśli ma być przeprowadzona szczegółowa analiza danego typu pozycji, należy użyć jednego z udostępnionych modelowych zbiorów wyjściowych bazy danych. Tabela 132 na stronie 278 zawiera nazwę zbioru wyjściowego bazy danych modeli dla każdego typu pozycji. Dodatek F, “Układ pozycji kroniki kontroli”, na stronie 581 zawiera układy wszystkich zbiorów wyjściowych bazy danych modeli.

Na przykład, aby utworzyć zbiór wyjściowy o nazwie AUDJRNAF5 w QGPL, zawierający tylko wpisy o błędach 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. użyj programu lub zapytania w celu przeanalizowania informacji w zbiorze AUDJRNAF5.

Oto przykłady wykorzystania informacji 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 132 na stronie 278 pokazuje, jakie pozycje kroniki są zapisywane dla każdego komunikatu o naruszeniu uprawnień.

Związek godziny/daty modyfikacji obiektu z rekordami kontroli

Raporty zapisywane w celu wykrycia modyfikacji w programach lub innych obiektach, często bazują na polu data/godzina modyfikacji obiektu, zamiast na informacjach z kroniki kontroli ochrony. Poniższa lista zawiera główne powody, dla jakich mogą występować różnice pomiędzy datą dla obiektu i datą dla jego źródła.

- Użyto komendy CHGPGM w celu wymuszenia odtworzenia programu, aby zaktualizować pole Data/godzina modyfikacji (Change Date/Time) tego programu. Operacja ta zapisuje rekord kontroli ZC (Modyfikacja obiektu).
- Program lub komenda zostały cyfrowo podpisane za pomocą funkcji API Podpis obiektu (Sign Object - QYDOSGNO), aby zaktualizować ich pole Data/godzina modyfikacji (Change Date/Time). Operacja ta zapisuje rekord kontroli ZC.

System operacyjny może również automatycznie zaktualizować pole data/godzina modyfikacji obiektu w następujących sytuacjach:

- Jeśli profil użytkownika posiada uprawnienia prywatne do obiektu, a obiekt zostanie usunięty, system aktualizuje pole data/godzina modyfikacji tego profilu użytkownika i usuwa te uprawnienia prywatne.
- Jeśli kontrola ochrony jest włączona w momencie usunięcia obiektu, zapisywany jest rekord kontroli DO (Operacja usunięcia) dla usuniętego obiektu.
- Ponieważ system automatycznie aktualizuje każdy profil użytkownika posiadający uprawnienia prywatne do usuniętego obiektu, dla tych profili użytkowników nie są zapisywane rekordy kontroli, pomimo aktualizacji ich pól data/godzina modyfikacji.

Posługując się kroniką kontroli ochrony można śledzić wykorzystywanie przez użytkowników normalnych interfejsów systemowych do zmian obiektów. Raporty wykrywania zmian w obiektach opierane są wyłącznie na polach daty/godziny modyfikacji obiektów i dają niepełne rezultaty.

Dlaczego nie należy korzystać z pola Data/godzina (Date/Time) do celów ogólnej kontroli bezpieczeństwa

Główną wskazówką dotyczącą tego, co powinno być kontrolowane w systemie i5/OS jest kontrolowanie działań użytkowników związanych z ochroną. Drugą wskazówką jest nie zapisywanie rekordów kontroli dla działań wykonywanych przez system automatycznie. W niektórych przypadkach, operacje automatyczne nie mogą być kontrolowane, jeśli system wykonuje operację za pomocą funkcji, z której mogą również korzystać użytkownicy.

Cele utrzymywania pola daty/godziny modyfikacji dla obiektu różnią się od celów kontroli. Głównym zadaniem pola daty/godziny jest zaznaczanie ostatniej modyfikacji zbioru. Zaktualizowane pole godziny/daty modyfikacji nie określa, co zostało zmienione w obiekcie ani też kto dokonał zmian. Jedną z głównych funkcji tego pola jest określenie, czy obiekt powinien zostać zapisany przez komendę Składowanie zmienionych obiektów (Save Changed Objects - SAVCHGOBJ). Komenda ta nie sprawdza, kiedy dokonano zmian. Sprawdza wyłącznie czy obiekt został zmieniony od czasu jego ostatniego składowania. Opcja ta pozwala na optymalizację wydajności zbiorów baz danych. Pole data/godzina modyfikacji aktualizowane jest tylko po pierwszej modyfikacji zbioru po jego ostatnim składowaniu. Aktualizowanie pola z datą i godzina modyfikacji przy każdej aktualizacji, dodaniu, lub usunięciu rekordu w zbiorze mogłoby mieć negatywny wpływ na wydajność systemu.

Inne techniki monitorowania bezpieczeństwa

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 bezpieczeństwa”, na stronie 735. Ta sekcja zawiera przykłady użycia komend oraz informacje dotyczące menu dla narzędzi serwisowych.

Monitorowanie komunikatów dotyczących bezpieczeństwa

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

W protokole QHST nie są zapisywane wszystkie komunikaty o błędach uprawnień ani naruszeniach integralności. Komunikaty te zostaly wymienione tutaj.

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 wydania 3 programu licencjonowanego i5/OS, niektóre komunikaty błędów uprawnień i integralności nie są wysyłane do protokołuQHST (historia). 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.
- CPF2220. Te zdarzenia mogą być przechwycone w kronice kontroli, przez podanie parametru *AUTFAIL dla wartości systemowej QAUDLVL.
- CPF4AAE. Te zdarzenia mogą być przechwycone w kronice kontroli, przez podanie parametru *AUTFAIL dla wartości systemowej QAUDLVL.
- CPF2246. 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 w systemie, warto wyświetlić bardziej szczegółowe informacje na temat dostępu i zmian do konkretnych danych. Kronikowanie obiektu może udostępnić takie szczegóły. Podstawową funkcją kronikowania obiektu jest zapewnienie jego integralności oraz możliwości odzyskania. Lista obiektów, które mogą być kronikowane i informacje o tym, co jest kronikowane dla każdego typu obiektu znajdują się w temacie Zarządzanie kroniką. W celu przeglądania zmian obiektu, te pozycje kroniki mogą być używane także przez osobę odpowiedzialną za bezpieczeństwo 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 dotyczące otwierania obiektu, zamykania go, modyfikacji, składowania, usuwania itp.

Pozycja kroniki nie może być zmieniona przez żadnego użytkownika, nawet przez osobę odpowiedzialną za bezpieczeństwo. Cała kronika lub dziennik może zostać usunięta, ale jest to łatwe do wykrycia.

W przypadku kronikowania zbioru bazy danych, obszaru danych, kolejki danych, biblioteki lub obiektu zintegrowanego systemu plików można użyć komendy DSPJRN w celu wydrukowania wszystkich zmian dotyczących danego obiektu. Oto kilka przykładów:

```
| Wpisz następującą komendę dla pewnego zbioru bazy danych.
| DSPJRN JRN(biblioteka/kronika) +
|        FILE(biblioteka/zbiór) OUTPUT(*PRINT)
|
| Wpisz następującą komendę dla pewnego obszaru danych.
| DSPJRN JRN(biblioteka/kronika) +
|        OBJ((biblioteka/nazwa_obiektu *DTAARA))  OUTPUT(*PRINT)
|
| Wpisz następującą komendę dla pewnej kolejki danych.
| DSPJRN JRN(biblioteka/kronika) +
|        OBJ((biblioteka/nazwa_obiektu *DTAQ)  OUTPUT(*PRINT)
|
| Wpisz następującą komendę dla pewnego obiektu zintegrowanego systemu plików.
| DSPJRN JRN(biblioteka/kronika) +
|        OBJPATH(('nazwa_ścieżki')) OUTPUT(*PRINT)
|
| Wpisz następującą komendę dla danej biblioteki.
| DSPJRN JRN(biblioteka/kronika) +
|        OBJ(*LIBL/nazwa-biblioteki *LIB) OUTPUT(*PRINT)
```

Na przykład jeśli do zapisywania informacji dotyczących zbioru CUSTFILE (z biblioteki CUSTLIB) wykorzystywana jest kronika JRNCUST z biblioteki CUSTLIB, komenda może wyglądać następująco:

```
DSPJRN JRN(CUSTLIB/JRNCUST) +
       FILE(CUSTLIB/CUSTFILE) OUTPUT(*PRINT)
```

Można również utworzyć zbiór wyjściowy i wysłać zapytanie, lub użyć SQL w celu zaznaczenia wszystkich rekordów ze zbioru wyjściowego w celu uzyskania konkretnych danych wyjściowych.

Wpisz następującą komendę, aby utworzyć zbiór wyjściowy dla konkretnego zbioru bazy danych.

```
DSPJRN JRN(biblioteka/kronika) +
                   FILE(biblioteka/nazwa_zbioru) +
               OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(biblioteka/zbiór_wyjściowy) ENTDTALEN(*CALC)
```

Wpisz następującą komendę, aby utworzyć zbiór wyjściowy dla konkretnego obszaru danych.

```
DSPJRN JRN(biblioteka/kronika) +
                   OBJ((biblioteka/nazwa_obiektu *DTAARA)) +
               OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(biblioteka/zbiór_wyjściowy) ENTDTALEN(*CALC)
```

Wpisz następującą komendę, aby utworzyć zbiór wyjściowy dla konkretnej kolejki wyjściowej.

```
DSPJRN JRN(biblioteka/kronika) +
                   OBJ((biblioteka/nazwa_obiektu *DTAQ)) +
               OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(biblioteka/zbiór_wyjściowy) ENTDTALEN(*CALC)
```

Wpisz następującą komendę, aby utworzyć zbiór wyjściowy dla konkretnego obiektu zintegrowanego systemu plików.

```
DSPJRN JRN(biblioteka/kronika) +
                   OBJPATH(('nazwa_ścieżki')) +
               OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(biblioteka/zbiór_wyjściowy) ENTDTALEN(*CALC)
```

Wpisz następującą komendę, aby utworzyć zbiór wyjściowy dla konkretnej biblioteki.

```
DSPJRN JRN(biblioteka/kronika) +
                   OBJ((*LIBL/nazwa-biblioteki *LIB)) +
               OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(biblioteka/zbiór_wyjściowy) ENTDTALEN(*CALC)
```

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).

Informacje pokrewne

Zarządzanie kronikami

Analizowanie profili użytkowników

Za pomocą komendy Wyświetlenie uprawnionych użytkowników (Display Authorized Users - DSPAUTUSR) można wyświetlić lub wydrukować pełną listę użytkowników w systemie.

Lista może być posortowana według nazwy profilu lub profilu grupowego. Oto przykład sekwencji profilu grupowego.

```
                          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       Sprzedaż i marketing
            DPTWH     08/13/0x    X       Warehouse
            RICHARDS  09/05/0x            Janet Richards
            SMITHJ    09/18/0x            John Smith
```

Drukowanie wybranych profili użytkowników

Komendą Wyświetlenie profilu użytkownika (Display User Profile - DSPUSRPRF) można utworzyć zbiór wyjściowy, a następnie przetwarzać go narzędziem do 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 posiadające uprawnienia specjalne poprzez zaznaczenie rekordów, dla których pole UPSPAU posiada wartość inną niż *NONE.
- wyświetlić wszystkich użytkowników mogących wprowadzać komendy poprzez zaznaczenie wszystkich rekordów, dla których pole *Ograniczenie możliwości* (nazywane UPLTCP w zbiorze wyjściowym bazy danych modeli) posiada wartość *NO lub *PARTIAL.
- wyświetlać wszystkich użytkowników z określonym menu lub programem początkowym,
- wyświetlać użytkowników nieaktywnych na podstawie pola z datą ostatniego wpisania się,
- wyświetlić wszystkich użytkowników nie posiadających haseł zgodnych z poziomem hasła 0 oraz 1 poprzez zaznaczenie rekordów, dla których pole Obecne hasło dla poziomu 0 lub 1 (nazywane UPENNPW w zbiorze wyjściowym modelu) posiada wartość N.
- wyświetlić wszystkich użytkowników posiadających hasła zgodne z poziomem hasła 2 oraz 3 poprzez zaznaczenie rekordów, dla których pole Obecne hasło dla poziomu 2 lub 3 (nazywane UPENNPW w zbiorze wyjściowym modelu) posiada wartość Y.

Badanie dużych profili użytkowników

Jeśli w systemie występują duże profile użytkowników, wskazane jest sprawdzenie efektywności ochrony. Przypadkowo rozmieszczone w systemie profile użytkowników o dużej liczbie uprawnień są oznaką źle zaplanowanej ochrony.

Jedna z metod znajdowania dużych profili użytkowników i ich oceniania jest przedstawiona poniżej.

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)
   ```

   Uwaga: Katalogi i obiekty oparte na katalogach nie są drukowane. Komendy WRKOBJOWN i WRKOBJPVT mogą zostać wykorzystane do wyświetlenia obiektów opartych o biblioteki i katalogi, ale nie posiadają one funkcji drukowania.

   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”.

   Odsyłacze pokrewne

   Dodatek B, “Profile użytkowników IBM”, na stronie 329
   Ta sekcja 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.

Analizowanie uprawnień do obiektów i bibliotek

Można kontrolować uprawnienia do obiektów i bibliotek w systemie.

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. Programy te mogą być analizowane w celu kontroli bezpieczeństwa systemu.

Za pomocą poniższej metody można wyszukać i sprawdzić programy, które adoptowały uprawnienia:

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 312 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)
```

   Uwaga: Może wystąpić konieczność, aby parametr typu obiektu miał wartość *PGM, *SQLPKG, lub *SRVPGM, w zależności od raportu DSPPGMADP.

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. Aplikacje korzystające z uprawnień adoptowanych błędów programów mogą być projektowane przy użyciu 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)
```

   Uwaga: Może wystąpić konieczność, aby parametr typu obiektu miał wartość *PGM, *SQLPKG, lub *SRVPGM, w zależności od raportu DSPPGMADP.

Sprawdzanie pod kątem zmodyfikowanych obiektów

Zmodyfikowany obiekt często wskazuje, że jakiś użytkownik próbował zmienić dane w systemie. Za pomocą komendy Sprawdzenie integralności obiektu (Check Object Integrity - CHKOBJITG) można sprawdzić obiekty, które zostały zmodyfikowane.

Komendy warto użyć podczas 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. Użytkownik może szukać obiektów, których domena została zmieniona i obiektów zmodyfikowanych. 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. Użytkownik może uruchomić skanowanie zintegrowanego systemu plików lub sprawdzić, czy obiekty zwracały błędy podczas poprzedniego skanowania zintegrowanego systemu plików.

Uruchomienie komendy CHKOBJITG wymaga posiadania specjalnych uprawnień *AUDIT. Wykonywanie komendy może trwać przez długi czas, ze względu na skanowania i obliczenia, jakie są przez nią wykonywane. Dlatego należy ją uruchamiać przy małym obciążeniu systemu.Większość komend IBM zduplikowanych z wydań wcześniejszych niż V5R2 będzie protokołowanych jako naruszenia. Komendy te powinny zostać usunięte i ponownie utworzone za pomocą komendy Tworzenie duplikatu obiektu (Create Duplicate Object - CRTDUPOBJ) przy każdym ładowaniu nowego wydania.

Informacje pokrewne

Obsługa skanowania

Sprawdzanie systemu operacyjnego

Użytkownik może skorzystać z API Sprawdzanie systemu (QYDOCHKS) w celu sprawdzenia, czy kluczowe obiekty systemu zostały zmienione od momentu ich podpisania.

Każdy obiekt, który nie został podpisany lub został zmieniony od momentu jego podpisania zwróci błąd. Za poprawne uznawane są tylko podpisy z zaufanych źródeł.

Uruchomienie funkcji API QYDOCHKS wymaga uprawnień specjalnych *AUDIT. Uruchomienie API może długo potrwać, ze względu na obliczenia, jakie są przez nią wykonywane. Dlatego należy ją uruchamiać przy małym obciążeniu systemu.

Odsyłacze pokrewne

Funkcja API Sprawdzanie systemu (Check System - QYDOCHKS)

Kontrola działań osoby odpowiedzialnej za bezpieczeństwo

Zapisy wszystkich działań wykonywanych przez użytkowników z uprawnieniami specjalnymi *ALLOBJ oraz *SECADM mogą zostać zachowane w celu śledzenia.

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 osoby odpowiedzialnej za bezpieczeństwo:

   ```
   CHGUSRAUD USER(SECUSER) +
             AUDLVL(*CMD *CREATE *DELETE +
                    *OBJMGT *OFCSRV *PGMADP +
                    *SAVRST *SERVICE, +
                    *SPLFDTA *SYSMGT)
   ```

   “Kontrola działań” na stronie 115 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.

   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 zapytania lub programu” na stronie 306.

Rozdział 10. Licencja na kod oraz Informacje dotyczące kodu

IBM udziela niewyłącznej licencji na prawa autorskie, stosowanej przy używaniu wszelkich przykładowych kodów programów, na podstawie których można wygenerować podobne funkcje dostosowane do indywidualnych wymagań.

Z ZASTRZEŻENIEM GWARANCJI WYNIKAJĄCYCH Z BEZWZGLĘDNIE OBOWIĄZUJĄCYCH PRZEPISÓW PRAWA, IBM, PROGRAMIŚCI ANI DOSTAWCY IBM NIE UDZIELAJĄ NA NINIEJSZY PROGRAM ANI W ZAKRESIE EWENTUALNEGO WSPARCIA TECHNICZNEGO ŻADNYCH GWARANCJI, W TYM TAKŻE RĘKOJMI, NIE USTALAJĄ ŻADNYCH WARUNKÓW, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI CZY WARUNKÓW PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CZY NIENARUSZANIA PRAW STRON TRZECICH.

W ŻADNYCH OKOLICZNOŚCIACH IBM, ANI TEŻ PROGRAMIŚCI CZY DOSTAWCY PROGRAMÓW IBM, NIE PONOSZĄ ODPOWIEDZIALNOŚCI ZA PONIŻSZE SZKODY, NAWET JEŚLI ZOSTALI POINFORMOWANI O MOŻLIWOŚCI ICH WYSTĄPIENIA:

1. UTRATA LUB USZKODZENIE DANYCH;
2. SZKODY BEZPOŚREDNIE, SZCZEGÓLNE, UBOCZNE, POŚREDNIE ORAZ SZKODY, KTÓRYCH NIE MOŻNA BYŁO PRZEWIDZIEĆ PRZY ZAWIERANIU UMOWY, ANI TEŻ
3. UTRATA ZYSKÓW, KONTAKTÓW HANDLOWYCH, PRZYCHODÓW, REPUTACJI (GOODWILL) LUB PRZEWIDYWANYCH OSZCZĘDNOŚCI.

USTAWODAWSTWA NIEKTÓRYCH KRAJÓW NIE DOPUSZCZAJĄ WYŁĄCZENIA CZY OGRANICZENIA ODPOWIEDZIALNOŚCI ZA SZKODY BEZPOŚREDNIE, UBOCZNE LUB SZKODY, KTÓRYCH NIE MOŻNA BYŁO PRZEWIDZIEĆ PRZY ZAWIERANIU UMOWY, W ZWIĄZKU Z CZYM W ODNIESIENIU DO NIEKTÓRYCH KLIENTÓW POWYŻSZE WYŁĄCZENIE LUB OGRANICZENIE (TAK W CAŁOŚCI JAK I W CZĘŚCI) MOŻE NIE MIEĆ ZASTOSOWANIA.

Dodatek A. Komendy bezpieczeństwa

Ta sekcja zawiera komendy systemowe związane z bezpieczeństwem. Można ich używać zamiast menu systemowych, wpisując je w wierszu komend. Komendy podzielone zostały na grupy według zadań.

Temat Język CL zawiera więcej szczegółowych informacji na temat tych komend. Tabele w sekcji Dodatek D, “Uprawnienia wymagane dla obiektów używanych przez komendy”, na stronie 351 prezentują uprawnienia wymagane do korzystania z tych komend.

Więcej informacji na temat narzędzi oraz sugestie dotyczące używania narzędzi bezpieczeństwa znajdują się w temacie Konfigurowanie systemu pod kątem używania narzędzi bezpieczeństwa.

Komendy magazynu uprawnień

Ta tabela zawiera listę komend, które pozwalają na pracę z magazynami uprawnień.

Tabela 134. Komendy magazynu uprawnień

Nazwa komendy	Nazwa opisowa	Funkcja
CRTAUTHLR	Tworzenie magazynu uprawnień (Create Authority Holder)	Ochrona zbioru przed powstaniem. Magazyny uprawnień są poprawne tylko dla zbiorów bazy danych opisanych przez program.
DLTAUTHLR	Usunięcie magazynu uprawnień (Delete Authority Holder)	Usuwa magazyn uprawnień. Jeśli powiązany zbiór istnieje, informacje magazynu uprawnień kopiowane są do zbioru.
DSPAUTHLR	Wyświetlenie magazynu uprawnień (Display Authority Holder)	Umożliwia wyświetlenie wszystkich magazynów uprawnień w systemie.

Komendy list autoryzacji

Komendy te mogą być używane do wykonywania różnych zadań na listach autoryzacji.

Tabela 135. Komendy list autoryzacji

Nazwa komendy	Nazwa opisowa	Funkcja
ADDAUTLE	Dodanie pozycji listy autoryzacji (Add Authorization List Entry)	Powoduje dodanie użytkownika do listy autoryzacji. Należy podać uprawnienia użytkownika do wszystkich obiektów na liście.
CHGAUTLE	Zmiana pozycji listy autoryzacji (Change Authorization List Entry)	Powoduje zmianę uprawnień użytkowników do obiektów na liście autoryzacji.
CRTAUTL	Tworzenie listy autoryzacji (Create Authorization List)	Powoduje utworzenie listy autoryzacji.
DLTAUTL	Usunięcie listy autoryzacji (Delete Authorization List)	Powoduje usunięcie całej listy autoryzacji.
DSPAUTL	Wyświetlenie listy autoryzacji (Display Authorization List)	Powoduje wyświetlenie listy użytkowników i ich uprawnień do listy autoryzacji.
DSPAUTLOBJ	Wyświetlenie obiektów listy autoryzacji (Display Authorization List Objects)	Powoduje 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.

Tabela 135. Komendy list autoryzacji (kontynuacja)

Nazwa komendy	Nazwa opisowa	Funkcja
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)	Praca z listami autoryzacji z wyświetlanej listy.

Komendy uprawnień do obiektu i komendy kontroli

W tej tabeli wymienione zostały komendy, których można używać do pracy z uprawnieniami do obiektu i kontrolą.

Tabela 136. Komendy uprawnień do obiektu i komendy kontroli

Nazwa komendy	Nazwa opisowa	Funkcja
CHGAUD	Zmiana kontroli (Change Auditing)	Powoduje zmianę wartości kontroli dla obiektu.
CHGAUT	Zmiana uprawnień (Change Authority)	Powoduje zmianę uprawnień użytkowników do obiektów.
CHGOBJAUD	Zmiana kontroli obiektu (Change Object Auditing)	Określa, czy dostęp do obiektu jest kontrolowany.
CHGOBJOWN	Zmiana właściciela obiektu (Change Object Owner)	Powoduje zmianę prawa własności do obiektu z jednego użytkownika na innego.
CHGOBJPGP	Zmiana grupy podstawowej obiektu (Change Object Primary Group)	Powoduje zmianę grupy podstawowej dla obiektu na innego użytkownika lub ustawienie bez grupy podstawowej.
CHGOWN	Zmiana właściciela (Change Owner)	Powoduje zmianę prawa własności do obiektu z jednego użytkownika na innego.
CHGPGP	Zmiana grupy podstawowej (Change Primary Group)	Powoduje zmianę grupy podstawowej dla obiektu na innego użytkownika lub ustawienie bez grupy podstawowej.
DSPAUT	Wyświetlenie uprawnień (Display Authority)	Powoduje wyświetlenie uprawnień użytkowników dla obiektu.
DSPLNK	Wyświetlenie dowiązań (Display Links)	Wyświetla listę nazw określonych obiektów w katalogach i opcje pozwalające na wyświetlenie informacji dotyczących tych obiektów.
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)	Powoduje dodanie, zmianę lub usunięcie uprawnień użytkownika dla obiektu.
GRTOBJAUT	Nadanie uprawnień dla obiektu (Grant Object Authority)	Powoduje jawne nadanie uprawnień dla wymienionych użytkowników, wszystkich użytkowników (*PUBLIC) lub użytkowników obiektu odniesienia dla obiektów wymienionych w tej komendzie.
RVKOBJAUT	Odwołanie uprawnień dla obiektu (Revoke Object Authority)	Powoduje usunięcie uprawnienia lub wielu uprawnień (lub wszystkich) nadanych użytkownikowi dla wymienionych obiektów.
WRKAUT	Praca z uprawnieniami (Work with Authority)	Praca z uprawnieniami do obiektu przez wybranie opcji na ekranie listy.

Tabela 136. Komendy uprawnień do obiektu i komendy kontroli (kontynuacja)

Nazwa komendy	Nazwa opisowa	Funkcja
WRKLNK	Praca z dowiązaniami (Work with Links)	Powoduje wyświetlenie listy nazw określonych obiektów w katalogach i opcji pozwalających na pracę z tymi obiektami.
WRKOBJ	Praca z obiektami (Work with Objects)	Praca z uprawnieniami do obiektu przez wybranie opcji na ekranie listy.
WRKOBJOWN	Praca z obiektami wg właścicieli (Work with Objects by Owner)	Praca z obiektami posiadanymi przez profil użytkownika.
WRKOBJPGP	Praca z obiektami wg grupy podstawowej (Work with Objects by Primary Group)	Praca z obiektami, dla których profil jest z grupy podstawowej, za pomocą opcji z wyświetlonej listy.
WRKOBJPVT	Praca z obiektami poprzez uprawnienia prywatne	Praca z obiektami, dla których profil posiada uprawnienia prywatne, za pomocą opcji z wyświetlonej listy.

Komendy haseł

Komendy te pozwalają administratorowi bezpieczeństwa przypisywać, zmieniać lub resetować hasła powiązane z profilem użytkownika, a także sprawdzać ich poprawność.

Tabela 137. Komendy haseł

Nazwa komendy	Nazwa opisowa	Funkcja
CHGDSTPWD	Zmiana hasła narzędzi DST (Change Dedicated Service Tools Password)	Przywrócenie domyślnego hasła dla profilu możliwości bezpieczeństwa narzędzi DST.
CHGPWD	Zmiana hasła (Change Password)	Zmiana własnego hasła użytkownika.
CHGUSRPRF	Zmiana profilu użytkownika (Change User Profile)	Zmiana wartości podanych w profilu użytkownika, w tym hasła użytkownika.
CHKPWD	Sprawdzenie hasła (Check Password)	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). Jednakże, jeśli użytkownik ma uprawnienia prywatne do obiektu na niezależnej ASP lub jest właścicielem obiektu na niezależnej ASP, lub jest grupą podstawową obiektu na niezależnej ASP, nazwa profilu jest zapisywana na niezależnej ASP. 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 taki profil nie istnieje, zostanie on utworzony. Użytkownik nie będzie miał żadnych uprawnień specjalnych, a jego hasło będzie miało wartość *NONE.

Komendy profili użytkowników

Administrator bezpieczeństwa używa tych komend do pracy z profilami użytkowników.

Tabela 138. Komendy profili użytkowników

Nazwa komendy	Nazwa opisowa	Funkcja
CHGPRF	Zmiana profilu (Change Profile)	Zmienia niektóre atrybuty własnego profilu użytkownika.
CHGUSRAUD	Zmiana kontroli użytkownika (Change User Audit)	Określa kontrolowanie obiektu i działania dla profilu użytkownika.

Tabela 138. Komendy profili użytkowników (kontynuacja)

Nazwa komendy	Nazwa opisowa	Funkcja
CHGUSRPRF	Zmiana profilu użytkownika (Change User Profile)	Zmiana 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)	Dodanie użytkownika do systemu oraz określenie wartości takich jak hasło użytkownika, uprawnienia specjalne, menu początkowe, biblioteka bieżąca oraz limit priorytetu.
DLTUSRPRF	Usunięcie profilu użytkownika (Delete User Profile)	Usunięcie profilu użytkownika z systemu. Ta komenda udostępnia opcję usunięcia lub zmiany prawa własności do obiektu, którego właścicielem jest inny profil użytkownika.
DMPUSRPRF	Zrzut profilu użytkownika (Dump User Profile)	Umożliwia zrzucenie profilu użytkownika oraz informacji pokrewnych.
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.
DSPSSTUSR	Wyświetlenie ID użytkownika narzędzi serwisowych (Display Service Tools User ID)	Wyświetlenie listy identyfikatorów użytkowników narzędzi serwisowych. Może służyć również do wyświetlenia informacji szczegółowych o konkretnym ID użytkownika narzędzi serwisowych, w tym statusu i uprawnień tego użytkownika.
DSPUSRPRF	Wyświetlenie profilu użytkownika (Display User Profile)	Wyświetlenie profilu użytkownika w kilku różnych formatach.
GRTUSRAUT	Nadanie uprawnień użytkownika (Grant User Authority)	Skopiowanie uprawnień prywatnych jednego profilu użytkownika do innego.
PRTPRFINT	Drukowanie wewnętrznych danych profilu (Print Profile Internals)	Drukowanie raportu zawierającego wewnętrzne informacje dotyczące liczby pozycji.
PRTUSRPRF	Drukowanie profilu użytkownika (Print User Profile)	Analizowanie profili użytkowników spełniających podane kryterium.
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)	Praca z profilami użytkowników przez wprowadzanie opcji na ekranie listy.

Pokrewne komendy profilu użytkownika

Poniższa tabela wymienia kilka innych komend dotyczących profili użytkownika. Komendy te umożliwiają odtwarzanie i zapisywanie profili użytkownika wraz z atrybutami.

Tabela 139. Pokrewne komendy profilu użytkownika

Nazwa komendy	Nazwa opisowa	Funkcja
DSPPGMADP	Wyświetlenie programów, które adoptują uprawnienia (Display Programs That Adopt)	Wyświetla listę programów i pakietów SQL, które adoptują podany profil użytkownika.
RSTAUT	Odtwarzanie uprawnień (Restore Authority)	Umożliwia odtworzenie uprawnień dla obiektów, które były zawarte w profilu użytkownika w momencie jego zapisywania. 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 odtworzenie profilu użytkownika wraz z atrybutami. 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.

Komendy kontroli

Komendy te służą do zarządzania kontrolą obiektu.

Tabela 140. Komendy kontroli

Nazwa komendy	Nazwa opisowa	Funkcja
CHGAUD	Zmiana kontroli (Change Auditing)	Określa kontrolę dla obiektu.
CHGDLOAUD	Zmiana kontroli DLO (Change Document Library Object Auditing)	Określa, czy dostęp do obiektu biblioteki dokumentów jest kontrolowany.
CHGOBJAUD	Zmiana kontroli obiektu (Change Object Auditing)	Określa kontrolę dla obiektu.
CHGUSRAUD	Zmiana kontroli użytkownika (Change User Audit)	Określa kontrolowanie obiektu i działania dla profilu użytkownika.

Komendy obiektów biblioteki dokumentów

Niniejsza tabela zawiera komendy, przy pomocy których można pracować z obiektami biblioteki dokumentów.

Tabela 141. Komendy obiektów biblioteki dokumentów

nazwa komendy	Nazwa opisowa	Funkcja
ADDDLOAUT	Dodanie uprawnienia dla DLO (Add Document Library Object Authority)	Przyznanie użytkownikowi dostępu do dokumentu lub folderu, czy też zabezpieczenie dokumentu lub folderu za pomocą listy autoryzacji lub kodu dostępu.
CHGDLOAUD	Zmiana kontroli DLO (Change Document Library Object Auditing)	Określenie poziomu kontroli obiektu dla obiektu biblioteki dokumentów.
CHGDLOAUT	Zmiana uprawnienia dla DLO (Change Document Library Object Authority)	Zmiana uprawnienia dla dokumentu lub folderu.

Tabela 141. Komendy obiektów biblioteki dokumentów (kontynuacja)

nazwa komendy	Nazwa opisowa	Funkcja
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)	Zmiana grupy podstawowej dla obiektu biblioteki dokumentów.
DSPAUTLDLO	(Wyświetlenie listy autoryzacji DLO - Display Authorization List Document Library Objects)	Wyświetlenie dokumentów i folderów zabezpieczanych przez określoną listę autoryzacji.
DSPDLOAUD	Wyświetlenie kontroli obiektu DLO (Display Document Library Object Auditing)	Wyświetla poziom kontroli obiektu dla obiektu biblioteki dokumentów.
DSPDLOAUT	Wyświetlenie uprawnienia dla DLO (Display Document Library Object Authority)	Wyświetlanie informacji o uprawnieniach dla dokumentu lub folderu.
EDTDLOAUT	Edycja uprawnienia dla DLO (Edit Document Library Object Authority)	Dodanie, zmiana lub usunięcie uprawnień użytkowników 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)	Usuwanie uprawnienia użytkowników 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.

Komendy pozycji uwierzytelniania serwera

Komendy te umożliwiają wyświetlanie, dodawanie, usuwanie lub zmianę pozycji uwierzytelniania serwera dla proflu użytkownika.

Tabela 142. Komendy pozycji uwierzytelniania serwera

Nazwa komendy	Nazwa opisowa	Funkcja
ADDSVRAUTE	Dodanie pozycji uwierzytelniania serwera (Add Server Authentication Entry)	Dodaje informacje o uwierzytelnianiu serwera dla profilu użytkownika.
CHGSVRAUTE	Zmiana pozycji uwierzytelniania serwera (Change Server Authentication Entry)	Zmienia istniejące pozycje uwierzytelniania serwera dla profilu użytkownika.
DSPSVRAUTE	Wyświetlenie pozycji uwierzytelniania serwera (Display Server Authentication Entries)	Wyświetla pozycje uwierzytelniania serwera dla profilu użytkownika.
RMVSVRAUTE	Usuwanie pozycji uwierzytelniania serwera (Remove Server Authentication Entry)	Usuwa pozycje 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.		

Komendy katalogu dystrybucyjnego systemu

Omówionych komend można użyć w celu dodania, usunięcia lub zmiany pozycji w katalogu dystrybucyjnym systemu.

Tabela 143. Komendy katalogu dystrybucyjnego 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.

Komendy list sprawdzania

Dwie przedstawione komendy umożliwiają tworzenie i usuwanie list sprawdzania w bibliotece.

Tabela 144. Komendy list sprawdzania

Nazwa komendy	Nazwa opisowa	Funkcja
CRTVLDL	Tworzenie listy sprawdzania (Create Validation List)	Tworzy obiekt listy sprawdzania zawierający 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)	Usuwa podaną listę sprawdzania z biblioteki.

Komendy informacji o używaniu funkcji

Komendy te mogą być używane do zmiany lub wyświetlania informacji o używaniu funkcji.

Tabela 145. Komendy informacji o używaniu funkcji

Nazwa komendy	Nazwa opisowa	Funkcja
CHGFCNUSG	Zmiana użycia funkcji (Change function usage)	Zmiana informacji o używaniu zarejestrowanej funkcji.
DSPFCNUSG	Wyświetlenie użycia funkcji (Display function usage)	Wyświetlenie listy identyfikatorów funkcji oraz szczegółowych informacji o używaniu dla podanej funkcji.
WRKFCNUSG	Praca z użyciem funkcji (Work with function usage)	Wyświetlenie listy identyfikatorów funkcji oraz zmiana lub wyświetlenie informacji o użyciu funkcji.

Komendy kontroli narzędzi bezpieczeństwa

Komendy te umożliwiają pracę z kontrolą bezpieczeństwa, pozycjami z kroniki kontroli bezpieczeństwa oraz wartościami systemowymi sterującymi kontrolą bezpieczeństwa.

Więcej informacji o narzędziach ochrony zawiera sekcja Dodatek G, “Komendy i menu dla komend bezpieczeństwa”, na stronie 735.

Tabela 146. Komendy kontroli narzędzi bezpieczeństwa

Nazwa komendy	Nazwa opisowa	Funkcja
CHGSECAUD	Zmiana kontroli ochrony (Change Security Auditing)	Konfiguruje kontrolę bezpieczeństwa i służy do zmiany wartości systemowych sterujących kontrolą bezpieczeństwa.
CPYAUDJRNE	Kopiowanie wpisów kroniki kontroli	Kopiuje pozycje z kroniki kontroli bezpieczeństwa do zbiorów wyjściowych, do których można wysłać zapytanie. Można wybrać konkretne typy wpisów, konkretnych użytkowników i przedział czasowy.
DSPAUDJRNE[1]	Wyświetlenie pozycji kroniki kontroli (Display Audit Journal Entries)	Wyświetla lub drukuje informacje o pozycjach w kronice kontroli bezpieczeństwa. Można wybrać konkretne typy wpisów, konkretnych użytkowników i przedział czasowy.
DSPSECAUD	Wyświetlenie wartości kontroli ochrony (Display Security Auditing Values)	Wyświetla informacje o kronice kontroli bezpieczeństwa i wartościach systemowych, które sterują kontrolą bezpieczeństwa.
1 Firma IBM nie dostarcza już rozszerzeń dla komendy DSPAUDJRNE. Komenda ta nie obsługuje wszystkich typów rekordów kontroli ochrony i nie wyświetla wszystkich pól dla rekordów, które obsługuje.		

Komendy uprawnień narzędzi bezpieczeństwa

Za pomocą tych komend można wykonywać różne zadania wydruku związane z ustawieniami bezpieczeństwa.

Tabela 147. Komendy uprawnień narzędzi bezpieczeństwa

Nazwa komendy	Nazwa opisowa	Funkcja
PRTJOBDAUT	Drukowanie uprawnień opisu dla zadania (Print Job Description Authority)	Drukuje listę 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)	Drukuje listę obiektów podanego typu, których uprawnienia publiczne są inne niż *EXCLUDE.
PRTPVTAUT	Drukowanie uprawnień prywatnych (Print Private Authorities)	Drukuje listę uprawnień prywatnych dla obiektów podanego typu.
PRTQAUT	Drukowanie uprawnień dla kolejki (Print Queue Authoriy)	Drukuje ustawienia bezpieczeństwa 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)	Drukuje listę opisów podsystemów w bibliotece, które zawierają użytkownika domyślnego w pozycji podsystemu.
PRTTRGPGM	Drukowanie programów wyzwalaczy (Print Trigger Programs)	Drukuje listę programów wyzwalanych, które są powiązane ze zbiorami bazy danych w systemie.
PRTUSROBJ	Drukowanie obiektów użytkownika (Print User Objects)	Drukuje listę obiektów użytkowników (obiektów, które nie są dostarczane przez IBM), które znajdują się w bibliotece.

Komendy narzędzi bezpieczeństwa systemu

Komendy te służą do prac związanych z bezpieczeństwem systemu.

Tabela 148. Komendy narzędzi bezpieczeństwa systemu

Nazwa komendy	Nazwa opisowa	Funkcja
CHGSECA [1]	Zmiana atrybutów ochrony (Change Security Attributes)	Ustawia nowe wartości początkowe do generowania numerów ID użytkownika lub grupy. Użytkownicy mogą podać początkowy numer ID użytkownika oraz początkowy numer ID grupy.
CFGSYSSEC	Konfigurowanie ochrony systemu (Configure System Security)	Ustawia wartości systemowe dotyczące bezpieczeństwa zgodnie z zaleceniami. Komenda ta konfiguruje również kontrolę bezpieczeństwa w systemie.
CLRSVRSEC	Usuwanie zawartości danych ochrony serwera (Clear Server Security Data)	Usuwa możliwe do rozszyfrowania dane dotyczące uwierzytelniania, które są powiązane z profilami użytkowników oraz pozycjami listy sprawdzania (*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)	Wyświetla bieżące i oczekujące wartości niektórych atrybutów bezpieczeństwa systemu.
PRTCMNSEC	Drukowanie ochrony komunikacji (Print Communications Security)	Drukuje atrybuty bezpieczeństwa obiektów *DEVD, *CTL i *LIND w systemie.
PRTSYSSECA	Drukowanie atrybutów ochrony systemu (Print System Security Attributes)	Drukuje listę wartości systemowych i atrybutów sieciowych dotyczących bezpieczeństwa. Raport zawiera wartość bieżącą i zalecaną.
RVKPUBAUT	Odwołanie uprawnień publicznych (Revoke Public Authority)	Ustawia uprawnienia publiczne na wartość *EXCLUDE dla zestawu komend istotnych dla bezpieczeństwa w danym systemie.

[1] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *SECADM.

Dodatek B. Profile użytkowników IBM

Ta sekcja 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.

Wartości domyślne dla profili użytkowników

Niniejsza tabela wskazuje domyślne wartości, które są używane dla profili użytkowników IBM i komendy Tworzenie profilu użytkownika (Create User Profile -CRTUSRPRF.Parametry są ułożone według kolejności ich pojawiania się na ekranie Tworzenie profilu użytkownika (Create User Profile).

Tabela 149. Wartości domyślne dla profili użytkowników

	Wartości domyślne	
Parametry profili użytkownika	**Profile użytkowników IBM**	**Ekran Tworzenie profilu użytkownika**
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
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

Tabela 149. Wartości domyślne dla profili użytkowników (kontynuacja)

Parametry profili użytkownika	Wartości domyślne	
	Profile użytkowników IBM	Ekran Tworzenie profilu użytkownika
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. Jeśli jednak użytkownik posiada uprawnienia prywatne do puli dyskowej, jest właścicielem obiektu w niezależnej puli dyskowej lub jest grupą podstawową w obiekcie w niezależnej puli dyskowej, w tej puli dyskowej zostanie umieszczona nazwa profilu. Jeśli niezależna pula dyskowa jest przenoszona do innego systemu, uprawnienia prywatne, prawa własności do obiektu oraz pozycje grupy podstawowej będą dołączone w systemie docelowym do profilu o tej samej nazwie. Jeśli w systemie docelowym taki profil nie istnieje, zostanie on utworzony.Użytkownik nie będzie miał żadnych uprawnień specjalnych, a jego hasło będzie miało wartość *NONE.

Profile użytkowników IBM

W tej tabeli opisano listę profili użytkowników IBM, ich przeznaczenie oraz wartości, które są inne niż domyślne dla profili użytkowników IBM.

Uwaga:

Profile użytkowników IBM obejmują 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.

Ważne:

- Hasło dla profilu SECOFR

  Po zainstalowaniu systemu należy zmienić hasło dla profilu QSECOFR. To hasło jest takie samo dla każdego produktu System i i do czasu jego zmiany istnieje ryzyko naruszenia bezpieczeństwa. 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 150. 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
QDFTOWN	Profil właściciela domyślnego	• PTYLMT: 3

Tabela 150. Profile użytkowników IBM (kontynuacja)

Nazwa profilu	Nazwa opisowa	Parametry inne niż wartości domyślne
QDIRSRV	Profil użytkownika serwera katalogów i5/OS	• LMTCPB: *YES • JOBD: QGPL/QBATCH • DSPSGNINF: *NO • LMTDEVSSN: *NO • DLVRY: *HOLD • SPCENV: *NONE • ATNPGM: *NONE
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	

Tabela 150. Profile użytkowników IBM (kontynuacja)

Nazwa profilu	Nazwa opisowa	Parametry inne niż wartości domyślne
QNETSPLF	Profil buforowania sieciowego	
QNTP	Profil NTP	• JOBD: QTOTNTP • JOBD LIBRARY: QSYS
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 System i (PM System i)	• 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)

Tabela 150. Profile użytkowników IBM (kontynuacja)

Nazwa profilu	Nazwa opisowa	Parametry inne niż wartości domyślne
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)
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 osoby odpowiedzialnej za bezpieczeństwo	• 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: *EXCLUDE

Tabela 150. Profile użytkowników IBM (kontynuacja)

Nazwa profilu	Nazwa opisowa	Parametry inne niż wartości domyślne
QSRV	Profil usługi	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1], *SAVSYS [1], *JOBCTL, *SERVICE • ASTLVL: *INTERMED • ATNPGM: QSYS/QSCATTN
QSRVAGT	Profil użytkownika aplikacji Service Agent	
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

Tabela 150. Profile użytkowników IBM (kontynuacja)

Nazwa profilu	Nazwa opisowa	Parametry inne niż wartości domyślne
QTCP	Profil protokołu Transmission control protocol (TCP)	• USRCLS: *SYSOPR • SPCAUT: *JOBCTL • CCSID: *HEX • SRTSEQ: *HEX
QTFTP	Protokół Trivial File Transfer Protocol	
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	

Tabela 150. Profile użytkowników IBM (kontynuacja)

Nazwa profilu	Nazwa opisowa	Parametry inne niż wartości domyślne
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

W tej sekcji wskazano komendy z ograniczoną autoryzacją (uprawnienia publiczne *EXCLUDE) ustawioną fabrycznie w systemie. Zawiera ona także informacje o tym, które profile użytkowników IBM są autoryzowane do korzystania z tych zastrzeżonych komend.

Więcej informacji na temat profili użytkowników IBM zawiera temat “Profile użytkowników IBM” na stronie 131.

Tabela 151 zawiera wykaz komend, a komendy, które są zastrzeżone dla osoby odpowiedzialnej za bezpieczeństwo oraz profilu użytkownika z uprawnieniami *ALLOBJ, oznaczono literą **R**. Komendy, do których uprawnienia ma jeden lub więcej profili użytkowników IBM, oprócz osoby odpowiedzialnej za bezpieczeństwo, 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 351

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 351.

Tabela 151. Uprawnienia profili użytkowników IBM do komend zastrzeżonych

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ADDCLUNODE	R				
ADDCMDCRQA		S	S	S	S
ADDCRGDEVE	R				
ADDCRGNODE	R				
ADDCRSDMNK	R				
ADDDEVDMNE	R				
ADDDSTQ		S	S		
ADDDSTRTE		S	S		
ADDDSTSYSN		S	S		
ADDEXITPGM	R				
ADDDWDFN					
ADDJWDFN					
ADDMFS	R				
ADDMSTPART					
ADDNETJOBE	R				
ADDOBJCRQA		S	S	S	S
ADDOPTCTG	R				
ADDOPTSVR	R				
ADDPEXDFN		S		S	
ADDPEXFTR		S		S	

Tabela 151. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ADDPRDCRQA		S	S	S	S
ADDPTFCRQA		S	S	S	S
ADDRPYLE		S			
ADDRSCCRQA		S	S	S	S
ADDTRCFTR	R				
ANSQST	R				
ANZBESTMDL	R				
ANZCMDPFR	R				
ANZDBF	R				
ANZDBFKEY	R				
ANZDFTPWD	R				
ANZJVM		S	S	S	S
ANZOBJCVN	R				
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				
CHGASPA	R				
CHGASPACT					
CHGCLUCFG	R				
CHGCLUNODE	R				
CHGCLURCY	R				
CHGCLUVER	R				
CHGCMDCRQA		S	S	S	S
CHGCRG	R				
CHGCRGDEVE	R				
CHGCRGPRI	R				
CHGCRSDMNK	R				
CHGDIRSRVA					
CHGDSTQ		S	S		
CHGDSTRTE		S	S		

Tabela 151. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CHGEXPSCDE	R				
CHGFCNARA	R				
CHGGPHFMT	R				
CHGGPHPKG	R				
CHGJOBTRC	R				
CHGJOBTYP	R				
CHGJRN		S	S	S	
CHGJRNA		S	S		
CHGLICINF	R				
CHGMGDSYSA		S	S	S	S
CHGMGRSRVA		S	S	S	S
CHGMSTK	R				
CHGNETA	R				
CHGNETJOBE	R				
CHGNFSEXP	R				
CHGNWSA	R				
CHGNWSCFG	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	
CHKMSTKVV					
CHKPRDOPT		S	S	S	S
CLRMSTKEY					
CPHDTA	R				
CPYFCNARA	R				
CPYFRMLDIF					
CPYGPHFMT	R				

Tabela 151. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CPYGPHPKG	R				
CPYPFRCOL	R				
CPYPFRDTA	R				
CPYPTF		S	S	S	S
CPYPTFGRP		S	S	S	S
CPYTOLDIF					
CRTADMDMN	R				
CRTAUTHLR	R				
CRTBESTMDL	R				
CRTCLS	R				
CRTCLU	R				
CRTCRG	R				
CRTFCNARA	R				
CRTGPHFMT	R				
CRTGPHPKG	R				
CRTHSTDTA	R				
CRTJOBD	R				
CRTNWSCFG	R				
CRTPFRDTA	R				
CRTPFRSUM					
CRTLASREP		S			
CRTPEXDTA		S		S	
CRTQSTDB	R				
CRTQSTLOD	R				
CRTSBSD		S	S		
CRTUDFS	R				
CRTUDFS	R				
CRTVLDL	R				
CVTBASSTR	R				
CVTBASUNF	R				
CVTBGUDTA	R				
CVTDIR	R				
CVTPFRCOL	R				
CVTPFRDTA	R				
CVTPFRTHD	R				
CVTS36FCT	R				
CVTS36JOB	R				
CVTS38JOB	R				
CVTTCPCL		S	S	S	S
DB2LDIF					

Tabela 151. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
DLTADMDMN	R				
DLTAPARDTA		S	S	S	S
DLTBESTMDL	R				
DLTCLU	R				
DLTCMNTRC				S	
DLTCRGCLU	R				
DLTEXPSPLF	R				
DLTFCNARA	R				
DLTGPHFMT	R				
DLTGPHPKG	R				
DLTHSTDTA	R				
DLTLICPGM	R				
DLTNWSCFG	R				
DLTPEXDTA		S		S	
DLTPFRCOL	R				
DLTPFRDTA	R				
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				
DLTWNTSVR	R				
DMPDLO		S	S	S	S
DMPJOB		S	S	S	S
DMPJOBINT		S	S	S	S
DMPJVM		S	S	S	S
DMPMEMINF					
DMPOBJ				S	S
DMPSYSOBJ		S	S	S	S
DMPTRC	R	S		S	
DMPUSRPRF					
DSPDSTLOG	R				
DSPHSTGPH	R				
DSPMGDSYSA		S	S	S	S
DSPNWSCFG	R				
DSPPFRDTA	R				
DSPPFRGPH	R				

Tabela 151. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
DSPPTF		S	S	S	S
DSPSRVSTS		S	S	S	S
EDTCPCST			S		
EDTQST	R				
EDTRBDAP			S		
EDTRCYAP		S	S		
ENCCPHK	R				
ENCFRMMSTK	R				
ENCTOMSTK	R				
ENDASPBAL	R				
ENDCHTSVR	R				
ENDCLUNOD	R				
ENDCMNTRC	R			S	
ENDCRG	R				
ENDDBGSVR		S	S	S	S
ENDDW					
ENDHOSTSVR		S	S	S	S
ENDIDXMON	R				
ENDIPSIFC		S	S	S	S
ENDJOBABN		S	S	S	
ENDJOBTRC	R				
ENDJW					
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
ENDWCH	R				
GENCPHK	R				
GENCRSDMNK	R				
GENMAC	R				
GENPIN	R				
GENS36RPT	R				

Tabela 151. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
GENS38RPT	R				
GRTACCAUT	R				
HLDCMNDEV		S	S	S	S
HLDDSTQ		S	S		
INSPTF[2]				S	
INSRMTPRD		S	S	S	S
INSWNTSVR	R				
INZDSTQ		S	S		
INZNWSCFG	R				
INZSYS	R				
LDIF2DB					
LODOPTFMW	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				
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				

Tabela 151. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
PRTDSKINF	R				
PRTERRLOG		S	S	S	S
PRTINTDTA		S	S	S	S
PRTPRFINT	R				
PWRDWNSYS	R		S		
RCLDBXREF	R				
RCLOBJOWN	R				
RCLOPT	R				
RCLSPLSTG		S	S	S	S
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				
RMVCRGDEVE	R				
RMVCRGNODE	R				
RMVCRSDMNK	R				
RMVDEVDMNE	R				
RMVDFRID	R				
RMVDSTQ		S	S		
RMVDSTRTE		S	S		
RMVDSTSYSN		S	S		
RMVDWDFN					
RMVEXITPGM	R				
RMVJRNCHG		S		S	
RMVJWDFN					
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			

Tabela 151. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
RMVTRCFTR	R				
RSTAUT	R				
RST[3]					
RSTCFG	R				
RSTDFROBJ	R				
RSTDLO	R				
RSTLIB	R				
RSTLICPGM	R				
RSTOBJ[3]					
RSTPFRCOL	R				
RSTPFRDTA					
RSTS36F	R				
RSTS36FLR	R				
RSTS36LIBM	R				
RSTS38AUT	R				
RSTUSFCNR[4]					
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				
SAVPFRCOL	R				
SAVPFRDTA					
SAVRSTCHG	R				
SAVRSTLIB	R				
SAVRSTOBJ	R				
SBMFNCJOB	R				
SBMNWSCMD	R				
SETMSTK	R				
SETMSTKEY					
SNDDSTQ		S	S		
SNDPRD		S	S	S	S
SNDPTF		S	S	S	S
SNDPTFORD				S	S

Tabela 151. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
SNDSMGOBJ		S	S	S	S
SNDSRVRQS				S	S
STRASPBAL	R				
STRBEST	R				
STRCHTSVR	R				
STRCLUNOD	R				
STRCMNTRC				S	
STRCRG	R				
STRDBG		S		S	S
STRDBGSVR		S	S	S	S
STRDW					
STRHOSTSVR		S	S	S	S
STRIDXMON	R				
STRIPSIFC		S	S	S	S
STRJW	R				
STRJOBTRC					
STRMGDSYS		S	S	S	S
STRMGRSRV		S	S	S	S
STRMSF[1]			S	S	S
STRNFSSVR	R				
STROBJCVN	R				
STRPEX		S		S	
STRPFRG	R				
STRPFRT	R				
STRPFRTRC	R			S	
STRRGZIDX	R				
STRSPLRCL	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				
STRWCH	R				
TRCASPBAL	R				
TRCCPIC	R				

Tabela 151. Uprawnienia profili użytkowników IBM do komend zastrzeżonych (kontynuacja)

Nazwa komendy	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
TRCICF	R				
TRCINT		S		S	
TRCJOB		S	S	S	S
TRCTCPAPP				S	S
TRNPIN	R				
UPDPTFINF	R				
VFYCMN		S	S	S	S
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				
WRKJRN		S	S	S	
WRKLIB					
WRKLIBPDM					
WRKLICINF	R				
WRKNWSCFG	R				
WRKORDINF			S	S	
WRKPEXDFN		S		S	
WRKPEXFTR		S		S	
WRKPGMTBL	R				
WRKPRB		S	S	S	S
WRKPTFGRP		S	S	S	S
WRKPTFORD	R			S	S
WRKSRVPVD				S	S
WRKSYSACT	R				
WRKTRC	R				
WRKTXTIDX	R				
WRKUSRTBL	R				
WRKWCH	R				

[1] Profil użytkownika QMSF także ma uprawnienia do korzystania z tej komendy.

[2] Użytkownik QSRV nie może uruchomić tej komendy podczas IPL.

[3] Oprócz użytkownika QSYS, uprawnienia ma profil użytkownika QRDARS400.

[4] Oprócz użytkownika QSYS, uprawnienia ma profil użytkownika QUMB.

Dodatek D. Uprawnienia wymagane dla obiektów używanych przez komendy

Tabele znajdujące się w tej sekcji przedstawiają uprawnienia wymagane dla obiektów, do których odnoszą się komendy.

Na przykład w pozycji komendy Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF) w tabeli znajduje się lista wszystkich obiektów, takich jak kolejka komunikatów użytkownika, opis zadania i program początkowy, do których konieczne są uprawnienia.

Tabele ułożone są w porządku alfabetycznym, według typu obiektu. Dodatkowo, dołączono tabele dla elementów, które nie są obiektami i5/OS (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 w tabelach.

Obiekt odniesienia

Obiekty wyświetlone na liście w kolumnie *Obiekt odniesienia* są obiektami, do których potrzebne są uprawnienia podczas używania tej komendy.

Uprawnienie wymagane dla obiektu

Uprawnienia określone w tabeli przedstawiają uprawnienia do obiektów i danych wymagane dla obiektu w przypadku użycia komendy.

Uprawnienie wymagane dla 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.

Typ obiektu

Wartość odnosi się do typu obiektu określonego w kolumnie Obiekt odniesienia.

System plików

Wartość odnosi się do typu systemu plików, do którego należy obiekt odniesienia.

Opis zintegrowanego systemu plików w systemie operacyjnym i5/OS można znaleźć w sekcji Zintegrowany system operacyjny.

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.

Tabela 152. Opis typów uprawnień

Uprawnienie	Nazwa	Dozwolone funkcje
Uprawnienia do obiektu:		

Tabela 152. Opis typów uprawnień (kontynuacja)

Uprawnienie	Nazwa	Dozwolone funkcje
*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.
*OBJREF	Odniesienie do obiektu	Określanie zbioru bazy danych jako nadrzędnego w ograniczeniu referencyjnym. Na przykład załóżmy, że chcemy zdefiniować regułę określającą, 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.
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), uprawnienia do istnienia obiektu nie są wymagane do wykonywania operacji składowania i odtwarzania obiektu.

Oprócz tych wartości kolumny *Wymagane uprawnienia* tabeli mogą zawierać zdefiniowane systemowo podzbiory tych uprawnień. W poniższej tabeli są wymienione podzbiory uprawnień do obiektów i danych.

Tabela 153. Uprawnienia zdefiniowane systemowo

Uprawnienie	*ALL	*CHANGE	*USE	*EXCLUDE
Uprawnienia do obiektu				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			

Tabela 153. Uprawnienia zdefiniowane systemowo (kontynuacja)

Uprawnienie	*ALL	*CHANGE	*USE	*EXCLUDE
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 154. 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

Założenia związane z użyciem komend

Istnieją pewne domyślne założenia, które należy wziąć pod uwagę przed użyciem każdej komendy.

1. Do użycia każdej komendy wymagane jest uprawnienie *USE. To uprawnienie nie jest wyraźnie zaznaczone w tabelach.
2. Aby wprowadzić dowolne komendy wyświetlania, wymagane są uprawnienia działania do zbioru ekranowego IBM, zbioru wydruku lub panelu grupowego używanego przez komendę. Te zbiory i panele grupowe dostarczane są z uprawnieniami publicznymi *USE.

Ogólne zasady uprawnień do obiektów w komendach

W poniższej tabeli podano ogólne zasady, dotyczące uprawnień do obiektów w komendach.

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	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
Komenda uzyskująca dostęp do obiektu w katalogu	Katalogi w przedrostku ścieżki	*X	
	Katalog przy określonym wzorcu (* lub ?)	*R	
Tworzenie obiektu w katalogu	Katalogi w przedrostku ścieżki	*X	
	Katalog dla nowego obiektu	*WX	
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 zbiór istnieje i dodawany jest nowy podzbiór oraz podano opcję *ADD, zaś podzbiór nie istniał wcześniej.	OBJOPR, *OBJMGT lub *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
	Format zbioru (QA*xxxxx*), jeśli zbiór wyjściowy nie istnieje	*OBJOPR	

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
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
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] eśli 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 dodatkowych 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 dla większości obiektów

W tej tabeli znajdują się komendy, wymienione w kolejności alfabetycznej, które działają na większości obiektów.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Tabela 155. Wspólne komendy dla większości obiektów

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
ALCOBJ [1,2,11]	Obiekt	*OBJOPR	*EXECUTE
ANZOBJCVN (Q) [20]			

Tabela 155. Wspólne komendy dla większości obiektów (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
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
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

Tabela 155. Wspólne komendy dla większości obiektów (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
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	
DSPOBJD [2, 28]	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Obiekt	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]			
RCLDBXREF			
RCLOBJOWN (Q)			
RCLSTG (Q)			
RCLTMPSTG (Q)	Obiekt	*OBJMGT	*EXECUTE
RMVDFRID (Q) [10]			

Tabela 155. Wspólne komendy dla większości obiektów (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
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	
RSTDFROBJ (Q) [10]	Zbiór wydruku QSYS/QPSRLDSP, jeśli określono OUTPUT(*PRINT)	*USE	*EXECUTE
	Zbiór wyjściowy, jeśli określono	Patrz zasady ogólne	Patrz zasady ogólne
	Zbiór opisów pól QSYS/QASRRSTO dla zbioru wyjściowego, jeśli określono nieistniejący zbiór wyjściowy	*USE	*EXECUTE
RSTOBJ (Q)[3,13, 31, 33]	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 (Q)	Jednostka taśm 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	

Tabela 155. Wspólne komendy dla większości obiektów (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
RSTSYSINF	Zbiór składowania	*USE	*EXECUTE
	Jednostka taśm lub jednostka optyczna	*USE	*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
RVKPUBAUT [20]			
RTVOBJD [2, 29]	Obiekt	Uprawnienia inne niż *EXCLUDE	*EXECUTE
RVKOBJAUT [3,5,15, 27]	Urządzenie ASP (jeśli jest podane)	*USE	
SAVCHGOBJ [3, 32]	Obiekt (8)	*OBJEXIST	*EXECUTE
	Jednostka taśm lub 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
	Przestrzeń komend użytkownika, jeśli została określona	*USE	*EXECUTE
SAVCHGOBJ	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	

Tabela 155. Wspólne komendy dla większości obiektów (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
SAVOBJ [3, 32]	Obiekt	*OBJEXIST [8]	*EXECUTE
	Definicja nośnika	*USE	*EXECUTE
	Jednostka taśm lub 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
	Przestrzeń komend użytkownika, jeśli została określona	*USE	*EXECUTE
SAVOBJ	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
SAVSYSINF	Definicja nośnika	*USE	*EXECUTE
	Jednostka taśm lub jednostka optyczna	*USE	*EXECUTE
	Zbiór składowania, jeśli jest pusty	*USE, *ADD	*EXECUTE
	Zbiór składowania, jeśli istnieją w nim rekordy	*OBJMGT, *USE, *ADD	*EXECUTE
	Zbiór nośnika optycznego (OPTFILE) [22]	*RW	Nie dotyczy
	Katalog nadrzędny zbioru 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	

Tabela 155. Wspólne komendy dla większości obiektów (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
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	
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
STROBJCVN (Q)[20]			
STRSAVSYNC[34]			
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

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.

Tabela 155. Wspólne komendy dla większości obiektów (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
[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 określić wartość inną niż *NONE dla parametru Zezwalaj na różnice w obiektach (Allow object differences - ALWOBJDIF), użytkownik musi posiadać specjalne uprawnienia. [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.			
[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 źródłowy (obiekt_z) ma grupę podstawową, nowy obiekt może nie mieć tej samej grupy podstawowej, ale uprawnienia, które grupa podstawowa nakłada na obiekt źródłowy zostaną 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.			

Tabela 155. Wspólne komendy dla większości obiektów (kontynuacja)

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do 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 razie wyświetlona zostanie wartość *NOTAVL, oznaczająca, że wartość nie może zostać wyświetlona. [29] Aby pobrać bieżącą wartość kontrolowania obiektu, użytkownik musi mieć uprawnienie specjalne *ALLOBJ lub *AUDIT. W przeciwnym razie zwrócona zostanie wartość *NOTAVL, oznaczająca, że wartość nie może zostać pobrana. [30] Aby określić, jakie uprawnienia potrzebne są do konwersji programów, programów serwisowych i modułów, należy zapoznać się z opisami komend CHGPGM, CHGSRVPGM i CHGMOD.			
[31] Aby określić wartość *YES dla parametru PVTAUT, należy mieć uprawnienie specjalne *ALLOBJ. [32] Aby określić wartość *YES dla parametru PVTAUT, należy mieć uprawnienie specjalne *ALLOBJ lub *SAVSYS. [33] Aby określić nazwę parametru DFRID, należy mieć uprawnienie specjalne *SAVSYS. [34] Należy mieć uprawnienia specjalne *SAVSYS i *JOBCTL.			

Komendy odtwarzania ścieżek dostępu

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend odtwarzania ścieżek dostępu

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Te komendy nie wymagają uprawnień do obiektu.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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] Do użycia tej komendy konieczne jest uprawnienie specjalne *JOBCTL. [2] Do użycia tej komendy konieczne jest uprawnienie specjalne (*ALLOBJ).			

Komendy funkcji Advanced Function Presentation (AFP)

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend funkcji Advanced Function Presentation (AFP).

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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
WRKOVL [1]	Nakładka	*USE	*USE
WRKPAGDFN [1]	Definicja strony	Dowolne uprawnienia	*USE

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
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

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend gniazd AF_INET przez SNA.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Te komendy nie wymagają żadnych uprawnień do obiektów:

Te komendy nie wymagają żadnych uprawnień do obiektów:			
ADDIPSIFC[1] ADDIPSRTE[1] ADDIPSLOC[1] CFGIPS	CHGIPSIFC[1] CHGIPSLOC[1] CHGIPSTOS[1] CVTIPSIFC	CVTIPSLOC ENDIPSIFC (Q) PRTIPSCFG RMVIPSIFC[1]	RMVIPSLOC[1] RMVIPSRTE[1] STRIPSIFC (Q)

[1] Do użycia tej komendy konieczne jest uprawnienie specjalne (*IOSYSCFG).

Komendy alertów

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend alertów

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend projektowania aplikacji

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
FNDSTRPDM	Część kodu źródłowego	*READ	*EXECUTE
MRGFORMD	Opis formularza	*READ	*EXECUTE
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, 4]			
WRKMBRPDM [1]	Zbiór źródłowy	*USE	*EXECUTE
WRKOBJPDM [1]	Zbiór (File)	*READ lub prawo własności	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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). [4] Komenda ta wymaga uprawnienia specjalnego *ALLOBJ.			

Komendy magazynu uprawnień

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend magazynu uprawnień.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend list autoryzacji.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki QSYS
WRKAUTL [3,4,5]	*AUTL		

[1] Użytkownik musi być właścicielem lub mieć uprawnienia do zarządzania listą autoryzacji.

[2] Jeśli użytkownik nie posiada uprawnień *OBJMGT lub *AUTLMGT, może odtworzyć własne uprawnienia i uprawnienia *PUBLIC. 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

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend katalogu konsolidacji.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend opisu żądania zmiany.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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	Zmiana opisu żądania zmiany	*CHANGE	*EXECUTE
CHGRSCCRQA (Q)	Opis żądania zmiany	*CHANGE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
CRTCRQD	Opis żądania zmiany		*READ, *ADD
DLTCRQD	Opis żądania zmiany	*OBJEXIST	*EXECUTE
RMVCRQDA	Opis żądania zmiany	*CHANGE	*EXECUTE
WRKCRQD [1]	Opis żądania zmiany		*EXECUTE

[1] Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

Komendy wykresów

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend wykresów.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend klas.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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 dotyczących usług

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend klas.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
CHGCOSD [3]	Opis klasy usług	*CHANGE, OBJMGT	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
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

[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

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend klastra.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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	
	Opis kontrolera	*USE, *OBJMGT	
	Opis linii	*USE, *OBJMGT	
	Opis serwera sieciowego	*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	

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
CHGCLURCY	Grupa zasobów klastra	*USE	
		*JOBCTL	
		*SERVICE lub funkcja śledzenia serwisowego	
CHGCLUVER (Q)[1]	Program usługowy QCSTCTL2	*USE	
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
	Opis kontrolera	*USE, *OBJMGT	
	Opis linii	*USE, *OBJMGT	
	Opis serwera sieciowego	*USE, *OBJMGT	
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	
	Opis kontrolera	*USE, *OBJMGT	
	Opis linii	*USE, *OBJMGT	
	Opis serwera sieciowego	*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	
	Opis kontrolera	*USE, *OBJMGT	
	Opis linii	*USE, *OBJMGT	
	Opis serwera sieciowego	*USE, *OBJMGT	
CRTADMDMN (Q)[1, 3]	Profil użytkownika QCLUSTER	*USE	
CRTCLU (Q)[1]	Program usługowy QCSTCTL	*USE	

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
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
	Opis kontrolera	*USE, *OBJMGT	
	Opis linii	*USE, *OBJMGT	
	Opis serwera sieciowego	*USE, *OBJMGT	
DLTADMDMN (Q) [1]	Grupa zasobów klastra	*OBJEXIST, *USE	
	QUSRSYS	*EXECUTE	
	QCLUSTER	*USE	
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	
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	

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
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	
	Opis kontrolera	*USE, *OBJMGT	
	Opis linii	*USE, *OBJMGT	
	Opis serwera sieciowego	*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	
	Opis kontrolera	*USE, *OBJMGT	
	Opis linii	*USE, *OBJMGT	
	Opis serwera sieciowego	*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	
	Opis kontrolera	*USE, *OBJMGT	
	Opis linii	*USE, *OBJMGT	
	Opis serwera sieciowego	*USE, *OBJMGT	
WRKCLU[4]	Grupa zasobów klastra	*USE	*EXECUTE

[1] Do użycia tej komendy konieczne jest uprawnienie specjalne (*IOSYSCFG).

[2] Uprawnienie dotyczy profilu wywołującego użytkownika i profilu użytkownika, który ma uruchomić program wyjściowy.

[3] Profil wywołującego użytkownika otrzymuje uprawnienia *CHANGE oraz *OBJEXIST dla grupy zasobów klastra.

[4] Użytkownik musi posiadać uprawnienie specjalne *SERVICE lub być upoważnionym do korzystania z funkcji śledzenia usług (Service Trace) systemu i5/OS za pośrednictwem programu Administrowanie aplikacją produktu System i 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 *CMD

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend związanych z działaniami na komendzie.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
CHGCMD	Komenda	*OBJMGT	*EXECUTE
CHGCMDDFT	Komenda	*OBJMGT, *USE	*EXECUTE
CHGPRXCMD	Komenda proxy	*OBJMGT	*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.
CRTPRXCMD	Komenda proxy: REPLACE(*NO)		*READ, *ADD
	Komenda proxy: REPLACE(*YES)	Patrz Zasady ogólne na stronie D-2	Patrz Zasady ogólne na stronie D-2
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

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend kontroli transakcji.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
COMMIT			
ENDCMTCTL	Kolejka komunikatów, jaką podano w słowie kluczowym NFYOBJ dla związanej z nim komendy STRCMTCTL.	*OBJOPR, *ADD	*EXECUTE
ROLLBACK			

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
STRCMTCTL	Kolejka komunikatów, gdy podano słowo kluczowe NFYOBJ	*OBJOPR, *ADD	*EXECUTE
	Obszar danych określony w słowie kluczowym NFYOBJ dla przypisanej komendy STRCMTCTL	*CHANGE	*EXECUTE
	Zbiory, określone w słowie kluczowym NFYOBJ dla przypisanej komendy STRCMTCTL	*OBJOPR *READ	*EXECUTE
WRKCMTDFN [1]			

[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

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane przez poszczególne komendy informacji po stronie komunikacyjnej

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla 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

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend konfiguracji.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
PRTDEVADR	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis urządzenia	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
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	Uprawnienia	*OBJOPR	*EXECUTE
RTVCFGSRC	Uprawnienia	*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, 5, 6, 7]	Uprawnienia	*USE, *OBJMGT	*EXECUTE
WRKCFGSTS [4]	Uprawnienia	*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 określić wartość inną niż *NONE dla parametru Zezwalaj na różnice w obiektach (Allow object differences - ALWOBJDIF), lub RESETSYS(*YES), użytkownik musi posiadać specjalne uprawnienia.

6 Użytkownik musi posiadać specjalne uprawnienie *IOSYSCFG, jeśli obiekt jest biblioteką nośnika i posiada status*ALLOCATE lub *DEALLOCATE.

7 Aby określić GENPTHCERT(*YES), użytkownik musi posiadać uprawnienia specjalne *IOSYSCFG oraz *SECADM.

Komendy list konfiguracji

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend list konfiguracji.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend listy połączeń.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy opisu kontrolera.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	Dla 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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla biblioteki**
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		
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		

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla biblioteki**
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 kryptograficzne

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy kryptograficzne.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla biblioteki**
ADDCKMKSFE	Zbiór użytkownika	*ADD, *OBJOPR, *READ	
	Biblioteka użytkownika		*EXECUTE
	Katalog użytkownika	*X	
	Plik strumieniowy użytkownika	*R	
ADDCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
	Kolejka komunikatów QHST	*OBJOPR, *ADD	*EXECUTE
ADDMSTPART (Q) [1]			
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
CHKMSTKVV (Q) [1]			
CLRMSTKEY (Q) [1]			
CPHDTA (Q)			

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla biblioteki**
CRTCKMKSF	Biblioteka użytkownika		*ADD, *EXECUTE
DSPCKMKSFE	Zbiór użytkownika	*OBJOPR, *READ	
	Biblioteka użytkownika		*EXECUTE
ENCCPHK (Q)			
ENCFRMMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
ENCTOMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
GENCKMKSFE	Zbiór użytkownika	*ADD, *OBJOPR, *READ	
	Biblioteka użytkownika		*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
RMVCKMKSFE	Zbiór użytkownika	*DLT, *OBJOPR	
	Biblioteka użytkownika		*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
SETMSTKEY (Q) [1]			
TRNCKMKSF	Zbiór użytkownika	*OBJOPR, *READ, *UPD	
	Biblioteka użytkownika		*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

1 Korzystanie z tej komendy wymaga posiadania uprawnień specjalnych *ALLOBJ i *SECADM.

Komendy obszaru danych

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy obszaru danych.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla biblioteki**
CHGDTAARA [1]	Obszar danych	*CHANGE	*EXECUTE
CRTDTAARA [1]	Obszar danych		*READ, *ADD
	Opis urządzenia APPC [4]	*CHANGE	

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla biblioteki**
DLTDTAARA	Obszar danych	*OBJEXIST	*EXECUTE
DSPDTAARA	Obszar danych	*USE	*EXECUTE
RTVDTAARA [2]	Obszar danych	*USE	*EXECUTE
WRKDTAARA [3]	Obszar danych	Dowolne uprawnienia	*USE

[1] Jeśli komendy tworzenia i zmiany obszaru danych są uruchamiane za pomocą funkcji języka wysokiego poziomu, to posiadanie tych uprawnień jest konieczne, mimo że same komendy ich nie wymagają.

[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 kolejki danych

W tabeli podano uprawnienia szczegółowe, niezbędne do korzystania z komend kolejki 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 opisu urządzenia

Poniższa tabela zawiera uprawnienia szczegółowe, wymagane przy komendach opisu urządzenia.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla biblioteki**
CFGDEVMLB [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGASPA (Q)			
CHGASPACT (Q)[7]	Opis urządzenia	*USE	
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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla biblioteki**
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
CHGDEVMLB [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVNET [4]	Opis urządzenia	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVNWSH[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		
CRTDEVNWSH[4]	Opis urządzenia		*EXECUTE
CRTDEVOPT [4]	Opis urządzenia		*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla biblioteki**
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		
CRTDEVTAP [4]	Opis kontrolera (CTL)	*USE	*EXECUTE
	Opis urządzenia		
DLTDEVD [1]	Opis urządzenia	*OBJEXIST	*EXECUTE
DSPASPSTS	Opis urządzenia	*USE	
DSPCNNSTS	Opis urządzenia	*OBJOPR	*EXECUTE
DSPDEVD	Opis urządzenia	*USE	*EXECUTE
ENDASPBAL (Q)			
ENDDEVRCY	Opis urządzenia	*USE	*EXECUTE
HLDCMNDEV [2]	Opis urządzenia	*OBJOPR	*EXECUTE
PRTCMNSEC [4, 5]			
RLSCMNDEV	Opis urządzenia	*OBJOPR	*EXECUTE
RSMDEVRCY	Opis urządzenia	*USE	*EXECUTE
SETASPGRP[6]	Wszystkie opisy urządzeń w grupie ASP	*USE	
	Zostają zmienione wszystkie określone biblioteki z listy bibliotek, przed przestrzenią nazw i listą bibliotek.	*USE	
STRASPBAL (Q)			
TRCASPBAL (Q)			
WRKDEVD [3]	Opis urządzenia	*OBJOPR	*EXECUTE

| [1] Usunięcie kolejki wyjściowej wymaga uprawnień istnienia obiektu (*OBJEXIST) do kolejki wyjściowej oraz uprawnień wykonawczych (*EXECUTE) do 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.

[6] Gdy dla grupy ASP (ASPGRP) lub bibliotek bieżącego wątku (USRLIBL) określono parametr *CURUSR, wymagane są też uprawnienia wykonawcze (*EXECUTE) do biblioteki, w której znajduje się opis zadania, oraz uprawnień odczytu (*READ) do opisu zadania podanego w danych profilu użytkownika.

| [7] Uruchomienie tej komendy wymaga uprawnienia specjalnego *JOBCTL.

Komendy emulacji urządzenia

Poniższa tabela zawiera uprawnienia szczegółowe, wymagane przy komendach emulacji urządzenia.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla 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
STREML3270	Zbiór konfiguracyjny emulacji	*OBJOPR	*EXECUTE
	Urządzenie emulowane, opis kontrolera emulowanego, urządzenie stacji roboczej i opis kontrolera stacji roboczej	*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 katalogów i tworzenia cienia katalogów

Poniższa tabela zawiera uprawnienia szczegółowe, wymagane przy komendach katalogów i tworzenia cienia katalogów.

Te komendy nie wymagają żadnych uprawnień do obiektu:			
ADDDIRE [2] ADDDIRSHD [1] CHGSYSDIRA [2] CHGDIRE [3]	CHGDIRSHD [1] CPYFRMDIR [1] CPYTODIR [1] DSPDIRE	ENDDIRSHD [4] RMVDIRE [1] RMVDIRSHD [1] RNMDIRE [2]	STRDIRSHD [4] WRKDIRE [3,5] WRKDIRLOC [1,5] 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 serwera katalogów

Poniższa tabela zawiera uprawnienia szczegółowe, wymagane przy komendach serwera katalogów.

		Wymagane uprawnienie	
Komenda	**Obiekt odniesienia**	**Dla obiektu**	**Dla biblioteki**
CHGDIRSRVA [1]			
CPYTOLDIF [2]	Plik strumieniowy LDIF (jeśli już istnieje)	*STMF	*W, *OBJEXIST, *OBJMGT
	Katalog nadrzędny lub plik strumieniowy LDIF	*DIR	*WX
CPYFRMLDIF [2]	Plik strumieniowy LDIF	*STMF	*R
	Katalog nadrzędny lub plik strumieniowy LDIF	*DIR	*X
DB2LDIF [2]	Plik strumieniowy LDIF (jeśli już istnieje)	*STMF	*W, *OBJEXIST, *OBJMGT
	Katalog nadrzędny lub plik strumieniowy LDIF	*DIR	*WX
LDIF2DB [2]	Plik strumieniowy LDIF	*STMF	*R
	Katalog nadrzędny lub plik strumieniowy LDIF	*DIR	*X

[1] Wymagane uprawnienia specjalne *ALLOBJ i *IOSYSCFG.

[2] Aby użyć tej komendy, należy spełnić następujące wymagania:
- Posiadać uprawnienia specjalne *ALLOBJ i *IOSYSCFG
- Wprowadzić nazwę wyróżniającą oraz hasło administratora
- Być administratorem serwera katalogów

Komendy dysków

Poniższa tabela zawiera uprawnienia szczegółowe, wymagane przy komendach dysków.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo 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 funkcji tranzytu terminalu

Poniższa tabela zawiera uprawnienia szczegółowe, wymagane przy komendach funkcji tranzytu terminalu.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

		Wymagane uprawnienie	
Komenda	**Obiekt odniesienia**	**Dla obiektu**	**Dla 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 w systemie docelowym musi mieć uprawnienie do tego obiektu.

Komendy dystrybucji

Poniższa tabela zawiera uprawnienia szczegółowe, wymagane przy komendach dystrybucji.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

		Wymagane uprawnienie	
Komenda	**Obiekt odniesienia**	**Dla obiektu**	**Dla biblioteki**
ADDDSTQ (Q)			
ADDDSTRTE (Q)			
ADDDSTSYSN (Q)			
CFGDSTSRV (Q)			
CFGRPDS (Q)			
CHGDSTD [1]	Dokument [2]	*CHANGE	*EXECUTE
CHGDSTQ (Q)			

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	Dla biblioteki
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)			
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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy list dystrybucyjnych.

Te komendy nie wymagają żadnych uprawnień do obiektu:			
ADDDSTLE [1] CHGDSTL[1]	CRTDSTL DLTDSTL [1]	DSPDSTL RMVDSTLE [1]	RNMDSTL [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

Poniższa tabela zawiera uprawnienia szczegółowe, wymagane przy komendach obiektów biblioteki dokumentów.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	Dla biblioteki
ADDDLOAUT	Obiekt biblioteki dokumentów	*ALL lub właściciel	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla biblioteki**
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
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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla biblioteki**
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
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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla biblioteki**
RSTDLO (Q)[7, 8, 9]	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 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
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 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	

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla biblioteki**
[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 katalog i wszystkie znajdujące się w nim obiekty, użytkownik musi posiadać uprawnienie *ALL dla wszystkich obiektów znajdujących się w katalogu.			
[4] Jeśli użytkownik ma uprawnienia specjalne *ALLOBJ lub *SECADM, nie potrzebuje uprawnień *ALL do listy biblioteki dokumentów.			
[5] Użytkownik musi posiadać uprawnienia dla obiektu będącego źródłem scalania. Na przykład, jeśli określono MRGTYPE(*QRY), należy wykorzystać uprawnienia dla zapytania określonego dla parametru QRYDFN.			
[6] W liście dokumentów zbioru wyjściowego zwracane są tylko obiekty spełniające kryteria zapytania, dla których użytkownik posiada co najmniej uprawnienie *USE.			
[7] Użytkownik musi posiadać uprawnienia *SAVSYS lub *ALLOBJ albo być zarejestrowany w katalogu dystrybucyjnym systemu.			
[8] Użytkownik musi posiadać uprawnienia specjalne *SAVSYS lub *ALLOBJ, aby móc korzystać z kombinacji parametrów RSTDLO DLO(*MAIL).			
[9] Aby określić wartość inną niż *NONE dla parametru Zezwalaj na różnice w obiektach (Allow object differences - ALWOBJDIF), użytkownik musi posiadać specjalne uprawnienia.			
[10] Jeśli użytkownik ma uprawnienia specjalne *SAVSYS lub *ALLOBJ, nie potrzebuje podanych tu uprawnień.			
[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] Użytkownik musi posiadać uprawnienia specjalne *SAVSYS lub *ALLOBJ, aby móc korzystać z następujących kombinacji parametrów: • 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. Funkcja obsługi nośnika optycznego obsługuje połączenie między woluminem optycznym i listą autoryzacji, zabezpieczające wolumin.			
[20] Użytkownik musi posiadać uprawnienia specjalne *ALLOBJ, jeśli OWNER (*ALL) lub OWNER (nazwa) są innym wywołującym profilem użytkownika.			
[21] Aby móc skorzystać z tej komendy, użytkownik musi posiadać uprawnienia specjalne *ALLOBJ lub *AUDIT.			
[22] Aby móc skorzystać z tej komendy podczas określania klasy obiektów *DST, która ma zostać zlokalizowana, użytkownik musi posiadać uprawnienia specjalne *ALLOBJ.			

Komendy systemu nazw domen

Poniższa tabela zawiera uprawnienia szczegółowe, wymagane przy komendach serwera nazw domen (DNS).

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla biblioteki**
CHKDNSCFG [1]	Istniejący zbiór konfiguracyjny	*R	
	Ścieżka do istniejącego zbioru konfiguracyjnego	*X	
	Istniejący zbiór wyjściowy	*W	
	Ścieżka do istniejącego zbioru wyjściowego	*X	
	Rodzic nowego zbioru wyjściowego	*RX	
CHKDNSZNE [1]	Istniejący zbiór strefy	*R	
	Ścieżka do istniejącego zbioru strefy	*X	
	Istniejący zbiór wyjściowy	*W	
	Ścieżka do istniejącego zbioru wyjściowego	*X	
	Rodzic nowego zbioru wyjściowego	*RX	
CRTRNDCCFG [1]	Istniejący zbiór źródłowy entropii	*R	
	Ścieżka do istniejącego zbioru źródłowego entropii	*X	
	Istniejący zbiór wyjściowy	*W	
	Ścieżka do istniejącego zbioru wyjściowego	*X	
	Rodzic nowego zbioru wyjściowego	*RX	
RUNDNSUPD	Istniejący zbiór wejściowy zadania wsadowego	*R	
	Ścieżka do istniejącego zbioru wejściowego zadania wsadowego	*X	
	Istniejący plik kluczy	*R	
	Ścieżka do istniejącego pliku kluczy	*X	
	Istniejący zbiór wyjściowy	*W	
	Ścieżka do istniejącego zbioru wyjściowego	*X	
	Rodzic nowego zbioru wyjściowego	*RX	
RUNRNDCCMD	Istniejący zbiór konfiguracyjny RNDC	*R	
	Ścieżka do istniejącego zbioru konfiguracyjnego RNDC	*X	
	Istniejący plik kluczy	*R	
	Ścieżka do istniejącego pliku kluczy	*X	
	Istniejący zbiór wyjściowy	*W	
	Ścieżka do istniejącego zbioru wyjściowego	*X	
	Rodzic nowego zbioru wyjściowego	*RX	

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	Dla biblioteki
STRDIGQRY	Istniejący zbiór wejściowy zadania wsadowego	*R	
	Ścieżka do istniejącego zbioru wejściowego zadania wsadowego	*X	
	Istniejący plik zaufanych kluczy	*R	
	Ścieżka do istniejącego pliku zaufanych kluczy	*X	
	Istniejący plik kluczy	*R	
	Ścieżka do istniejącego pliku kluczy	*X	
	Istniejący zbiór wyjściowy	*W	
	Ścieżka do istniejącego zbioru wyjściowego	*X	
	Rodzic nowego zbioru wyjściowego	*RX	
STRHOSTQRY	Istniejący zbiór wyjściowy	*W	
	Ścieżka do istniejącego zbioru wyjściowego	*X	
	Rodzic nowego zbioru wyjściowego	*RX	
[1] Aby uruchomić komendę, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.			

Komendy zestawu znaków dwubajtowych

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend zestawu znaków dwubajtowych.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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
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

Poniższa tabela zawiera uprawnienia szczegółowe, wymagane przy komendach opisu edycji.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla 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 zmiennej środowiskowej

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend 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

Poniższa tabela zawiera uprawnienia szczegółowe, wymagane przy komendach konfiguracji rozszerzonej bezprzewodowej sieci.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla 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
RMVEWCPTCE	Zbiór źródłowy	*USE	*EXECUTE

Komendy zbiorów

W poniższej tabeli zamieszczono uprawnienia szczegółowe wymagane dla komend zbiorów.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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
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

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
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 oraz (*OBJMGT lub *OBJALTER).	*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.
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
	komenda CRTDDMF	*USE	*USE

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
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)	*WX	*X
	Docelowy zbiór bazy danych, jeśli podano MBROPT(*REPLACE lub *NONE)	*WX, *OBJMGT	*X
	Docelowy zbiór bazy danych, jeśli utworzono nowy podzbiór	*WX	*X, *ADD
	Tabela konwersji *TBL używana do tłumaczenia danych	*R	*X
	Docelowy zbiór składowania istnieje	*RWX, *OBJMGT	*X
	Docelowy zbiór składowania jest tworzony		*RWX
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
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
	komenda CRTDDMF	*USE	*USE

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
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	
	Jeśli podano AUT(*FILE) lub AUT(*INDIRFILE), zbiór bazy danych i plik strumieniowy	*OBJMGT	
	Tabela konwersji *TBL używana do tłumaczenia danych	*R	*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 uprawnienia	
		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

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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 uprawnienia	
		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 uprawnienia	
		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
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

W poniższej tabeli zamieszczono uprawnienia szczegółowe wymagane dla komend filtrów.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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 uprawnienia	
		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

W poniższej tabeli zamieszczono uprawnienia szczegółowe wymagane dla komend finansowych.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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.			

Komendy programu Graphical Operations i5/OS

W poniższej tabeli zamieszczono uprawnienia szczegółowe wymagane dla komend programu Graphical Operations i5/OS.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
CHGFCNUSG[5]			
DSPFCNUSG			
EDTWSOAUT	Obiekt stacji roboczej [1]	*OBJMGT [2,3,4]	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
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
WRKFCNUSG			

[1] Obiekt stacji roboczej to obiekt wewnętrzny, który tworzony jest podczas instalowania opcji i5/OS 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 usunąć istniejącą listę autoryzacji, użytkownik musi posiadać jedno z następujących uprawnień:

- 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

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend zestawu symboli graficznych.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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

W poniższej tabeli zamieszczono uprawnienia szczegółowe wymagane dla komend serwera hosta.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Te komendy nie wymagają uprawnień do obiektu.			
ENDHOSTSVR (Q)		STRHOSTSVR (Q)	

Komendy katalogu obrazów

W poniższej tabeli zamieszczono uprawnienia szczegółowe wymagane dla komend katalogu obrazów

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Typ obiektu	Wymagane uprawnienia	
			Do obiektu	Do biblioteki[1]
ADDIMGCLGE	Katalog obrazów	*IMGCLG	*CHANGE	*EXECUTE
	Przedrostek ścieżki katalogu obrazów	*DIR	*X	
	Nazwa urządzenia, jeśli określono FROMDEV	*DEVD	*USE	
	Zbiór obrazu, jeśli określono FROMFILE	*STMF	*R, *OBJMGT	
	Przedrostek ścieżki zbioru obrazu, jeśli określono FROMFILE	*DIR	*X	
	Katalog nadrzędny zbioru obrazu, jeśli określono FROMFILE	*DIR	*RX	
CHGIMGCLG	Katalog obrazów	*IMGCLG	*CHANGE	*EXECUTE
	Przedrostek ścieżki katalogu obrazów	*DIR	Patrz zasady ogólne	
	Nowy przedrostek ścieżki katalogu obrazów, jeśli określono parametr DIR	*DIR	Patrz zasady ogólne	
CHGIMGCLGE	Katalog obrazów	*IMGCLG	*CHANGE	*EXECUTE
	Przedrostek ścieżki katalogu obrazów	*DIR	Patrz zasady ogólne	
CRTIMGCLG	QUSRSYS	*LIB		*READ, *ADD
	Katalog obrazów, jeśli określono DIR(*REFIMGCLG)	*IMGCLG	*USE	*OBJOPR, *READ, *ADD, *EXECUTE
	Przedrostek ścieżki katalogu obrazów[2]	*DIR	Patrz zasady ogólne	
DLTIMGCLG	Katalog obrazów	*IMGCLG	*OBJEXIST	*EXECUTE
	Przedrostek ścieżki katalogu obrazów	*DIR	Patrz zasady ogólne	
LODIMGCLG	Katalog obrazów	*IMGCLG	*USE	*EXECUTE
	Katalog obrazów, jeśli określono WRTPTC(*ALL) lub WRTPTC(*NONE)	*IMGCLG	*CHANGE	*EXECUTE
	Urządzenie wirtualne	*DEVD	*USE	
	Przedrostek ścieżki katalogu obrazów	*DIR	Patrz zasady ogólne	
LODIMGCLGE	Katalog obrazów	*IMGCLG	*USE	*EXECUTE
	Przedrostek ścieżki katalogu obrazów	*DIR	Patrz zasady ogólne	
RMVIMGCLGE	Katalog obrazów	*IMGCLG	*CHANGE	*EXECUTE
	Przedrostek ścieżki katalogu obrazów	*DIR	Patrz zasady ogólne	
RTVIMGCLG	Katalog obrazów	*IMGCLG	*USE	*EXECUTE
	Opis urządzenia, jeśli określono parametr DEV	*DEVD	*USE	
VFYIMGCLG	Katalog obrazów	*IMGCLG	*USE	*EXECUTE
	Urządzenie wirtualne	*DEVD	*USE	
	Przedrostek ścieżki katalogu obrazów	*DIR	Patrz zasady ogólne	
WRKIMGCLG	Katalog obrazów	*IMGCLG	*USE	*EXECUTE
WRKIMGCLGE	Katalog obrazów	*IMGCLG	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Typ obiektu	Wymagane uprawnienia	
			Do obiektu	Do biblioteki[1]

[1] Biblioteka, w której znajdują się obiekty katalogu obrazów, to QUSRSYS.

[2] Jeśli katalog zostanie utworzony, użytkownik musi posiadać uprawnienie *W dla katalogu, w którym znajdować się ma nowy katalog.

Komendy zintegrowanego systemu plików

W poniższej tabeli zamieszczono uprawnienia szczegółowe wymagane dla komend zintegrowanego systemu plików.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu [1]
ADDLNK	Obiekt , jeśli określono LNKTYPE(*HARD)	*STMF	QOpenSys, ″root″ (/),UDFS	*OBJEXIST
	Dowiązanie nadrzędne do nowego dowiązania	*DIR	QOpenSys, ″root″ (/),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, jeśli ustawiany jest atrybut inny niż *USECOUNT, *ALWCKPWRT, *DISKSTGOPT, *MAINSTGOPT, *ALWSAV, *SCAN, *CRTOBJSCAN, *SETUID, *SETGID, *RSTRDRNMUNL, *CRTOBJAUD	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, jeśli ustawiane są następujące atrybuty: *CRTOBJSCAN lub *SCAN[26]	*DIR i *STMF	QOpenSys, ″root″ (/),UDFS	
	Obiekt, jeśli ustawiane są następujące atrybuty: *SETUID, *SETGID, *RSTDRNMUNL	Dowolne	Wszystkie z wyjątkiem QSYS.LIB i QDLS	Prawo własności [15]
	*CRTOBJAUD[9]			
	Przedrostek ścieżki[9]	Więcej informacji znajduje się w zasadach ogólnych.		
CHGAUD [4]				
CHGAUT	Obiekt	Wszystkie	QOpenSys, ″root″ (/),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
	Katalog zawierający obiekty, jeśli określono SUBTREE(*ALL)	Dowolny katalog lub biblioteka	Wszystkie	*RX
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 [24]	Obiekt	Wszystkie	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		Wszystkie	QOpenSys, ″root″ (/),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
	Katalog zawierający obiekty, jeśli określono SUBTREE(*ALL)	Dowolny katalog lub biblioteka	Wszystkie	*RX
CHGPGP	Obiekt	Wszystkie	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		Wszystkie	QOpenSys, ″root″ (/),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
	Katalog zawierający obiekty, jeśli określono SUBTREE(*ALL)	Dowolny katalog lub biblioteka	Wszystkie	*RX
CHKIN	Obiekt, jeśli jest to użytkownik, który sprawdzał.	*STMF	QOpenSys, ″root″ (/),UDFS	*W
		*DOC	QDLS	*W
	Obiekt, jeśli nie jest to użytkownik, który sprawdzał.	*STMF	QOpenSys, ″root″ (/),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, ″root″ (/),UDFS	*X
	Katalog zawierający obiekty, jeśli określono SUBTREE(*ALL)	Dowolny katalog	Wszystkie	*RX
	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, ″root″ (/),UDFS	*W
		*DOC	QDLS	*W
	Katalog zawierający obiekty, jeśli określono SUBTREE(*ALL)	Dowolny katalog	Wszystkie	*RX
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
CPY[25]	Kopiowany obiekt, obiekt źródłowy	Dowolne	QOpenSys, ″root″ (/),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, ″root″ (/),UDFS	*RX, *OBJMGT
CPY[25]	Ścieżka (docelowa), katalog nadrzędny obiektu docelowego	*FILE	QSYS.LIB	*RX, *OBJMGT
		*LIB	QSYS.LIB	*RX, *ADD
		*DIR	QOpenSys, ″root″ (/),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, ″root″ (/),UDFS	*X
		*FLR	QDLS	*X
		Pozostałe	QSYS.LIB	*RX
		*DDIR	QOPT[11]	*X
	Przedrostek ścieżki (miejsce docelowe)	*LIB	QSYS.LIB	*WX
		*DIR	QOpenSys, ″root″ (/),UDFS	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
	Przedrostek ścieżki (obiekt źródłowy)	*DDIR	QOPT[11]	*X
CPYFRMSTMF	Patrz sekcja “Komendy zbiorów” na stronie 394			
CPYTOSTMF	Patrz sekcja “Komendy zbiorów” na stronie 394			
CRTDIR[21, 22]	Katalog nadrzędny	*DIR	QOpenSys, ″root″ (/),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, ″root″ (/),UDFS	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*DIR		*R
		*DDIR	QOPT[11]	*RX
DSPCURDIR	Katalog bieżący	*DIR	QOpenSys, ″root″ (/),UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DIR		*R
		*DDIR	QOPT[11]	*X
	Wolumin optyczny	*DDIR*	QOPT[8]	*USE

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu [1]
DSPF	Zbiór bazy danych	*FILE	QSYS.LIB	*USE
	Biblioteka zbioru bazy danych	*LIB	QSYS.LIB	*EXECUTE
	Plik strumieniowy	*STMF	QOpenSys, ″root″ (/), UDFS	*R
		*USRSPC	QSYS.LIB	*USE
	Przedrostek ścieżki	Patrz zasady ogólne		
DSPLNK	Dowolne	Dowolne	″root″ (/), QOpenSys, UDFS QSYS.LIB[27], QDLS, QOPT[11]	Brak
	Zbiór, opcja 12 (praca z dowiązaniami)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	″root″ (/), QOpenSys, UDFS	*R
DSPLNK	Obiekt dowiązania symbolicznego	*SYMLNK	″root″ (/), QOpenSys, UDFS	Brak
	Wolumin optyczny	*DDIR	QOPT[8]	*USE
	Katalog nadrzędny obiektu odniesienia - brak wzorca [13]	*DIR	″root″ (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Katalog nadrzędny obiektu odniesienia - podano wzorzec [13]	*DIR	″root″ (/), QOpenSys, UDFS	*R
		*LIB, *FILE	QSYS.LIB[27]	*R
		*FLR	QDLS	*R
		*DDIR	QOPT[11]	*R
		*DDIR		*R
	Katalog nadrzędny obiektu odniesienia - opcja 8 (Wyświetl atrybuty)	*DIR	″root″ (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*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 (Praca z dowiązaniami)	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*SYMLNK	″root″ (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Przedrostek nadrzędnego obiektu odniesienia - brak wzorca [13]	*DIR	″root″ (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Przedrostek nadrzędnego obiektu odniesienia - podano wzorzec [13]	*DIR	″root″ (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Przedrostek nadrzędnego obiektu odniesienia - opcja 8 (Wyświetl atrybuty)	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Przedrostek macierzystego obiektu odniesienia - opcja 12 (praca z dowiązaniami)	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*SYMLNK	″root″ (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*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	″root″ (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Względna nazwa ścieżki [14] : bieżący katalog roboczy zawierający obiekt - podany wzorzec [13]	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB[27]	*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	″root″ (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB[27]	*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	″root″ (/), QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB[27]	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
DSPMFSINF	Obiekt	Dowolne	Dowolne	Brak
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
EDTF	Zbiór bazy danych, istniejący podzbiór	*FILE	QSYS.LIB	*CHANGE
	Biblioteka zbioru bazy danych	*LIB	QSYS.LIB	*EXECUTE
	Zbiór bazy danych, nowy podzbiór	*FILE	QSYS.LIB	*CHANGE, *OBJMGT
	Biblioteka zbioru bazy danych, nowy podzbiór	*LIB	QSYS.LIB	*EXECUTE, *ADD
	Plik strumieniowy, istniejący plik	*STMF	QOpenSys, ″root″ (/), UDFS	*R
	Przestrzeń użytkownika	*USRSPC	QSYS.LIB	*CHANGE
	Katalog nadrzędny podczas tworzenia nowego pliku strumieniowego	*DIR	QOpenSys, ″root″ (/), UDFS	*WX
	Przedrostek ścieżki	Patrz zasady ogólne		

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu [1]
ENDJRN	Obiekt	*DIR jeśli parametr Subtree (*ALL)	QOpenSys, ″root″ (/),UDFS	*R, *X, *OBJMGT
		*DIR jeśli parametr Subtree (*NONE), *SYMLNK, *STMF	QOpenSys, ″root″ (/),UDFS	*R, *OBJMGT
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT
	Katalog nadrzędny	*DIR	QOpenSys, ″root″ (/),UDFS	*X
		*LIB	QSYS.LIB	*X
	Kronika	*JRN	QSYS.LIB	*OBJMGT, *OBJOPR
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
MOV[19]	Obiekt przeniesiony w obrębie tego samego systemu plików	*DIR	QOpenSys, ″root″ (/)	*OBJMGT, *W
		Nie *DIR	QOpenSys, ″root″ (/)	*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, ″root″ (/),UDFS	*WX
		*FLR	QDLS	*RWX
		*FILE	QSYS.LIB, ″root″ (/)	*RX, *OBJEXIST
		pozostałe	QOpenSys, ″root″ (/)	*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 pomiędzy systemami plików, doQOpenSys, ″root″ (/) lub QDLS (tylko pliki strumieniowe *STMF i *DOC, *MBR) .	*STMF	QOpenSys, ″root″ (/),UDFS	*R, *OBJEXIST, *OBJMGT
		*DOC	QDLS	*ALL
		*MBR	QSYS.LIB	Nie dotyczy
		*DSTMF	QOPT[11]	*RW
MOV	Przeniesiony do systemu QSYS, *MBR	*STMF	QOpenSys, ″root″ (/),UDFS	*R, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*ALL
		*DSTMF	QOPT[11]	*RW
MOV	Wolumin optyczny (źródłowy i docelowy)	*DDIR	QOPT[8]	*CHANGE
	Ścieżka (źródłowa), przeniesiony poprzez systemy plików, katalog nadrzędny	*DIR	QOpenSys, ″root″ (/),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.		
RCLLNK[16]				
RLSIFSLCK [18]	object (obiekt)	*STMF	″root″ (/), QOpenSys, UDFS	*R
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
RMVDIR[19,20]	Katalog	*DIR	QOpenSys, ″root″ (/),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, ″root″ (/),UDFS	*WX
		*FLR	QDLS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*DDIR	QOPT[11]	*WX
	Katalog zawierający obiekty, jeśli określono SUBTREE(*ALL)	Dowolny katalog	Wszystkie	*RX
	Wolumin optyczny	*DDIR	QOPT[8]	*CHANGE
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
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, ″root″ (/),UDFS	*OBJEXIST
RMVLNK	Katalog nadrzędny	*FLR	QDLS	*X
		*FILE	QSYS.LIB	*X, *OBJEXIST
		*LIB	QSYS.LIB	*X
		*DIR	QOpenSys, ″root″ (/),UDFS	*WX
		*DDIR	QOPT[11]	*WX
	Wolumin optyczny	*DDIR	QOPT[8]	*CHANGE
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
RNM[19]	Obiekt	*DIR	QOpenSys, ″root″ (/),UDFS	*OBJMGT, *W
		Nie *DIR	QOpenSys, ″root″ (/),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, ″root″ (/),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, ″root″ (/), UDFS, QDLS	*X
RST (Q) [23, 28, 30]	Obiekt, jeśli istnieje [2]	Dowolne	QOpenSys, ″root″ (/),UDFS	*W, *OBJEXIST
			QSYS.LIB	Zależności [10]
			QDLS	*ALL
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
	Katalog nadrzędny utworzony przez operację odtwarzania, ze względu na CRTPRNDIR(*YES)[2]	*DIR	QOpenSys, ″root″ (/),UDFS	*WX
	Właściciel katalogu nadrzędnego, określony przez parametr PRNDIROWN[2, 6]	*USRPRF	QSYS.LIB	*ADD
RST (Q)	Katalog nadrzędny odtwarzanego obiektu [2]	*DIR	QOpenSys, ″root″ (/),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 optyczna lub zbiór składowania	*DEVD, *FILE	QSYS.LIB	*RX
	Definicja nośnika	*MEDDFN	QSYS.LIB	*USE
RST (Q)	Biblioteka opisu urządzenia, definicji nośnika lub zbioru składowania	*LIB	QSYS.LIB	*EXECUTE
	Zbiór wyjściowy, jeśli został podany	*STMF	QOpenSys, ″root″ (/),UDFS	*W
		*USRSPC	QSYS.LIB	*RWX
	Przedrostek ścieżki zbioru wyjściowego	*DIR	QOpenSys, ″root″ (/),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, ″root″ (/), UDFS, QDLS, QOPT[11]	*RX
		*DDIR	QOPT[11]	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		Dowolne		*R
RTVCURDIR	Katalog bieżący	*DIR	QOpenSys, ″root″ (/), UDFS, QOPT [11]	*X
		*DDIR	QOPT[11]	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		Dowolne		*R
SAV[29]	Obiekt [2]	Dowolne	QOpenSys, ″root″ (/),UDFS	*R, *OBJEXIST
			QSYS.LIB	Zależności [10]
			QDLS	*ALL
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
	Jednostka taśm, jednostka optyczna	*DEVD	QSYS.LIB	*RX
	Definicja nośnika	*MEDDFN	QSYS.LIB	*USE
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, definicji nośnika, zbioru składowania, lub kolejki składowania podczas użycia	*LIB	QSYS.LIB	*EXECUTE
SAV	Zbiór wyjściowy, jeśli został podany	*STMF	QOpenSys, ″root″ (/),UDFS	*W
		*USRSPC	QSYS.LIB	*RWX
	Przedrostek ścieżki zbioru wyjściowego	*DIR	QOpenSys, ″root″ (/),UDFS	*X
		*LIB	QSYS.LIB	*RX

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu [1]
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, ″root″ (/),UDFS	*R, *X, *OBJMGT
		*DIR jeśli parametr Subtree (*NONE), *SYMLNK, *STMF	QOpenSys, ″root″ (/),UDFS	*R, *OBJMGT
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT
	Katalog nadrzędny	*DIR	QOpenSys, ″root″ (/),UDFS	*X
		*LIB	QSYS.LIB	*X
	Kronika	*JRN	QSYS.LIB	*OBJMGT, *OBJOPR
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
WRKAUT[6, 7]	Obiekt	*DOC lub *FLR	QDLS	*ALL
		Wszystkie	Nie QDLS	*OBJMGT lub prawo własności
		*DDIR i *DSTMF	QOPT[11]	*NONE
	Wolumin optyczny	*DDIR	QOPT[8]	*USE
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu [1]
WRKLNK	Dowolne	Dowolne	″root″ (/), QOpenSys, UDFS, QSYS.LIB[27], QDLS, QOPT[11]	Brak
	Zbiór, opcja 12 (praca z dowiązaniami)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	″root″ (/), QOpenSys, UDFS	*R
	Obiekt dowiązania symbolicznego	*SYMLNK	″root″ (/), QOpenSys, UDFS	Brak
	Wolumin optyczny	*DDIR	QOPT[8]	*USE
WRKLNK	Katalog nadrzędny obiektu odniesienia - brak wzorca [13]	*DIR	″root″ (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Katalog nadrzędny obiektu odniesienia - podano wzorzec	*DIR	″root″ (/), QOpenSys, UDFS	*R
		*LIB *FILE	QSYS.LIB[27]	*R
		*FLR	QDLS	*R
		*DDIR	QOPT[11]	*R
		*DDIR		*R
WRKLNK	Katalog nadrzędny obiektu odniesienia - opcja 8 (Wyświetl atrybuty)	*DIR	″root″ (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Katalog nadrzędny obiektu odniesienia - opcja 12 (Praca z dowiązaniami)	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*SYMLNK	″root″ (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB[27]	*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	″root″ (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Przedrostek nadrzędnego obiektu odniesienia - podano wzorzec [13]	*DIR	″root″ (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Przedrostek nadrzędnego obiektu odniesienia - opcja 8 (Wyświetl atrybuty)	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Przedrostek macierzystego obiektu odniesienia - opcja 12 (praca z dowiązaniami)	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*SYMLNK	″root″ (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*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	″root″ (/), QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Względna nazwa ścieżki [14] : bieżący katalog roboczy zawierający obiekt - podany wzorzec [13]	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB[27]	*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	″root″ (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB[27]	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Względna nazwa ścieżki [14] przedrostek bieżącego katalogu roboczego zawierającego obiekt - podano wzorzec [13]	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB[27]	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R

[1] Uprawnienia adoptowane nie są wykorzystywane przez komendy zintegrowanego systemu plików

[2] Jeśli użytkownik posiada uprawnienie specjalne *SAVSYS, nie potrzebuje uprawnień określonych dla systemów plików QSYS.LIB, QDLS, QOpenSys oraz ″root″ (/).

[3] Wymagane uprawnienia zależą do typu obiektu. Patrz opis funkcji QLIRNMO API. 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.

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu [1]
[6] Jeśli operacja odtwarzania wykonywana jest przez profil użytkownika innego, niż ten określony parametrem PRNDIROWN, wymagane są uprawnienia specjalne *SAVSYS lub *ALLOBJ.				
[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.				
[9] Użytkownik musi posiadać uprawnienia specjalne *AUDIT, aby móc zmienić atrybut *CRTOBJAUD. Użytkownik nie potrzebuje zwykłych uprawnień nazwy ścieżki (*X i *R).				
[10] Wymagane uprawnienia zmieniają się w zależności od użytej 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 specjalne do wszystkich obiektów (*ALLOBJ). • Użytkownik jest właścicielem odłączanego obiektu. • Użytkownik jest właścicielem jest właścicielem katalogu.				
[20] Jeśli podano wartość RMVLNK (*YES), użytkownik musi mieć także uprawnienia *OBJEXIST do wszystkich obiektów w podanym katalogu.				
[21] W systemach plików QSYS.LIB, ″root″ (/), QOpenSys i systemach plików użytkownika, jeśli dla parametru CRTOBJAUD określono wartość inną niż *SYSVAL, 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 określić wartość inną niż *NONE dla parametru Zezwalaj na różnice w obiektach (Allow object differences - ALWOBJDIF), użytkownik musi posiadać specjalne uprawnienia. Aby określić *UDFS jako wartość parametru RBDMFS, użytkownik musi mieć uprawnienia specjalne *SAVSYS lub *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.				

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu [1]

[26] Aby określić atrybuty *CRTOBJSCAN i *SCAN, użytkownik musi mieć uprawnienia do wszystkich obiektów (*ALLOBJ) i administratora ochrony (*SECADM).

[27] Podczas wyświetlania zawartości katalogu /QSYS.LIB, obiekty profilu użytkownika (*USRPRF), do których program wywołujący nie posiada żadnych uprawnień (takich jak *EXCLUDE), nie są zwracane.

[28] Aby określić wartość *YES dla parametru PVTAUT, użytkownik musi mieć uprawnienia specjalne *ALLOBJ.

[29] Aby określić wartość *YES dla parametru PVTAUT, użytkownik musi mieć uprawnienia specjalne *ALLOBJ lub *SAVSYS.

[30] Aby określić *UDFS jako wartość parametru RBDMFS, użytkownik musi mieć uprawnienia specjalne *SAVSYS lub *ALLOBJ.

Komendy IDD (interactive data definition)

W poniższej tabeli zamieszczono uprawnienia szczegółowe wymagane dla komendy IDD (interactive data definition).

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
ADDDTADFN	Słownik danych	*CHANGE	*EXECUTE
	Zbiór (File)	*OBJOPR, *OBJMGT	*EXECUTE
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 (Internetwork Packet Exchange)

W poniższej tabeli zamieszczono uprawnienia szczegółowe wymagane dla komend IPX (Internetwork Packet Exchange).

Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
DLTIPXD	Opis IPX	*OBJEXIST	*EXECUTE
DSPIPXD	Opis IPX	*USE	*EXECUTE
WRKIPXD	Opis IPX	*OBJOPR	*EXECUTE

Komendy indeksu wyszukiwania informacji

W poniższej tabeli zamieszczono uprawnienia szczegółowe wymagane dla komend indeksu wyszukiwania informacji.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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

Komendy atrybutów IPL

W poniższej tabeli zamieszczono uprawnienia szczegółowe wymagane dla komend atrybutów IPL.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo 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

W poniższej tabeli zamieszczono uprawnienia szczegółowe wymagane dla komend języka Java.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
ANZJVM	Komenda QSYS/STRSRVJOB	*USE	
	Komenda QSYS/STRDBG	*USE	
DSPJVMJOB[1]	Zadania wirtualnej maszyny języka Java		

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
GENJVMDMP [1]			
PRTJVMJOB [1]			
WRKJVMJOB [1]			
[1] Do użycia tej komendy konieczne jest uprawnienie specjalne *JOBCTL.			

Komendy zadań

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy zadań.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo 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
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 jest zmieniana	*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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
DLYJOB [4]			
DMPUSRTRC	Bufor śledzenia użytkownika [15]	*OBJOPR	*EXECUTE
DSCJOB [1]			
DSPACTPJ	Opis urządzenia puli pamięci dyskowej (ASP)	*USE	
	Biblioteka programów		*EXECUTE
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]			
ENDLOGSVR[6]			
ENDPJ [6]	Opis urządzenia puli pamięci dyskowej (ASP)	*USE	
	Biblioteka programów		*EXECUTE
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
SBMJOB [2, 12, 17, 18]	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
STRLOGSVR[6]			
STRPJ [6]	Opis podsystemu	*USE	
	Program	*USE	*EXECUTE
	Opis urządzenia puli pamięci dyskowej (ASP)	*USE	

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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			
WRKARMJOB[16]			
WRKASPJOB	Opis urządzenia	*USE	
WRKJOB [1]			
WRKJOBLOG			
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 posiadającego uprawnienia specjalne do wszystkich obiektów (*ALLOBJ), użytkownik musi posiadać uprawnienia specjalne *ALLOBJ lub zostać uprawniony do korzystania z funkcji Protokół zadań wszystkich obiektów (All Object Job Log) systemu i5/OS przez funkcję Administrowanie Aplikacjami w programie System i 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.

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.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
[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 do sterowania zadaniem (*JOBCTL) może uruchamiać te komendy dla dowolnych zadań. [15] Bufor śledzenia użytkownika jest obiektem przestrzeni użytkownika (*USRSPC) w bibliotece QUSRSYS o nazwie QPOZ*nnnnnn*, gdzie '*nnnnnn*' jest numerem zadania używającego funkcji śledzenia użytkownika.			
[16] Praca z konkretnym zadaniem lub wyświetlanie szczegółów konkretnego zadania jest możliwe, jeśli spełniony jest jeden z następujących warunków: • Komenda została wydana z tego zadania. • Komenda została wydana z profilu użytkownika, który jest taki sam jak tożsamość użytkownika zadania dla tego zadania. • Komenda została wydana wydana z profilu użytkownika, który ma uprawnienia specjalne do sterowania zadaniami (*JOBCTL). [17] Do określenia wartości znakowej kodu rozliczeniowego w parametrze Kod rozliczeniowy (Accounting Code - ACGCDE) niezbędne jest uprawnienie do korzystania (*USE) z komendy Zmiana kodu rozliczeniowego (Changing Accounting Code - CHGACGCDE). [18] Do korzystania z parametru Wprowadzone dla (Submitted for - SBMFOR) niezbędne jest posiadanie uprawnień specjalnych do sterowania zadaniami (*JOBCTL).			

Komendy opisu zadania

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy opisu zadania.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, "Komendy z uprawnieniami publicznymi *EXCLUDE", na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo 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	
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	
DLTJOBD	Opis zadania	*OBJEXIST	*EXECUTE
DSPJOBD	Opis zadania	*OBJOPR, *READ	*EXECUTE
PRTJOBDAUT [1]			

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 kolejki zadań

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy kolejki zadań.

Komenda	Obiekt odniesienia	Parametry kolejki zadań [4]		Uprawnienia specjalne	Wymagane uprawnienie	
		AUTCHK	OPRCTL		Do obiektu	Do biblioteki
CHGJOBQ	Kolejka zadań	*DTAAUT			*READ, *ADD, *DLT, *OBJMGMT	*EXECUTE
		*OWNER			Właściciel [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
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
WRKJOBQD	Kolejka zadań				*READ	*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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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 kronik

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy kronik.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki lub katalogu**
ADDRMTJRN	Kronika źródłowa	*CHANGE, *OBJMGT	*EXECUTE
	Kronika docelowa		*EXEC, *ADD

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki lub katalogu**
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)
APYJRNCHGX (Q)	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
CHGJRNA (Q) [10]			
CHGJRNOBJ [9]	Kronika	*OBJOPR, *OBJMGT	
	Obiekty niezintegrowanego systemu plików	*READ, *OBJMGT	
	Obiekty zintegrowanego systemu plików	*R, *OBJMGT	*X
	Ścieżka do obiektu SUBTREE(*ALL)	*RX, *OBJMGT	
	Ścieżka do obiektu SUBTREE(*NONE)	*R, *OBJMGT	
CHGRMTJRN	Kronika źródłowa	*CHANGE, *OBJMGT	*EXECUTE
	Kronika źródłowa	*USE, *OBJMGT	*EXECUTE
CMPJRNIMG	Kronika	*USE	*EXECUTE
	Dziennik	*USE	*EXECUTE
	Zbiór (File)	*USE	*EXECUTE
CPYAUDJRNE[8]	Zbiór wyjściowy już istnieje	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Zbiór wyjściowy nie istnieje		*EXECUTE, *ADD
CRTJRN	Kronika		*READ, *ADD
	Dziennik	*OBJOPR, *OBJMGT, *READ	*EXECUTE
DLTJRN	Kronika	*OBJOPR, *OBJEXIST	*EXECUTE
DSPAUDJRNE[8]			

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki lub katalogu**
DSPJRN [6]	Kronika	*USE	*EXECUTE
	Kronika, jeśli określono FILE(*ALLFILE), nie określono żadnego obiektu, określony obiekt został usunięty z systemu, określony obiekt nie był nigdy kronikowany, określono *IGNFILSLT lub *IGNOBJSLT dla wybranych kodów kroniki, określono OBJJID lub kronika jest kroniką zdalną.	*OBJEXIST, *USE	*EXECUTE
	Dziennik	*USE	*EXECUTE
	Obiekt niezintegrowanego systemu plików, jeśli został określony	*USE	*EXECUTE
	Zbiór wyjściowy	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
	Obiekt zintegrowanego systemu plików, jeśli został określony	*R (Możliwe jest również *X, jeśli obiekt jest katalogiem i określono SUBTREE (*ALL)).	*X
DSPJRNMNU[1]			
ENDJRN	Patrz “Komendy zintegrowanego systemu plików” na stronie 406.		
ENDJRNAP	Kronika	*OBJOPR, *OBJMGT	*EXECUTE
	Zbiór (File)	*OBJOPR, *OBJMGT	*EXECUTE
ENDJRNLIB	Kronika	*OBJOPR, *OBJMGT	*EXECUTE
	Biblioteka	*OBJOPR, *OBJMGT, *READ	
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]			

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki lub katalogu**
RCVJRNE	Kronika	*USE	*EXECUTE
	Kronika, jeśli określono FILE(*ALLFILE), nie określono żadnego obiektu, określony obiekt został usunięty z systemu, określony obiekt nie był nigdy kronikowany, określono *IGNFILSLT lub *IGNOBJSLT dla wybranych kodów kroniki, określono OBJJID lub kronika jest kroniką zdalną.	*OBJEXIST, *USE	*EXECUTE
	Dziennik	*USE	*EXECUTE
	Obiekt niezintegrowanego systemu plików, jeśli został określony	*USE	*EXECUTE
	Obiekt zintegrowanego systemu plików, jeśli został określony	*R (Możliwe jest również *X, jeśli obiekt jest katalogiem i określono SUBTREE (*ALL)).	*X
	Program obsługi wyjścia	*EXECUTE	*EXECUTE
RMVJRNCHG (Q)	Kronika	*USE	*EXECUTE
	Dziennik	*USE	*EXECUTE
	Obiekty niezintegrowanego systemu plików, których zmiany w kronice są usuwane	*OBJMGT, *CHANGE	*EXECUTE
RTVJRNE	Kronika	*USE	*EXECUTE
	Kronika, jeśli określono FILE(*ALLFILE), nie określono żadnego obiektu, określony obiekt został usunięty z systemu, określony obiekt nie był nigdy kronikowany, określono *IGNFILSLT lub *IGNOBJSLT dla wybranych kodów kroniki, określono OBJJID lub kronika jest kroniką zdalną.	*OBJEXIST, *USE	*EXECUTE
	Dziennik	*USE	*EXECUTE
	Obiekt niezintegrowanego systemu plików, jeśli został określony	*USE	*EXECUTE
	Obiekt zintegrowanego systemu plików, jeśli został określony	*R (Możliwe jest również *X, jeśli obiekt jest katalogiem i określono SUBTREE (*ALL)).	*X
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 406.		
STRJRNAP	Kronika	*OBJOPR, *OBJMGT	*EXECUTE
	Zbiór (File)	*OBJOPR, *OBJMGT	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki lub katalogu
STRJRNLIB	Kronika	*OBJOPR, *OBJMGT	*EXECUTE
	Biblioteka	*OBJOPR, *OBJMGT, *READ	
STRJRNPF	Kronika	*OBJOPR, *OBJMGT	*EXECUTE
	Zbiór (File)	*OBJOPR, *OBJMGT	*EXECUTE
STRJRNOBJ	Kronika	*OBJOPR, *OBJMGT	*EXECUTE
	Obiekt	*OBJOPR, *READ, *OBJMGT	*EXECUTE
WRKJRN [4] (Q)	Kronika	*USE	*READ[7]
	Dziennik	*USE	*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 opis komendy WRKJRN (komenda ta pełni identyczną 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 posiadać odpowiednie uprawnienia dla komendy RSTOBJ lub RST.

[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.

[10] Do użycia tej komendy konieczne jest uprawnienie specjalne *JOBCTL.

Komendy dzienników

W poniższej tabeli zamieszczono uprawnienia szczegółowe wymagane dla komend dzienników.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
CRTJRNRCV	Dziennik		*READ, *ADD
DLTJRNRCV	Dziennik	*OBJOPR, *OBJEXIST i uprawnienia do danych inne niż *EXECUTE	*EXECUTE
	Kronika	*OBJOPR	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
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 protokołu Kerberos

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy protokołu Kerberos.

Komenda	Obiekt odniesienia	Typ obiektu	Wymagane uprawnienie do obiektu
ADDKRBKTE	Każdy katalog w nazwie ścieżki poprzedzającej docelowy zbiór tabeli kluczy, który ma zostać otwarty.	*DIR	*X
	Katalog nadrzędny docelowego zbioru tabeli kluczy w przypadku dodawania, jeśli zbiór jeszcze nie istnieje.	*DIR	*WX
	Zbiór tabeli kluczy, jeśli jest podana lista.	*STMF	*R
	Docelowy zbiór tabeli kluczy w przypadku dodawania lub usuwania.	*STMF	*RW
	Każdy katalog w ścieżce do zbiorów konfiguracyjnych.	*DIR	*X
	Zbiory konfiguracyjne	*STMF	*R
ADDKRBTKT	Każdy katalog w nazwie ścieżki poprzedzającej zbiór tabeli kluczy	*DIR	*X
	Zbiór tabeli kluczy	*STMF	*R
	Każdy katalog w nazwie ścieżki poprzedzającej zbiór pamięci podręcznej referencji	*DIR	*X
	Zbiór pamięci podręcznej referencji	*STMF	*RW
	Katalog nadrzędny zbioru pamięci podrzędnej, który ma zostać użyty, jeśli jest określony przez zmienną środowiskową KRB5CCNAME i jest tworzony zbiór.	*DIR	*WX
	Każdy katalog w nazwie ścieżki do zbiorów konfiguracyjnych	*DIR	*X
	Zbiory konfiguracyjne	*STMF	*R
CHGKRBPWD			

Komenda	Obiekt odniesienia	Typ obiektu	Wymagane uprawnienie do obiektu
DLTKRBCCF	Każdy katalog w nazwie ścieżki poprzedzającej zbiór pamięci podręcznej referencji, jeśli zbiór pamięci podręcznej referencji nie znajduje się w katalogu domyślnym.	*DIR	*X
	Katalog nadrzędny zbioru pamięci podręcznej referencji, jeśli zbiór pamięci podręcznej referencji nie znajduje się w katalogu domyślnym.	*DIR	*WX
	Zbiór pamięci podręcznej referencji, jeśli zbiór pamięci podręcznej referencji nie znajduje się w katalogu domyślnym.	*STMF	*RW, *OBJEXIST
	Każdy katalog w nazwie ścieżki do zbiorów konfiguracyjnych, jeśli zbiór pamięci podręcznej referencji nie znajduje się w katalogu domyślnym.	*DIR	*X
	Zbiory konfiguracyjne, jeśli zbiór pamięci podręcznej referencji nie znajduje się w katalogu domyślnym.	*STMF	*R
DLTKRBCCF	Wszystkie katalogi w nazwie ścieżki, jeśli zbiór pamięci podręcznej referencji znajduje się w katalogu domyślnym.	*DIR	*X
	Zbiór pamięci podręcznej referencji, jeśli zbiór pamięci podręcznej referencji znajduje się w katalogu domyślnym.	*STMF	*RW
	Każdy katalog w ścieżce do zbiorów konfiguracyjnych, jeśli zbiór pamięci podręcznej referencji znajduje się w katalogu domyślnym.	*DIR	*X
	Zbiory konfiguracyjne, jeśli zbiór pamięci podręcznej referencji znajduje się w katalogu domyślnym.	*STMF	*R
DSPKRBCCF	Każdy katalog w nazwie ścieżki poprzedzającej zbiór tabeli kluczy	*DIR	*X
	Zbiór tabeli kluczy	*STMF	*R
	Każdy katalog w nazwie ścieżki poprzedzającej zbiór pamięci podręcznej referencji	*DIR	*X
	Zbiór pamięci podręcznej referencji	*STMF	*RW
DSPKRBKTE	Każdy katalog w nazwie ścieżki poprzedzającej docelowy zbiór tabeli kluczy, który ma zostać otwarty.	*DIR	*X
	Katalog nadrzędny docelowego zbioru tabeli kluczy w przypadku dodawania, jeśli zbiór jeszcze nie istnieje.	*DIR	*WX
	Zbiór tabeli kluczy, jeśli jest podana lista.	*STMF	*R
	Docelowy zbiór tabeli kluczy w przypadku dodawania lub usuwania.	*STMF	*RW
	Każdy katalog w ścieżce do zbiorów konfiguracyjnych.	*DIR	*X
	Zbiory konfiguracyjne	*STMF	*R

Komenda	Obiekt odniesienia	Typ obiektu	Wymagane uprawnienie do obiektu
RMVKRBKTE	Każdy katalog w nazwie ścieżki poprzedzającej docelowy zbiór tabeli kluczy, który ma zostać otwarty.	*DIR	*X
	Katalog nadrzędny docelowego zbioru tabeli kluczy w przypadku dodawania, jeśli zbiór jeszcze nie istnieje.	*DIR	*WX
	Zbiór tabeli kluczy, jeśli jest podana lista.	*STMF	*R
	Docelowy zbiór tabeli kluczy w przypadku dodawania lub usuwania.	*STMF	*RW
	Każdy katalog w ścieżce do zbiorów konfiguracyjnych.	*DIR	*X
	Zbiory konfiguracyjne	*STMF	*R

Komendy języka

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy języka.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CLOSE	Komenda zamykania	*USE	*EXECUTE
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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTBNDCL	Zbiór źródłowy	*USE	*EXECUTE
	Włączenie zbioru	*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
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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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
CRTCLMOD	Zbiór źródłowy	*USE	*EXECUTE
	Włączenie zbioru	*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
	Włączenie zbioru	*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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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
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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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
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
CRTSQLCI (program licencjonowany DB2 Query Manager and SQL Development for i5/OS) [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 i5/OS) [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 i5/OS) [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 i5/OS) [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 i5/OS) [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 i5/OS) [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 i5/OS) [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 i5/OS) [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
INCLUDE	Zbiór źródłowy	*USE	*EXECUTE
RTVCLDSRC	Obiekt ustawień narodowych	*USE	*EXECUTE
	Docelowy zbiór	Więcej informacji znajduje się w zasadach ogólnych.	Więcej informacji znajduje się w zasadach ogólnych.
RUNSQLSTM[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 i5/OS) [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 bezpieczeństwa dotyczących instrukcji w języku SQL znajduje się w sekcji Autoryzacja, przywileje i prawo własności do obiektów.

Komendy bibliotek

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy bibliotek.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki, na której jest wykonywana komenda
ADDLIBLE	Biblioteka.		*USE
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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki, na której jest wykonywana komenda
RSTLIB (Q)[7, 17, 19]	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 (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 jest wykonywana komenda
SAVLIB[18]	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
	Przestrzeń komend użytkownika, jeśli została określona	*USE	*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	W systemie źródłowym, takie same uprawnienia, jak te wymagane przez komendę SAVLIB.		
	W systemie docelowym, takie same uprawnienia, jak te wymagane przez komendę RSTLIB.		

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki, na której jest wykonywana komenda
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, 16]	Biblioteka.		*USE

[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 określić wartość inną niż *NONE dla parametru Zezwalaj na różnice w obiektach (Allow object differences - ALWOBJDIF), użytkownik musi posiadać specjalne uprawnienia.

[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.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki, na której jest wykonywana komenda
[16] Komenda ta wymaga uprawnienia specjalnego *ALLOBJ.			
[17] Określenie wartości *YES parametru PVTAUT wymaga uprawnień specjalnych *ALLOBJ.			
[18] Określenie wartości *YES parametru PVTAUT wymaga uprawnień specjalnych *ALLOBJ lub *SAVSYS.			
[19] Określenie nazwy dla parametru DFRID wymaga uprawnień specjalnych *SAVSYS.			

Komendy kluczy licencyjnych

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy kluczy licencyjnych.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo 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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy programów licencjonowanych.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo 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)			

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki

[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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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
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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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]			
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)

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy sieci lokalnej (LAN).

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Te komendy nie wymagają żadnych uprawnień do obiektu:			
ADDLANADPI CHGLANADPI	DSPLANADPP DSPLANSTS	RMVLANADPT (Q) RMVLANADPI	WRKLANADPT

Komendy ustawień narodowych

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy ustawień narodowych.

		Wymagane uprawnienie	
Komenda	**Obiekt odniesienia**	**Do obiektu**	**Do biblioteki**
CRTLOCALE	Zbiór źródłowy	*USE	*USE, *ADD
DLTLOCALE	Ustawienia narodowe	*OBJEXIST	*EXECUTE

Komendy struktury serwera poczty

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy struktury serwera poczty.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Ta komenda nie wymaga żadnych uprawnień do obiektów:			
ENDMSF (Q)	STRMSF (Q)		

Komendy nośników

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy nośników.

		Wymagane uprawnienie	
Komenda	**Obiekt odniesienia**	**Do obiektu**	**Do biblioteki**
ADDTAPCTG	Opis biblioteki taśm	*USE	*EXECUTE
CFGDEVMLB[1]	Opis biblioteki taśm	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVMLB (Q)	Opis biblioteki taśm	*CHANGE, *OBJMGT	*EXECUTE
CHGJOBMLBA[4]	Opis biblioteki taśm	*CHANGE	*EXECUTE
CHGTAPCTG	Opis biblioteki taśm	*USE	*EXECUTE
CHKDKT	Opis jednostki dyskietek	*USE	*EXECUTE
CHKTAP	Opis napędu taśm	*USE	*EXECUTE
CLRDKT	Opis jednostki dyskietek	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CRTTAPCGY	Opis biblioteki taśm		
DLTDKTLBL	Opis jednostki dyskietek	*USE	*EXECUTE
DLTMEDDFN	Definicja nośnika	*OBJEXIST	*EXECUTE
DLTTAPCGY	Opis biblioteki taśm		
DMPTAP (Q)[5]	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.

[5] Aby skorzystać z tej komendy, użytkownik musi posiadać uprawnienie specjalne *ALLOBJ, jeśli określony został TYPE(*HEX), lub jeśli taśma posiada włączoną flagę wolumin chroniony lub zbiór chroniony.

Komendy paneli grupowych i menu

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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
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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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 zbioru komunikatów

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy zbioru komunikatów.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
CHGMSGF	Zbiór komunikatów	*USE, *DLT	*EXECUTE
CRTMSGF	Zbiór komunikatów		*READ, *ADD
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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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. Dostarczane są z uprawnieniami publicznymi *EXCLUDE. Użytkownik musi posiadać uprawnienie specjalne *ALLOBJ aby móc korzystać z tych komend.			

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ANZS34OCL ANZS36OCL CHGS34LIBM CHKS36SRCA CVTBASSTR CVTBASUNF CVTBGUDTA CVTS36FCT	CVTS36JOB CVTS38JOB GENS36RPT GENS38RPT MGRS36 MGRS36APF [1] MGRS36CBL MGRS36DFU [1]	MGRS36DSPF MGRS36ITM MGRS36LIB MGRS36MNU MGRS36MSGF MGRS36QRY [1] MGRS36RPG MGRS36SEC MGRS38OBJ	MIGRATE QMUS36 RESMGRNAM RSTS38AUT STRS36MGR STRS38MGR
[1] Użytkownik musi mieć uprawnienia specjalne *ALLOBJ i zainstalowaną opcję 4 i5/OS.			

Komendy opisu trybu

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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

[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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy sieciowe.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo 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			
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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy sieciowego systemu plików.

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu
ADDMFS [1,3]	katalog_do_podłączenia	*DIR	″root″ (/)	*W
CHGNFSEXP [1,2]	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
DSPMFSINF	niektóre_katalogi	*DIR	″root″ (/)	*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	″root″ (/)	*W
RLSIFSLCK [1]	obiekt	*STMF	″root″ (/), QOpenSys, UDFS	*R
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
RMVMFS [1]				
STATFS	niektóre_katalogi	*DIR	″root″ (/)	*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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
[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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy serwera sieciowego.

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu
ADDNWSSTGL [2]	Ścieżka (/QFPNWSSTG)	*DIR	″root″ (/)	*X
	Katalog nadrzędny (nazwa przestrzeni pamięci)	*DIR	″root″ (/)	*WX
	Zbiory tworzące przestrzeń pamięci	*STMF	″root″ (/)	*RW
	Opis serwera sieciowego	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
CHGNWSSTG[2]	Ścieżka (katalog główny i /QFPNWSSTG)	*DIR	″root″ (/)	*WX
CHGNWSUSRA [4]	Profil użytkownika	*USRPRF		*OBJMGT, *USE
CRTNWSSTG [2]	Ścieżka (katalog główny i /QFPNWSSTG)	*DIR	″root″ (/)	*WX
DLTNWSSTG [2]	Ścieżka (/QFPNWSSTG)	*DIR	″root″ (/)	*WX
	Katalog nadrzędny (nazwa przestrzeni pamięci)	*DIR	″root″ (/)	*RWX, *OBJEXIST
	Zbiory tworzące przestrzeń pamięci	*STMF	″root″ (/)	*OBJEXIST
DLTWNTSVR[5]	Opis serwera sieciowego	*NWSD	QSYS.LIB	*OBJEXIST
	Opis linii	*LIND	QSYS.LIB	*OBJEXIST
	Konfiguracja serwera sieciowego	*NWSCFG	QSYS.LIB	*OBJEXIST
	Przestrzeń pamięciowa serwera sieciowego - Ścieżka (/QFPNWSSTG)	*DIR	″root″ (/)	*WX
	Katalog nadrzędny (nazwa przestrzeni pamięci)	*DIR	″root″ (/)	*RWX, *OBJEXIST
	Zbiory tworzące przestrzeń pamięci	*STMF	″root″ (/)	*OBJEXIST
DSPNWSSTG	Przedrostek ścieżki	Patrz zasady ogólne		
	Zbiory tworzące przestrzeń pamięci	*STMF	″root″ (/)	*R
INSWNTSVR[6, 7]	Opis serwera sieciowego	*NWSD	Nie dotyczy	*USE
	Opis linii	*LIND	Nie dotyczy	*USE
	Konfiguracja serwera sieciowego	*NWSCFG	Nie dotyczy	*USE
	Przestrzeń pamięciowa serwera sieciowego - Ścieżka (/QFPNWSSTG)	*DIR	″root″ (/)	*WX

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu
RMVNWSSTGL [2]	Ścieżka (/QFPNWSSTG)	*DIR	″root″ (/)	*X
	Katalog nadrzędny (nazwa przestrzeni pamięci)	*DIR	″root″ (/)	*WX
	Zbiory tworzące przestrzeń pamięci	*STMF	″root″ (/)	*RW
	Opis serwera sieciowego	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
WRKNWSSTG	Przedrostek ścieżki	Patrz zasady ogólne		
	Zbiory tworzące przestrzeń pamięci	*STMF	″root″ (/)	*R
Te komendy nie wymagają żadnych uprawnień do obiektu:				
ADDRMTSVR CHGNWSA [4](Q) CHGNWSALS CRTNWSALS DLTNWSALS DSPNWSA	DSPNWSALS DSPNWSSSN DSPNWSSTC DSPNWSUSRA SBMNWSCMD (Q) [3]		SNDNWSMSG WRKNWSALS WRKNWSENR WRKNWSSSN WRKNWSSTS	

[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.

[5] Aby móc korzystać z tej komendy, użytkownik musi posiadać uprawnienia specjalne *IOSYSCFG i *ALLOBJ.

[6] Aby móc korzystać z tej komendy, użytkownik musi posiadać uprawnienia specjalne *IOSYSCFG, *ALLOBJ i *JOBCTL.

[7] Aby móc nadać parametrowi IPSECRULE, CHAPAUT lub SPCERTID wartość inną niż domyślna, użytkownik musi posiadać uprawnienia specjalne *SECADM.

Komendy konfiguracji serwera sieciowego

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend konfiguracji serwera sieciowego.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki QUSRSYS
CHGNWSCFG[1, 3]	Konfiguracja serwera sieciowego	*CHANGE	*EXECUTE
CRTNWSCFG [1, 3]	Konfiguracja serwera sieciowego	*USE	*READ, *ADD
DLTNWSCFG[1, 3]	Konfiguracja serwera sieciowego	*OBJEXIST	*EXECUTE
DSPNWSCFG[1, 3]	Konfiguracja serwera sieciowego	*USE	*EXECUTE
INZNWSCFG[1, 2]	Konfiguracja serwera sieciowego	*CHANGE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki QUSRSYS
WRKNWSCFG[1]	Konfiguracja serwera sieciowego	*USE	*EXECUTE

[1] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *IOSYSCFG.

[2] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *SECADM.

[3] Aby móc nadać parametrowi IPSECRULE, CHAPAUT, lub SPCERTID wartość inną niż domyślna, użytkownik musi posiadać uprawnienia specjalne *SECADM.

Komendy opisu serwera sieciowego

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy usług biurowych.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Te komendy nie wymagają uprawnień do obiektu.			
ADDACC (Q) DSPACC DSPACCAUT DSPUSRPMN	GRTACCAUT [2,3,6] (Q) GRTUSRPMN [1,2] RMVACC [1] (Q) RVKACCAUT [1]	RVKUSRPMN [1,2] WRKDOCLIB [4] WRKDOCPRTQ [5]	

[1] Aby nadać lub odebrać uprawnienia dla kodu dostępu lub uprawnienia do dokumentów innym użytkownikom, użytkownik musi mieć uprawnienia specjalne *ALLOBJ.

[2] Dostęp do dokumentów, katalogów i listów, które nie są osobiste, jest ograniczony.

[3] Przed nadaniem uprawnień kod dostępu musi 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

Poniższa tabela zawiera uprawnienia szczegółowe, wymagane przy komendach kursów elektronicznych.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

		Wymagane uprawnienie	
Komenda	**Obiekt odniesienia**	**Dla obiektu**	**Dla biblioteki**
CVTEDU			
STREDU			

Komendy asysty operacyjnej

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy asysty operacyjnej.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

		Wymagane uprawnienie	
Komenda	**Obiekt odniesienia**	**Do obiektu**	**Do biblioteki**
CHGBCKUP [1]	QUSRSYS/QEZBACKUPL *USRIDX	*CHANGE	*EXECUTE
CHGCLNUP[2]			

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
CHGPWRSCD [3]			
CHGPWRSCDE [3]			
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	
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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy urządzeń optycznych.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie		
		Obiekt	Biblioteka.	Wolumin optyczny [1]
ADDOPTCTG (Q)	Urządzenie optyczne	*USE	*EXECUTE	
ADDOPTSVR (Q)	Serwer CSI	*USE	*EXECUTE	

Komenda	Obiekt odniesienia	Wymagane uprawnienie		
		Obiekt	**Biblioteka.**	**Wolumin optyczny** [1]
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
CHKOPTVOL	Urządzenie optyczne	*USE	*EXECUTE	*USE
	Katalog główny (/) woluminu	*RWX	Nie dotyczy	Nie dotyczy
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

Komenda	Obiekt odniesienia	Wymagane uprawnienie		
		Obiekt	**Biblioteka.**	**Wolumin optyczny** [1]
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
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
LODOPTFMW	Plik strumieniowy	*R	Nie dotyczy	Nie dotyczy
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
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	

Komenda	Obiekt odniesienia	Wymagane uprawnienie		
		Obiekt	**Biblioteka.**	**Wolumin optyczny [1]**
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	

[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 kolejek wyjściowych

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend kolejek wyjściowych.

Komenda	Obiekt odniesienia	Parametry kolejki wyjściowej		Uprawnienia specjalne	Wymagane uprawnienia	
		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
	Kolejka komunikatów				*OBJOPR *ADD	*EXECUTE
	Obiekt dostosowywania stacji roboczej				*USE	*EXECUTE
	Program transformacji danych użytkownika				*OBJOPR *EXECUTE	*EXECUTE
	Program sterownika użytkownika				*OBJOPR *EXECUTE	*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
	Kolejka komunikatów				*OBJOPR *ADD	*EXECUTE
	Obiekt dostosowywania stacji roboczej				*USE	*EXECUTE
DLTOUTQ	Kolejka wyjściowa				*OBJEXIST	*EXECUTE
HLDOUTQ [1]	Kolejka wyjściowa	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
PRTQAUT [4]						
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

Komenda	Obiekt odniesienia	Parametry kolejki wyjściowej		Uprawnienia specjalne	Wymagane uprawnienia	
		AUTCHK	OPRCTL		Do obiektu	Do biblioteki

[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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy wydajności.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
ADDDWDFN (Q) [7]			
ADDJWDFN (Q) [7]			
ADDPEXDFN (Q) [5]	Biblioteka PGM		*EXECUTE
ADDPEXFTR (Q)[5]	Biblioteka PGMTRG		*EXECUTE
	Biblioteka PGMFTR		*EXECUTE
	Ścieżka JVAFTR	*X dla katalogu	
	Ścieżka PATHFTR	*X dla katalogu	

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ANZBESTMDL (Q)[4]	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Biblioteki aplikacji, które zawierają analizowane zbiory bazy danych		*EXECUTE
	Opis zadania	*USE	*EXECUTE
ANZCMDPFR (Q)	Plik komend	*USE	*EXECUTE
	Zbiór wyjściowy	*USE	*EXECUTE, *ADD
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
CHGMGTCOL	MGTCOL	*OBJMGT	
	Biblioteka użytkownika		*EXECUTE
CHGPEXDFN (Q)[5]	Biblioteka PGM		*EXECUTE
CHKPFRCOL (Q)			
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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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
CPYPFRCOL (Q)	Z biblioteki		*EXECUTE
	Do biblioteki		*EXECUTE, *ADD
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
CRTGPHPKG (Q)	QPFR/QPGCRTPK *PGM	*USE	*EXECUTE
	Biblioteka, w której tworzone są dane historyczne		*ADD, *READ
	Opis zadania	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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
CRTPFRSUM (Q)	Biblioteka użytkownika		*ADD, *READ
CVTPFRCOL (Q)	Z biblioteki		*USE
	Do biblioteki		*USE, *ADD
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]
DLTPFRCOL (Q)	Biblioteka		*EXECUTE
DLTPFRDTA (Q)[4]	QPFR/QPTDLTCP *PGM	*USE	*EXECUTE
DMPMEMINF	Zbiór wyjściowy	Patrz zasady ogólne	Patrz zasady ogólne
DMPTRC (Q)[5]	Biblioteka, w której przechowywane są dane śledzenia		*EXECUTE, *ADD
	Zbiór wyjściowy (QAPTPAGD)	*CHANGE	*EXECUTE, *ADD
DSPHSTGPH (Q)[4]	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Biblioteka danych historycznych		*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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
ENDDW (Q)[7]			
ENDJOBTRC (Q)[4]	QPFR/QPTTRCJ0 *PGM	*USE	*EXECUTE
ENDJW (Q)[7]			
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
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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
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
RMVDWDFN (Q) [7]			
RMVJWDFN (Q) [7]			
RMVPEXDFN (Q)[5]			
RMVPEXFTR (Q)[5]			
RSTPFRCOL (Q)	Biblioteka powiązana z kolekcją odtwarzania	*EXECUTE,, *ADD [6]	
	Zbiór składowania	*USE	*EXECUTE
SAVPFRCOL (Q)	Biblioteka zawierająca kolekcję do składowania	*EXECUTE [6]	
	Zbiór składowania, jeśli jest pusty	*USE, *ADD	*EXECUTE, *ADD
	Zbiór składowania, jeśli istnieją w nim rekordy	*OBJMGT, *USE, *ADD	*EXECUTE
STRBEST (Q)[4]	QPFR/QCYBMAIN *PGM	*USE	*EXECUTE
STRDBMON[3, 4]	Zbiór wyjściowy	*OBJOPR, *ADD	*EXECUTE
STRDW (Q)[7]	Biblioteka użytkownika		*EXECUTE
STRJOBTRC (Q)	QPFR/QPTTRCJ1 *PGM	*USE	*EXECUTE
STRJW (Q) [7]	Biblioteka użytkownika		*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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	Do biblioteki
Te komendy nie wymagają żadnych uprawnień do obiektu: • ENDDBMON[3] • ENDPFRTRC (Q) • STRPFRTRC (Q)			

[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] Do korzystania z tej komendy niezbędne są uprawnienia specjalne *SERVICE lub upoważnienie do korzystania z funkcji Śledzenie serwisowe systemu i5/OS poprzez funkcję Administrowanie Aplikacjami w programie System i Navigator. W celu zmiany listy użytkowników, którzy są upoważnieni do wykonywania operacji śledzenia, można także użyć komendy Zmiana użycia funkcji (Change Function Usage - CHGFCNUSG) z identyfikatorem funkcji QIBM_SERVICE_TRACE.

[6] Jeśli użytkownik ma uprawnienia specjalne *SAVSYS, nie potrzebuje podanych tu uprawnień.

[7] Do używania tej komendy niezbędne są uprawnienia specjalne do usług (*SERVICE) lub upoważnienie do korzystania z funkcji Monitorowanie dysku systemu operacyjnego przez obsługę funkcji Administrowanie aplikacjami w programie System i Navigator. W celu zmiany listy użytkowników, którzy są upoważnieni do korzystania z narzędzia monitorowania dysku, można także użyć komendy Zmiana użycia funkcji (CHGFCNUSG) z identyfikatorem funkcji QIBM_SERVICE_DISK_WATCHER.

Komendy grupy deskryptorów wydruków

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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 narzędzia Print Services Facility

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy konfiguracji narzędzia 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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy problemów.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDPRBACNE (Q)	Filtr	*USE, *ADD	*EXECUTE
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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne 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 438.			
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]			
CHGPGM	Program	*OBJMGT, *USE	*USE
	Program, jeśli określono opcję odtworzenia, zmieniono poziom optymizacji, lub zmieniono kolekcję danych dotyczących 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 serwisowy, jeśli określono opcję odtworzenia, zmieniono poziom optymizacji, lub zmieniono kolekcję danych dotyczących 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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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]			
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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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
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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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 bezpieczeństwa dotyczących instrukcji SQL znajduje się w sekcji Autoryzacja, przywileje i prawo własności do obiektów.

[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 interpretera powłoki QSH

W poniższej tabeli przedstawiono uprawnienia szczegółowe, niezbędne do korzystania z komend interpretera powłoki QSH.

Komendy znajdujące się w tej tabeli nie wymagają uprawnień do obiektów.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
STRQSH [1, 2]			
QSH[1, 2]			

[1] QSH jest aliasem dla komendy CL STRQSH.

[2] Użytkownik musi mieć uprawnienia *RX dla wszystkich skryptów i uprawnienia *X dla wszystkich katalogów w ścieżce dostępu do skryptu.

Komendy zapytań

W poniższej tabeli przedstawiono uprawnienia szczegółowe, niezbędne do korzystania z komend zapytań.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ANZQRY	Definicja zapytania	*USE	*EXECUTE
CHGQRYA[4]			
CRTQMFORM	Formularz menedżera zapytań: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Formularz menedżera zapytań: REPLACE(*YES)	*ALL	*READ, *ADD, *EXECUTE
	Zbiór źródłowy	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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
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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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 z grupy pytań i odpowiedzi

W tabeli podano uprawnienia szczegółowe, niezbędne do korzystania z komend z grupy pytań i odpowiedzi.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo 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
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] QAQA*xx*BQPY [1]	*READ	*USE
WRKCNTINF			*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**

[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

W poniższej tabeli przedstawiono uprawnienia szczegółowe, niezbędne do korzystania z komend 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

W poniższej tabeli przedstawiono uprawnienia szczegółowe, niezbędne do korzystania z komend narzędzia do rejestracji.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
ADDEXITPGM (Q)			
RMVEXITPGM (Q)			
WRKREGINF			

Komendy dotyczące relacyjnych baz danych

W tabeli podano uprawnienia szczegółowe, niezbędne do korzystania z komend dotyczących relacyjnych baz 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

W poniższej tabeli przedstawiono uprawnienia szczegółowe, niezbędne do korzystania z komend 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 (Remote Job Entry - pozycja zadania zdalnego)

W poniższej tabeli przedstawiono uprawnienia szczegółowe, niezbędne do korzystania z komend RJE (Remote Job Entry - Pozycja zadania zdalnego).

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
CHGRJERDRE	Opis sesji	*USE, *ADD, *DLT	*READ, *EXECUTE
	Kolejka zadań[2]	*USE	*READ, *EXECUTE
	Kolejka komunikatów[2]	*USE, *ADD	*READ, *EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Do obiektu	**Do biblioteki**
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

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 Zbiory wejściowe to m. in. zbiory osadzone za pomocą instrukcji sterującej .. READFILE.

7 Należy przejrzeć uprawnienia wymagane dla komendy SBMJOB.

8 Aby korzystać z pojedynczych operacji, użytkownik musi mieć uprawnienia wymagane przez operację.

Komendy atrybutów bezpieczeństwa

W poniższej tabeli przedstawiono uprawnienia szczegółowe, niezbędne do korzystania z komend atrybutów bezpieczeństwa

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

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend pozycji uwierzytelniania serwera.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend usług.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
ADDTRCFTR[11]			
APYPTF (Q)	Biblioteka produktu	*OBJMGT	
CHGSRVA [3] (Q)			
CHKCMNTRC [3] (Q)			*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
CHKPRDOPT (Q)	Wszystkie obiekty w opcji produktu [4]		
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)			
DSPSSTUSR [20]			
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	
EDNWCH[16] (Q)	Sesje podglądu czekające na komunikat w protokole zadania[18]		
INSPTF[9] (Q)			

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
LODPTF (Q)	Opis urządzenia	*USE	*EXECUTE
LODRUN [2]	Komenda RSTOBJ	*USE	*EXECUTE
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[11](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)	CRTIMGCLG	*USE	
	QUSRSYS		*ADD, *READ
SNDSRVRQS (Q)			
STRCMNTRC [11] (Q)	NWID (ID sieci) lub opis linii	*USE	*EXECUTE
	Obserwowane zadanie[17]		
	Program śledzący	*OBJOPR i *EXECUTE	*EXECUTE
	Kolejka komunikatów	*USE	*USE
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)[11, 15]	Obserwowane zadanie[17]		
	Program śledzący	*OBJOPR i *EXECUTE	*EXECUTE
	Kolejka komunikatów	*USE	*USE

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
STRWCH[16] (Q)	Obserwowane zadanie[17]		
	Program służący do podglądu	*OBJOPR i *EXECUTE	*EXECUTE
	Kolejka komunikatów	*USE	*USE
TRCCNN[11](Q)	Obserwowane zadanie[17]		
	Program śledzący	*OBJOPR i *EXECUTE	*EXECUTE
	Kolejka komunikatów	*USE	*USE
TRCCPIC (Q)			
TRCICF (Q)			
TRCINT[11] (Q)	Obserwowane zadanie[17]		
	Program śledzący	*OBJOPR i *EXECUTE	*EXECUTE
	Kolejka komunikatów	*USE	*USE
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
TRCTCPAPP[11] (Q)	Opis linii	*USE	
	Interfejs sieciowy	*USE	
	Interfejs sieciowy	*USE	
	Obserwowane zadanie[17]		
	Program śledzący	*OBJOPR i *EXECUTE	*EXECUTE
	Kolejka komunikatów	*USE	*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)			
WRKPTFORD (Q)	QESCPTFO i SNDPTFORD	*USE	
WRKSRVPVD (Q)			
WRKTRC[11] (Q)			
WRKWCH[19] (Q)			

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
[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] Aby użyć tej komendy, użytkownik musi mieć uprawnienie specjalne serwisu (*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. Poniższe ograniczenia dotyczą parametru IMGDIR: • Użytkownik musi posiadać uprawnienia *X do każdego katalogu w ścieżce dostępu. • Użytkownik musi posiadać uprawniania *WX do katalogu zawierającego obraz nośnika optycznego.			
[11] Aby móc skorzystać z tej komendy, użytkownik musi mieć uprawnienie specjalne *SERVICE lub być upoważnionym do funkcji Śledzenie serwisowe w systemie i5/OS poprzez Administrowanie aplikacjami w programie System i 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. [12] Aby móc skorzystać z tej komendy, użytkownik musi mieć uprawnienie specjalne *SERVICE lub być upoważnionym do funkcji Zrzut serwisowy w systemie i5/OS poprzez Administrowanie aplikacjami w programie System i 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. [15] Jeśli dla parametru nazwy zadania (JOB) określona zostanie ogólna nazwa użytkownika, użytkownik musi mieć uprawnienia specjalne *ALLOBJ lub być upoważnionym do korzystania z funkcji Śledzenie dowolnego użytkownika systemu i5/OS poprzez Administrowanie aplikacjami w programie System i Navigator. Aby zmienić listę użytkowników upoważnionych do korzystania z operacji śledzenia, można posłużyć się komendą zmiany wykorzystania funkcji (change function usage - CHGFCNUSG), podając jako identyfikator funkcji QIBM ALLOBJ TRACE ANY USER.			

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**

[16] Aby móc skorzystać z tej komendy, użytkownik musi mieć uprawnienia specjalne *SERVICE, lub być upoważnionym do korzystania z funkcji podglądu serwisowego systemu i5/OS poprzez Administrowanie aplikacjami w programie System i Navigator. Aby zmienić listę użytkowników upoważnionych do uruchamiania i przerywania operacji podglądu, można posłużyć się komendą zmiany wykorzystania funkcji (change function usage - CHGFCNUSG), podając jako identyfikator funkcji QIBM_SERVICE_WATCH.

[17] Jeśli zadanie uruchomione jest przez innego użytkownika niż tego, który korzysta z funkcji podglądu zadania, konieczne jest posiadanie uprawnień specjalnych *JOBCTL. Jeśli dla nazwy zadania określono *ALL, lub jeśli określono ogólną nazwę użytkownika, konieczne jest posiadanie uprawnień specjalnych *ALLOBJ. Użytkownik bez uprawnień specjalnych *ALLOBJ może korzystać z tej funkcji jeśli ma uprawnienia do funkcji Podgląd dowolnego zadania w systemie i5/OS poprzez Administrowanie aplikacjami w programie System i Navigator. Aby zmienić listę użytkowników upoważnionych do uruchamiania i przerywania operacji podglądu, można posłużyć się komendą zmiany wykorzystania funkcji (change function usage - CHGFCNUSG), podając jako identyfikator funkcji QIBM_WATCH_ANY_JOB.

[18] Takie same uprawnienia wymagane są przez komendę STRWCH.

[19] Aby móc skorzystać z tej komendy, użytkownik musi mieć uprawnienia specjalne *SERVICE, lub być upoważnionym do korzystania z funkcji śledzenia i podglądu serwisowego systemu i5/OS poprzez Administrowanie aplikacjami w programie System i Navigator. Aby zmienić listę użytkowników upoważnionych do korzystania z operacji śledzenia, można również skorzystać z komendy Zmiana wykorzystania funkcji (CHGFCNUSG), podając jako identyfikator funkcji QIBM_SERVICE_TRACE oraz QIBM_SERVICE_WATCH,

[20] Aby użyć tej komendy, konieczne są uprawnienia specjalne: do kontroli (*AUDIT) i administratora bezpieczeństwa (*SECADM).

Komendy słownika sprawdzania pisowni

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend słownika sprawdzania pisowni.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy sfery sterowania.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla biblioteki**
ADDSOCE	Sfera sterowania [1]	*USE, *ADD	*EXECUTE
DSPSOCSTS			
RMVSOCE	Sfera sterowania [1]	*USE, *DLT	*EXECUTE
WRKSOC	Sfera sterowania [1]	*USE	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	Dla biblioteki
[1] Sfera sterowania to zbiór fizyczny QUSRSYS/QAALSOC.			

Komendy zbioru buforowego

W tej tabeli przedstawiono uprawnienia szczegółowe wymagane dla komend zbioru buforowego

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Parametry kolejki wyjściowej			Uprawnienia specjalne	Wymagane uprawnienia	
		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					Patrz zasady ogólne dla wyświetlania (DSP) lub innych operacji korzystających ze zbioru wyjściowego (OUTPUT (*OUTFILE))	Patrz zasady ogólne dla wyświetlania (DSP) lub innych operacji korzystających ze zbioru wyjściowego (OUTPUT (*OUTFILE))
	Zbiór buforowy	*OWNER				Właściciel [6]	
	Kolejka wyjściowa [3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Właściciel [4]	
		*YES lub *NO		*YES	*JOBCTL		
DLTEXPSPLF (Q) [10]	Niezależna pula dyskowa[9]					*USE	

Komenda	Obiekt odniesienia	Parametry kolejki wyjściowej			Uprawnienia specjalne	Wymagane uprawnienia	
		DSPDTA	AUTCHK	OPRCTL		Do obiektu	Do biblioteki
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) [10]	Niezależna pula dyskowa[9]					*USE	
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]	
SNDTCPSPLF [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]	
STRSPLRCL (Q)[9, 10]	Niezależna pula dyskowa[9]					*USE	
WRKSPLF							

Komenda	Obiekt odniesienia	Parametry kolejki wyjściowej			Uprawnienia specjalne	Wymagane uprawnienia	
		DSPDTA	AUTCHK	OPRCTL		Do obiektu	Do biblioteki
[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. [9] Należy mieć uprawnienie *USE do wszystkich niezależnych pul dyskowych znajdujących się w grupie niezależnych pul dyskowych. [10] Aby uruchomić tę komendę, należy mieć uprawnienia specjalne *SPLCTL.							

Komendy opisu podsystemu

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend opisu podsystemu.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
ADDAJE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Opis zadania[9]	*OBJOPR, *READ	*EXECUTE
ADDCMNE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Opis zadania[9]	*OBJOPR, *READ	*EXECUTE
	Profil użytkownika	*USE	
ADDJOBQE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
ADDPJE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Profil użytkownika	*USE	
	Opis zadania[9]	*OBJOPR, *READ	*EXECUTE
ADDRTGE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
ADDWSE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Opis zadania[9]	*OBJOPR, *READ	*EXECUTE
CHGAJE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Opis zadania[9]	*OBJOPR, *READ	*EXECUTE
CHGCMNE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Opis zadania[9]	*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[9]	*OBJOPR, *READ	*EXECUTE
CHGRTGE	Opis podsystemu	*OJBOPR, *OBJMGT, *READ	*EXECUTE
CHGSBSD [5, 7]	Opis podsystemu	*OJBOPR, *OBJMGT, *READ	*EXECUTE
	zbiór ekranowy wpisywania się[4]	*USE	*EXECUTE
CHGWSE	Opis podsystemu	*OJBOPR, *OBJMGT, *READ	*EXECUTE
	Opis zadania[9]	*OBJOPR, *READ	*EXECUTE
CRTSBSD [5] (Q)	Opis podsystemu		*READ, *ADD
	zbiór ekranowy wpisywania się[4]	*USE	*EXECUTE
	Opis urządzenia puli pamięci dyskowej (ASP) [8]	*USE	
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
RMVRTGE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVWSE	Opis podsystemu	*OBJOPR, *OBJMGT, *READ	*EXECUTE

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
STRSBS [1]	Opis podsystemu	*USE	*EXECUTE
	Opis urządzenia puli pamięci dyskowej (ASP)	*USE	
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.

[7] Aby zmienić nazwę grupy puli pamięci dyskowej (ASP) wymagane są uprawnienia specjalne *ALLOBJ i *SECADM.

[8] Aby określić opis urządzenia ASP, który jeszcze nie istnieje, należy mieć uprawnienia specjalne do wszystkich obiektów (*ALLOBJ).

[9] Aby określić opis zadania, który jeszcze nie istnieje, należy mieć uprawnienia specjalne do wszystkich obiektów (*ALLOBJ).

Komendy systemowe

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend systemowych.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. W temacie Komendy z uprawnieniami publicznymi *EXCLUDE znajdują się informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z danej komendy. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
PWRDWNSYS[1]	Katalog obrazów (jeśli podano)	*USE	
RTVSYSINF (Q)[2]	Biblioteka	*READ, *ADD, *EXECUTE	
Te komendy nie wymagają żadnych uprawnień do obiektu:			
CHGSHRPOOL DSPSYSSTS ENDSYS[1] PRTSYSINF (Q)	RCLACTGRP[1] RCLRSC RETURN RTVGRPA	SIGNOFF UPDSYSINF (Q)[3] WRKSHRPOOL	WRKSYSSTS

[1] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne sterowania zadaniem (*JOBCTL).

[2] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *SAVSYS.

[3] Aby użyć tej komendy, użytkownik musi mieć uprawnienia specjalne *SECADM, *ALLOBJ, *AUDIT, *JOBCTL i *SAVSYS.

Komendy listy odpowiedzi systemowych

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend listy odpowiedzi systemowych.

Te komendy nie wymagają uprawnień do obiektu:			
ADDRPYLE (Q)	CHGRPYLE (Q)	RMVRPYLE (Q)	WRKRPYLE

Komendy wartości systemowych

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend wartości systemowych.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo 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

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend środowiska System/36.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

		Wymagane uprawnienia	
Komenda	**Obiekt odniesienia**	**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

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
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
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

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
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
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

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
[1] Jeśli dokument ma być zastąpiony, wymagane są uprawnienia *ALL. Użytkownik musi mieć uprawnienia do działania oraz uprawnienia do danych dla folderu, jeśli odtwarza nowe informacje do folderów lub uprawnienie specjalne *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

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend tabel.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend TCP/IP.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
ADDTCPSVR[1]	Program do wywołania	*EXECUTE	*EXECUTE
CHGTCPSVR[1]	Program do wywołania	*EXECUTE	*EXECUTE
CPYTCPHT [6]	Obiekty zbioru		
CVTTCPCL (Q)	Obiekty zbioru	*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

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
SETVTTBL	Obiekty tabeli	*USE	*EXECUTE
SNDTCPSPLF [2]	Obiekt dostosowania stacji roboczej	*USE	*EXECUTE
STRTCPFTP	Obiekty tabeli	*USE	*EXECUTE
	Obiekty zbioru	*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] ADDNETTBLE [1] ADDOSPFARA[1] ADDOSPFLNK[1] ADDOSPFIFC[1] ADDOSPFRNG[1] ADDPCLTBLE [1] ADDRIPACP[1] ADDRIPFLT[1] ADDRIPIFC[1] ADDRIPIGN[1] ADDSRVTBLE [1] ADDTCPHTE [1] ADDTCPIFC [1] ADDTCPPORT [1] ADDTCPRSI [1] ADDTCPRTE [1] CFGTCP CFGTCPAPP CFGTCPFTP [1] CFGTCPLPD [1]	CFGRTG CFGTCPSMTP CFGTCPSNMP CFGTCPTELN CHGCOMSNMP [1] CHGFTPA [1] CHGLPDA [1] CHGOSPFA[1] CHGOSPFARA[1] CHGOSPFIFC[1] CHGOSPFLNK[1] CHGOSPFRNG[1] CHGRIPA[1] CHGRIPFLT[1] CHGRIPIFC[1] CHGSMTPA [1] CHGSNMPA [1] CHGTCPA [1] CHGTCPHTE[1] CHGTCPIFC[1] CHGTCPRTE [1] CHGTELNA [1]	CHGVTMAP DSPVTMAP ENDTCP (Q) ENDTCPCNN ENDTCPIFC (Q) MGRTCPHT [1] NETSTAT PING RMVCOMSNMP [1] RMVNETTBLE [1] RMVOSPFARA[1] RMVOSPFIFC[1] RMVOSPFLNK[1] RMVOSPFRNG[1] RMVPCLTBLE [1] RMVRIPACP[1] RMVRIPFLT[1] RMVRIPIFC[1] RMVRIPIGN[1] RMVSRVTBLE [1] RMVTCPHTE[1] RMVTCPIFC[1] RMVTCPPORT [1]	RMVTCPRSI [1] RMVTCPRTE [1] RMVTCPSVR [1] RNMTCPHTE [1] SETVTMAP STRTCP (Q) STRTCPIFC (Q) VFYTCPCNN WRKNAMSMTP [3] WRKNETTBLE[1] WRKPCLTBLE[1] WRKSRVTBLE[1] WRKTCPSTS

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki

[1] Do użycia tej komendy konieczne jest uprawnienie specjalne (*IOSYSCFG).

[2] Komendy SNDTCPSPLF i LPR używają tych samych kombinacji uprawnień obiektu odniesienia, co 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.

6 Informacje o wymaganych uprawnieniach zawiera opis w sekcji Wyświetlenie (Display - DSP) lub inna operacja korzystająca ze zbioru wyjściowego (OUTPUT(*OUTFILE)) w temacie Zasady ogólne dotyczące uprawnień do obiektów dla komend.

Komendy opisu strefy czasowej

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend opisu strefy czasowej.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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 aktualizacji

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend danych zamówienia aktualizacji.

Te komendy mają uprawnienia publiczne *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	Do biblioteki
WRKORDINF	Zbiór QGPL/QMAHFILE	*CHANGE, *OBJALTER	*EXECUTE

Komendy indeksu użytkownika, kolejki użytkownika, przestrzeni użytkownika

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend indeksu użytkownika, kolejki użytkownika i przestrzeni użytkownika.

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 systemu plików użytkownika

W poniższej tabeli zamieszczono uprawnienia szczegółowe wymagane dla komend systemu plików użytkownika.

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu
ADDMFS [1,2,3]	katalog_do_podłączenia	*DIR	″root″ (/)	*W
	Przedrostek ścieżki	Więcej informacji znajduje się w zasadach ogólnych.		
CRTUDFS [1,2,6,7] (Q)	/dev/QASP*xx* lub /dev/IASPname	*DIR	″root″ (/)	*RWX
DLTUDFS [1,2,4,5,8,9,10] (Q)	/dev/QASP*xx* lub /dev/IASPname	*DIR	″root″ (/)	*RWX
	dowolny obiekt zintegrowanego systemu plików w systemie UDFS		″root″ (/)	*OBJEXIST
	Dowolny niepusty obiekt katalogu	*DIR	″root″ (/)	*WX
DSPUDFS	jakieś_katalogixx	*DIR	″root″ (/)	*RX
MOUNT [1,2,3]	katalog_do_podłączenia	*DIR	″root″ (/)	*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] Istnieją dwie konwencje nazewnictwa, w zależności od miejsca, w którym znajduje się system plików użytkownika (UDFS). Należy korzystać z jednej z poniższych konwencji:

- - /dev/QASPxx, gdzie zamiast *xx* należy podać 01 dla systemowej asp, lub 02-32 dla podstawowych asp użytkowników.
- - /dev/IASPnazwa, gdzie zamiast *IASPnazwa* należy podać nazwę niezależnej ASP.

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.

Komenda	Obiekt odniesienia	Typ obiektu	System plików	Wymagane uprawnienie do obiektu

[6] Użytkownik musi posiadać uprawnienia specjalne *ALLOBJ i *SECADM, aby móc określić wartość inną niż *PARENT dla opcji skanowania dla obiektów (CRTOBJSCAN).

[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).

[8] Użytkownik musi posiadać uprawnienia zapisu (*W) i uruchamiania (*X) dla wszystkich obiektów katalogu w systemie plików UDFS, które nie są puste.

[9] Jeśli obiekt katalogu, który nie jest pusty, ma w systemie plików UDFS atrybut ″ograniczona zmiana nazwy i usuwanie dowiązań″ ustawiony na Tak (atrybut ten jest równoważny z bitem trybu S_ISVTX), to musi być spełniony co najmniej jeden z poniższych warunków:

- Użytkownik musi być właścicielem wszystkich obiektów znajdujących się w katalogu.
- Użytkownik musi być właścicielem katalogu.
- Użytkownik musi posiadać uprawnienie specjalne *ALLOBJ.

[10] Systemu plików UDFS nie można usunąć, jeśli zawiera on obiekt z wartością atrybutu *tylko do odczytu* ustawioną na *tak* lub jeśli zawiera obiekt, który został pobrany.

Komendy profilu użytkownika

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend profilu użytkownika.

Komendy oznaczone literą (Q) wymagają uprawnień publicznych *EXCLUDE. Dodatek C, “Komendy z uprawnieniami publicznymi *EXCLUDE”, na stronie 339 zawiera informacje o tym, które profile użytkowników IBM mają uprawnienia do korzystania z tych komend. Osoba odpowiedzialna za bezpieczeństwo może nadawać innym uprawnienie *USE.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		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)			

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
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			
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
DMPUSRPRF [22](Q)	Profil użytkownika		
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.
DSPSSTUSR [23]			
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	

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
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	

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 określić wartość inną niż *NONE dla parametru Zezwalaj na różnice w obiektach (Allow object differences - ALWOBJDIF), użytkownik musi posiadać specjalne uprawnienia.

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 Do użycia tej komendy konieczne jest uprawnienie specjalne *JOBCTL.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**

[16] Aby podać wartość SECDTA(*PWDGRP), USRPRF(*ALL) lub OMITUSRPRF, użytkownik musi mieć uprawnienia specjalne *ALLOBJ i *SECADM.

[17] Komendą 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 jest przenoszona do innego systemu, uprawnienia prywatne, prawa własności do obiektu oraz pozycje grupy podstawowej będą dołączone w systemie docelowym do profilu o tej samej nazwie. Jeśli w systemie docelowym taki profil nie istnieje, zostanie on 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 wyświetlić bieżącą wartość kontrolowania obiektu i działania, użytkownik musi posiadać uprawnienia specjalne *ALLOBJ lub *AUDIT. W przeciwnym razie wyświetlona zostanie wartość *NOTAVL, oznaczająca, że wartości nie mogły zostać wyświetlone.

[20] Aby pobrać bieżące wartości OBJAUD i AUDLVL kontrolowania obiektu, użytkownik musi mieć uprawnienie specjalne *ALLOBJ lub *AUDIT. W przeciwnym razie zostanie zwrócona wartość *NOTAVL, oznaczająca, że wartości nie mogły zostać pobrane.

[21] Aby użyć tej komendy, należy mieć uprawnienie specjalne serwisu (*SERVICE) lub być upoważnionym do funkcji Zrzut serwisowy w systemie i5/OS poprzez obsługę Administrowanie aplikacjami w programie System i Navigator. Do zmiany listy użytkowników mających prawo wykonywania operacji zrzutu można użyć również komendy Zmiana użycia funkcji (Change Function Usage - CHGFCNUSG) z ID funkcji QIBM_SERVICE_DUMP.

[22] Aby użyć tej komendy, należy mieć uprawnienie specjalne *SERVICE lub upoważnienie do użycia funkcji QIBM_SERVICE_DUMP.

[23] Aby użyć tej komendy, należy mieć uprawnienie specjalne administratora bezpieczeństwa (*SECADM) lub kontroli (*AUDIT).

Komendy listy sprawdzania

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend listy sprawdzania.

Komenda	Obiekt odniesienia	Wymagane uprawnienia	
		Do obiektu	**Do biblioteki**
CRTVLDL	Lista weryfikacji		*ADD, *READ
DLTVLDL	Lista weryfikacji	*OBJEXIST	*EXECUTE

Komendy dostosowania stacji roboczej

W tej tabeli podane są uprawnienia szczegółowe wymagane przez poszczególne komendy dostosowania stacji roboczej.

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	**Dla 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

Komenda	Obiekt odniesienia	Wymagane uprawnienie	
		Dla obiektu	Dla biblioteki
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

Niniejsza tabela zawiera listę uprawnień szczegółowych wymaganych dla komend programu piszącego.

Komenda	Obiekt odniesienia	Parametry kolejki wyjściowej		Uprawnienia specjalne	Wymagane uprawnienia	
		AUTCHK	OPRCTL		Do obiektu	Do biblioteki
CHGWTR [2, 4]	Bieżąca kolejka wyjściowa [1]	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Właściciel [3]	
			*YES	*JOBCTL		
	Nowa kolejka wyjściowa	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
ENDWTR [1]	Kolejka wyjściowa	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Właściciel [3]	
			*YES	*JOBCTL		
HLDWTR [1]	Kolejka wyjściowa	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Właściciel [3]	
			*YES	*JOBCTL		
RLSWTR [1]	Kolejka wyjściowa	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Właściciel [3]	
			*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	

Komenda	Obiekt odniesienia	Parametry kolejki wyjściowej		Uprawnienia specjalne	Wymagane uprawnienia	
		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
	Obiekt dostosowywania stacji roboczej				*USE	*EXECUTE
	Program sterownika użytkownika				*OBJOPR *EXECUTE	*EXECUTE
	Program transformacji danych użytkownika				*OBJOPR *EXECUTE	*EXECUTE
	Program separatora użytkownika				*OBJOPR *EXECUTE	*EXECUTE
	Opis urządzenia				*OBJOPR, *READ	
STRRMTWTR [1]	Kolejka wyjściowa	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Właściciel [3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Kolejka komunikatów				*OBJOPR, *ADD	*EXECUTE
	Obiekt dostosowywania stacji roboczej				*USE	*EXECUTE
	Program sterownika użytkownika				*OBJOPR *EXECUTE	*EXECUTE
	Program transformacji danych użytkownika				*OBJOPR *EXECUTE	*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. Operacje na obiektach i kontrola

W tej kolekcji tematów opisano operacje, które można wykonywać na obiektach systemu oraz zamieszczono informacje o kontrolowaniu tych operacji.

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 dla akcji zapisywany jest rekord kontroli, zależy od kilku wartości systemowych, w tym wartości w profilu użytkownika wykonującego akcję i wartości zdefiniowanej dla obiektu. Sekcja “Planowanie kontroli dostępu do obiektu” na stronie 296 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

Poniżej znajduje się lista działań, które można wykonać wszystkich typach obiektów oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

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)

QSRSAVO
Zapisywanie API obiektu

QsrSave
Zapisywanie obiektu w API katalogu

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).

- Operacja zmiany

APYJRNCHG
Zastosowanie kronikowanych zmian (Apply Journaled Changes)

CHGJRNOBJ
Change Journaled Object (Zmiana kronikowanego obiektu)

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

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)

QSRRSTO
Odzyskiwanie API obiektu

QsrRestore
Odzyskiwanie obiektu w API katalogu

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[1]
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
Wyśw. uprawnień dla obiektu

EDTOBJAUT
Edycja uprawnień dla obiektu

---

1. Gdy wymagana jest podpowiedź dla komendy, program przesłonięcia podpowiedzi wyświetla bieżące wartości. Na przykład, po wpisaniu CHGURSPRF USERA i naciśnięciu F4 (podpowiedź), ekran Zmiana profilu użytkownika wyświetli wartości bieżące profilu użytkownika USERA

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)

RMVDFRID
Usuń identyfikator odroczenia

RSTDFROBJ
Odtwarzanie odroczonego obiektu biblioteki

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 obiekt. wg właścicieli

WRKxxx
Praca z komendami obiektu (Work with object commands)

Operacje na czasach odtworzenie ścieżki dostępu

Poniżej znajduje sie lista działań, które można wykonać na czasach odtworzenie ścieżki dostępu (*Times) oraz informacje, które z tych operacji są kontrolowane.

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.

- Operacje kontrolowane

  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 na tabeli alertów (*ALRTBL)

Poniżej znajduje sie lista działań, które można wykonać na tabeli alertów (*ALRTBL) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

Brak

- Operacja zmiany

  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 na liście autoryzacji (*AUTL)

Poniżej znajduje się lista działań, które można wykonać na liście autoryzacji (*AUTL) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Brak

- Operacja zmiany

  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 na magazynie uprawnień (*AUTHLR)

Poniżej znajduje się lista działań, które można wykonać na magazynie uprawnień (*AUTHLR) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Brak

- Operacja zmiany

  Powiązana
  Gdy jest używana do zabezpieczenia obiektu.

- Operacje, które nie są kontrolowane

  DSPAUTHLR
  Wyświetlenie magazynu uprawnień (Display Authority Holder)

Operacje na katalogu konsolidacji (*BNDDIR)

Poniżej znajduje sie lista działań, które można wykonać na katalogu konsolidacji (*BNDDIR) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  CRTPGM
  Tworzenie programu (Create Program)

  CRTSRVPGM
  Tworzenie programu usługowego (Create Service Program)

  RTVBNDSRC
  Odtworzenie źródła konsolid.

  UPDPGM
  Aktualizacja programu (Update Program)

  UPDSRVPGM
  Aktualizacja programu usługowego (Update Service Program)

- Operacja zmiany

  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 na liście konfiguracji (*CFGL)

Poniżej znajduje się lista działań, które można wykonać na liście konfiguracji (*CFGL) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

CPYCFGL
Kopiowanie listy konfiguracji (Copy Configuration List). Zapisywany jest wpis *Z listy konfiguracji*.

- Operacja zmiany

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 na plikach specjalnych (*CHRSF)

Poniżej znajduje sie lista działań, które można wykonać na plikach specjalnych (*CHRSF) oraz informacje, które z tych operacji są kontrolowane.

Informacje dotyczące kontrolowania plików specjalnych (*CHRSF) zawiera sekcja Operacje dotyczące pliku strumieniowego (*STMF).

Operacje na formatach wykresu (*CHTFMT)

Poniżej znajduje się lista działań, które można wykonać na formatach wykresu (*CHTFMT) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

Wyświetlanie (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

- Operacja zmiany

Brak

- Operacje, które nie są kontrolowane

Brak

Operacje na ustawieniach narodowych C(*CLD)

Poniżej znajduje sie lista działań, które można wykonać na ustawieniach narodowych C (*CLD) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

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.

- Operacja zmiany

  Brak

- Operacje, które nie są kontrolowane

  Brak

Operacje na opisach żądania zmiany (*CRQD)

Poniżej znajduje sie lista działań, które można wykonać na opisie żądania zmiany (*CRQD) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  QFVLSTA
  Funkcja API List Change Request Description Activities

  QFVRTVCD
  Funkcja API Retrieve Change Request Description

  SBMCRQ
  Wprowadzenie żądania CRQ (Submit Change Request)

- Operacja zmiany

  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 aktywności opisu żądania zmiany

- Operacje, które nie są kontrolowane

WRKCRQD
Praca z opisami CRQ (Work with Change Request Description)

Operacje na klasie(*CLS)

Poniżej znajduje się lista działań, które można wykonać na klasach (*CLS) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

Brak

- Operacja zmiany

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 na komendzie (*CMD)

Poniżej znajduje się lista działań, które można wykonać na komendzie (*CMD) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

Uruchamianie (Run)
Gdy komenda jest uruchamiana

- Operacja zmiany

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. Użycie tych komend nie jest kontrolowane.

CALL [1]
CALLPRC
CHGVAR
COPYRIGHT
DCL
DCLF
DO
ELSE
ENDDO
	ENDPGM
	ENDRCV
	GOTO
	IF
	MONMSG
	PGM
		RCVF
		RETURN
		SNDF
		SNDRCVF
		TFRCTL
		WAIT

[1] Komenda CALL jest kontrolowana, gdy zostanie uruchomiona interaktywnie. Nie jest kontrolowana w przypadku uruchamiania w programie CL.		

Operacje na liście połączeń (*CNNL)

Poniżej znajduje się lista działań, które można wykonać na liście połączeń (*CNNL) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Brak

- Operacja zmiany

  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 na opisach klasy usług (*COSD)

Poniżej znajduje sie lista działań, które można wykonać na opisach klasy usług (*COSD) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Brak

- Operacja zmiany

  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 na informacjach po stronie komunikacyjnej (*CSI)

Poniżej znajduje sie lista działań, które można wykonać na informacjach po stronie komunikacyjnej (*CSI) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  DSPCSI
  Wyświetlenie informacji po stronie komunikacyjnej (Display Communications Side Information)

  Inicjowanie (Initialize)
  Inicjowanie konwersacji (Initialize conversation)

- Operacja zmiany

  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 na międzysystemowej mapie produktu (*CSPMAP)

Poniżej znajduje się lista działań, które można wykonać na międzysystemowej mapie produktu (*CSPMAP) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Odniesienie
  Gdy dotyczy aplikacji CSP

- Operacja zmiany

  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 na międzysystemowej tabeli produktu (*CSPTBL)

Poniżej znajduje się lista działań, które można wykonać na międzysystemowej tabeli produktu (*CSPTBL) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Odniesienie
  Gdy dotyczy aplikacji CSP
- Operacja zmiany

  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 na opisach kontrolera (*CTLD)

Poniżej znajduje sie lista działań, które można wykonać na opisach kontrolera (*CTLD) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  SAVCFG
  Składowanie konfiguracji (Save Configuration)

  VFYCMN
  Testowanie łącza (Link test)
- Operacja zmiany

  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 na opisach urządzeń (*DEVD)

Poniżej znajduje sie lista działań, które można wykonać na opisach urządzeń (*DEVD) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Uzyskiwanie (Acquire)
  Pierwsze pozyskanie urządzenia podczas operacji otwarcia lub jawnej operacji uzyskiwania.

  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)

- Operacja zmiany

  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 na katalogu (*DIR)

Poniżej znajduje się lista działań, które można wykonać na obiektach katalogu(*DIR) oraz informacje, które z tych operacji są kontrolowane.

- 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 obiektów

  faccessx
  Określenie dostępności zbioru dla klasy użytkowników przez deskryptor

  getcwd, qlgGetcwd
  Funkcja API Get Path Name of Current Directory

  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 obiektu (Save Object)

  WRKLNK
  Praca z dowiązaniami (Work with Links)

- Operacja zmiany

CHGATR
Zmiana atrybutów (Change Attributes)

CHGAUD
Zmiana wartości kontroli

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 obiektu (Copy Object)

CRTDIR
Tworzenie katalogu

fchmod
Funkcja API Change File Authorizations by Descriptor

fchown
Funkcja API Change Owner and Group of File by Descriptor

mkdir, QlgMkdir
Funkcja API Make Directory

MOV Przeniesienie obiektu (Move Object)

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 obiektu (Rename Object)

RST Odtworzenie obiektu (Restore Object)

utime, QlgUtime
Funkcja API Set File Access and Modifcation Times

WRKAUT
Praca z uprawnieniami (Work with Authority)

WRKLNK
Praca z dowiązaniami obiektów

- 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 deskryptor

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 na serwerze katalogów

Poniżej znajduje się lista działań, które można wykonać na serwerze katalogów oraz informacje, które z tych operacji są kontrolowane.

Uwaga: Operacje serwera katalogów są kontrolowane, jeśli wartość systemowa kontroli działania (QAUDLVL) lub parametr kontroli działania (AUDLVL) w profilu użytkownika zawiera wartość *OFCSRV.

- peracje kontrolowane

  Dodanie (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 działające na katalogu mogą być kontrolowane oddzielnie, za pomocą funkcji kontroli obiektów.

  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)

  Sporządzenie listy (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 na obiektach biblioteki dokumentów(*DOC lub *FLR)

Poniżej znajduje się lista działań, które można wykonać na obiektach biblioteki dokumentów (*DOC lub *FLR) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

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 katalogu, zaś kontrolowanie obiektów określone jest dla katalogu, to 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

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.

- Operacja zmiany

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)

CHGDLOPGP
Zmiana grupy podstawowej DLO (Change DLO Primary Group)

CHGDOCD
Zmiana opisu dokumentu (Change Document Description)

CHGDSTD
Zmiana opisu dystrybucji (Change Distribution Description)

CPYDOC [2]
Kopiowanie dokumentu (Copy Document)

Uwaga: Jeśli dokument docelowy już istnieje, zapisywana jest pozycja zmiany.

CRTFLR
Tworzenie folderu (Create Folder)

CVTTOFLR [2]
Konwersja do folderu (Convert to Folder)

DLTDLO [2]
Usunięcie obiektu DLO (Delete DLO)

DLTSHF
Usunięcie półki (Delete Bookshelf)

DTLDOCL [2]
Usunięcie listy dokumentów (Delete Document List)

DLTDST [2]
Usunięcie dystrybucji (Delete Distribution)

---

2. Jeśli dokument docelowy dla operacji znajduje się w folderze, pozycja zmiany zapisywana jest zarówno dla dokumentu jak i dla folderu.

EDTDLOAUT
Edycja uprawnień dla DLO (Edit DLO Authority)

EDTDOC
Edycja dokumentu (Edit Document)

FILDOC [2]
Zapisanie dokumentu (File Document)

GRTACCAUT
Nadanie uprawnień dla kodu dostępu (Grant Access Code Authority)

GRTUSRPMN
Nadanie uprawnień specjalnych użytkowników (Grant User Permission)

MOVDOC [2]
Przeniesienie dokumentu (Move Document)

MRGDOC [2]
Scalanie dokumentu (Merge Document)

PAGDOC
Stronicowanie dokumentu (Paginate Document)

QHFCHGAT
Funkcja API Change Directory Entry Attributes

QHFSETSZ
Funkcja API Set Stream File Size

QHFWRTSF
Funkcja API Write Stream File

QRYDOCLIB [2]
Zapytanie o biblioteki dokumentów (Query Document Library)

Uwaga: Jeśli zastępowany jest odszukany istniejący dokument, zapisywana jest pozycja zmiany.

RCVDST [2]
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 [2]
Zmiana nazwy obiektu DLO (Rename DLO)

RPLDOC
Zastąpienie dokumentu (Replace Document)

RSTDLO [2]
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 [2]
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 na obszarze danych (*DTAARA)

Poniżej znajduje sie lista działań, które można wykonać na obszarze danych (*DTAARA) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

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

- Operacja zmiany

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 dla Narzędzia IDDU (*DTADCT)

Poniżej znajduje się lista działań, które można wykonać dla Narzędzia IDDU (*DTADCT) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

Brak

- Operacja zmiany

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

Wyświetlanie (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 na kolejce danych (*DTAQ)

Poniżej znajduje sie lista działań, które można wykonać na kolejce danych (*DTAQ) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

QMHRDQM
Funkcja API Retrieve Data Queue Message

- Operacja zmiany

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 na opisach edycji (*EDTD)

Poniżej znajduje sie lista działań, które można wykonać na opisach edycji (*EDTD) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

DSPEDTD
Wyświetlenie opisu edycji (Display Edit Description)

QECCVTEC
Funkcja API Edit code expansion (za pomocą procedury QECEDITU)

- Operacja zmiany

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 dla rejestrowania wyjścia (*EXITRG)

Poniżej znajduje sie lista działań, które można wykonać dla rejestrowania wyjścia (*EXITRG) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

QUSRTVEI
Funkcja API Retrieve Exit Information

QusRetrieveExitInformation
Funkcja API Retrieve Exit Information

- Operacja zmiany

ADDEXITPGM
Dodanie programu obsługi wyjścia (Add Exit Program)

QUSADDEP
Funkcja API Add Exit Program

QusAddExitProgram
Funkcja API Add Exit Program

QUSDRGPT
Funkcja API Unregister Exit Point

QusDeregisterExitPoint
Funkcja API Unregister 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 na tabelach sterujących formularzy (*FCT)

Poniżej znajduje sie lista działań, które można wykonać na tabelach sterujących formularzy (*FCT) oraz informacje, które z tych operacji są kontrolowane.

- Dla obiektu typu *FCT operacje odczytu lub zmiany nie są kontrolowane.

Operacje na zbiorze (*FILE)

Poniżej znajduje sie lista działań, które można wykonać na obiektach folderu (*FILE) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  CPYF Kopiowanie zbioru (Copy File) (korzysta z operacji otwierania)

  Otwarcie (Open)
  Otwarcie zbioru do odczytu

  DSPPFM
  Wyświetlenie podzbioru fizycznego (Display Physical File Member) (korzysta z operacji otwierania)

  Otwarcie (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

- Operacja zmiany

Otwarcie (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)

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

CHGPFTRG
Zmiana zbioru fizycznego (Change Physical File Trigger)

DSPCPCST
Wyświetlenie ograniczeń oczekujących na sprawdzenie (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 ograniczeń oczekujących na sprawdzenie (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 na plikach FIFO (*FIFO)

Poniżej znajduje się lista działań, które można wykonać na obiektach FIFO (*FIFO) oraz informacje, które z tych operacji są kontrolowane.

Informacje dotyczące kontroli zbiorów *FIFO zawiera sekcja Operacje dotyczące pliku strumieniowego (*STMF).

Operacje na folderze (*FLR)

Poniżej znajduje się lista działań, które można wykonać na obiektach folderu (*FLR) oraz informacje, które z tych operacji są kontrolowane.

Patrz publikacja na temat działań “Operacje na obiektach biblioteki dokumentów(*DOC lub *FLR)” na stronie 532

Operacje na zasobach czcionek (*FNTRSC)

Poniżej znajduje się lista działań, które można wykonać na zasobach czcionek (*FNTRSC) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Drukowanie (Print)
  Drukowanie zbioru buforowego, który odnosi się do zasobu czcionki

- Operacja zmiany

  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 na definicji formularza (*FORMDF)

Poniżej znajduje się lista działań, które można wykonać na definicji formularza (*FORMDF) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Drukowanie (Print)
  Drukowanie zbioru buforowego, który odnosi się do definicji formularza

- Operacja zmiany

  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 na obiektach filtra (*FTR)

Poniżej znajduje sie lista działań, które można wykonać na obiektach filtra (*FTR) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

Brak

- Operacja zmiany

  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 na zestawach symboli graficznych (*GSS)

Poniżej znajduje się lista działań, które można wykonać na zestawach symboli graficznych (*GSS) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Załadowany (Loaded)
  Gdy jest załadowany

  Czcionka (Font)
  Gdy jest używany jako czcionka w zbiorze drukarkowym opisanym zewnętrznie

- Operacja zmiany

Brak

- Operacje, które nie są kontrolowane

  WRKGSS
  Praca ze zestawem symboli graficznych (Work with Graphic Symbol Set)

Operacje na słownikach zestawów znaków dwubajtowych (*IGCDCT)

Poniżej znajduje się lista działań, które można wykonać na słownikach zestawów znaków dwubajtowych (*IGCDCT) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  DSPIGCDCT
  Wyświetlenie słownika IGC (Display IGC Dictionary)

- Operacja zmiany

  EDTIGCDCT
  Edycja słownika IGC (Edit IGC Dictionary)

Operacje dla sortowania zestawów znaków dwubajtowych (*IGCSRT)

Poniżej znajduje się lista działań, które można wykonać dla sortowania zestawów znaków dwubajtowych (*IGCSRT) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  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)

- Operacja zmiany

  CPYIGCSRT
  Kopiowanie tabeli 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)

  Aktualizacja
  Aktualizowanie aktywnej tabeli sortowania (opcja 5 z menu CGU)

- Operacje, które nie są kontrolowane

  FMTDTA
  Sortowanie rekordów lub pól w zbiorze

Operacje na tabeli zestawu znaków dwubajtowych (*IGCTBL)

Poniżej znajduje się lista działań, które można wykonać na tabeli zestawów znaków dwubajtowych (*IGCTBL) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  CPYIGCTBL
  Kopiowanie tabeli IGC (Copy IGC Table)

  STRFMA
  Uruchomienie FMA (Start Font Management Aid)
- Operacja zmiany

  STRFMA
  Uruchomienie FMA (Start Font Management Aid)
- Operacje, które nie są kontrolowane

  CHKIGCTBL
  Sprawdzanie tabeli IGC (Check IGC Table)

Operacje na opisach zadania (*JOBD)

Poniżej znajduje sie lista działań, które można wykonać na opisach zadania (*JOBD) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Brak
- Operacja zmiany

  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 na kolejce zadań (*JOBQ)

Poniżej znajduje się lista działań, które można wykonać na kolejce zadań (*JOBQ) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Brak
- Operacja zmiany

  Pozycja (Entry)
  Gdy pozycja jest umieszczana lub usuwana z kolejki

  CHGJOBQ
  Zmiana kolejki zadań

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 211
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 211
Zmiana pozycji kolejki zadań (Change Job Queue Entry)

QSPRJOBQ
Odtworzenie informacji kolejki zadań

RMVJOBQE “Opisy podsystemów” na stronie 211
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

WRKJOBQD
Praca z opisem kolejki zadań

Operacje na obiektach programu planującego zadania (*JOBSCD)

Poniżej znajduje się lista działań, które można wykonać na obiektach programu planującego zadania (*JOBSCD) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

Brak

- Operacja zmiany

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)

3. Rekord kontroli jest zapisywany wtedy, gdy w opisie podsystemu (*SBSD) określono kontrolowanie obiektu.

RLSJOBSCDE
Zwolnienie pozycji harmonogramu zadań (Release Job Schedule Entry)

- Operacje, które nie są kontrolowane

Wyświetlanie (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 na kronice (*JRN)

Poniżej znajduje się lista działań, które można wykonać na kronice (*JRN) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

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)

- Operacja zmiany

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)

Operacje na dzienniku (*JRNRCV)

Poniżej znajduje sie lista działań, które można wykonać na dzienniku (*JRNRCV) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

Brak

- Operacja zmiany

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 na bibliotece (*LIB)

Poniżej znajduje się lista działań, które można wykonać na bibliotece (*LIB) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  DSPLIB
  Wyświetlanie biblioteki (Jeśli biblioteka nie jest pusta. jeśli jest pusta, nie jest przeprowadzana żadna kontrola.)

  Odnajdywanie (Locate)
  Gdy ma być odszukany obiekt

  Uwaga:

  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 OBJ(AR/WRK*) OBJTYPE(*FILE)
     ```

     Jeśli biblioteka o nazwie “AR” nie posiada żadnych nazw zbiorów zaczynających się od “WRK”, nie jest zapisywany dla niej rekord kontroli.

  Lista bibliotek (Library list)
  Dodawanie biblioteki do listy bibliotek

- Operacja zmiany

  CHGLIB
  Zmiana biblioteki (Change Library)

  CLRLIB
  Usuwanie zawartości biblioteki (Clear Library)

  MOVOBJ
  Przeniesienie obiektu (Move Object)

  RNMOBJ
  Zmiana nazwy obiektu (Rename Object)

  Dodanie (Add)
  Dodawanie obiektu do biblioteki

  Usunięcie (Delete)
  Usunięcie obiektu z biblioteki

- Operacje, które nie są kontrolowane

  Brak

Operacje na opisach linii (*LIND)

Poniżej znajduje sie lista działań, które można wykonać na opisach linii (*LIND) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  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)

- Operacja zmiany

  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 na usługach poczty

Poniżej znajduje sie lista działań, które można wykonać na usługach poczty oraz informacje, które z tych operacji są kontrolowane.

Uwaga: Operacje usług pocztowych są kontrolowane, jeśli wartość systemowa kontroli działania (QAUDLVL) lub parametr kontroli działania (AUDLVL) w profilu użytkownika zawiera wartość *OFCSRV.

- Operacje kontrolowane

  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.

  Otwarcie (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

  Zbiór (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

  Wysłanie (Send)
  Wysyłanie pozycji poczty

  Przeglądanie (View)
  Przeglądanie pozycji poczty

Operacje dla menu (*MENU)

Poniżej znajduje sie lista działań, które można wykonać dla menu (*MENU) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Wyświetlanie (Display)
  Wyświetlanie menu przy użyciu komendy GO MENU lub okna dialogowego UIM
- Operacja zmiany

  CHGMNU
  Zmiana menu (Change menu)
- Operacje, które nie są kontrolowane

Powrót (Return)
Powracanie do menu - w stosie menu - które było już wyświetlane

DSPMNUA
Wyświetlanie atrybutów menu

WRKMNU
Praca z menu

Operacje na opisach trybów (*MODD)

Poniżej znajduje sie lista działań, które można wykonać na opisach trybu (*MODD) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Brak

- Operacja zmiany

  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 na obiekcie modułu(*MODULE)

Poniżej znajduje sie lista działań, które można wykonać na obiekcie modułu (*MODULE) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  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.

- Operacja zmiany

  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 na zbiorze komunikatów (*MSGF)

Poniżej znajduje się lista działań, które można wykonać na zbiorze komunikatów (*MSGF) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  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)

- Operacja zmiany

  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 na kolejce komunikatów (*MSGQ)

Poniżej znajduje sie lista działań, które można wykonać na kolejce komunikatów (*MSGQ) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

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.

- Operacja zmiany

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)

Program
Programowanie działania kolejki komunikatów

Operacje na grupie węzłów (*NODGRP)

Poniżej znajduje sie lista działań, które można wykonać na grupie węzłów (*NODGRP) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  DSPNODGRP
  Wyświetlenie grupy węzłów (Display Node Group)

- Operacja zmiany

  CHGNODGRPA
  Zmiana grupy węzłów (Change Node Group)

Operacje na liście węzłów (*NODL)

Poniżej znajduje się lista działań, które można wykonać na liście węzłów (*NODL) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  QFVLSTNL
  Listowanie pozycji listy węzłów (List node list entries)

- Operacja zmiany

  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 na opisie NetBIOS (*NTBD)

Poniżej znajduje sie lista działań, które można wykonać na opisie NetBIOS (*NTBD) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  SAVCFG
  Składowanie konfiguracji (Save Configuration)

- Operacja zmiany

  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 na interfejsie sieciowym (*NWID)

Poniżej znajduje sie lista działań, które można wykonać na interfejsie sieciowym (*NWID) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  SAVCFG
  Składowanie konfiguracji (Save Configuration)
- Operacja zmiany

  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 na opisach serwerów sieciowych (*NWSD)

Poniżej znajduje sie lista działań, które można wykonać na opisach serwerów sieciowych (*NWSD) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  SAVCFG
  Składowanie konfiguracji (Save Configuration)
- Operacja zmiany

  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 na kolejce wyjściowej (*OUTQ)

Poniżej znajduje sie lista działań, które można wykonać na kolejce wyjściowej (*OUTQ) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  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)
- Operacja zmiany

  Umieszczenie (Placement)
  Gdy pozycja jest umieszczana lub usuwana z kolejki

  CHGOUTQ
  Zmiana kolejki wyjściowej (Change Output Queue)

  CHGSPLFA [4]
  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 [4]
  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 [4]
  Zmiana atrybutów zbioru buforowego (Change Spooled File Attributes)

  CPYSPLF [4]
  Kopiowanie zbioru buforowego (Copy Spooled File)

  Twórz [4]
  Tworzenie zbioru buforowego

  DSPSPLF [4]
  Wyświetlenie zbioru buforowego (Display Spooled File)

HLDSPLF [4]
Wstrzymanie zbioru buforowego (Hold Spooled File)

QSPROUTQ
Odtwarzanie informacji kolejki wyjściowej (Retrieve output queue information)

RLSSPLF [4]
Zwolnienie zbioru buforowego (Release Spooled File)

SNDNETSPLF [4]
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 na nakładce (*OVL)

Poniżej znajduje sie lista działań, które można wykonać na nakładce (*OVL) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Drukowanie (Print)
  Drukowanie zbioru buforowego, który odnosi się do nakładki
- Operacja zmiany

  Brak
- Operacje, które nie są kontrolowane

  WRKOVL
  Praca z nakładkami (Work with overlay)

  Drukowanie (Print)
  Odniesienie do nakładki podczas tworzenia zbioru buforowego

Operacje na definicjach stron (*PAGDFN)

Poniżej znajduje sie lista działań, które można wykonać na definicjach stron (*PAGDFN) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Drukowanie (Print)
  Drukowanie zbioru buforowego, który odnosi się do definicji strony
- Operacja zmiany

  Brak
- Operacje, które nie są kontrolowane

  WRKPAGDFN
  Praca z definicjami stron (Work with Page Definition)

4. Kontrola ma miejsce również wtedy, gdy kontrolowanie działania (wartość systemowa QAUDLVL lub wartość AUDLVL w profilu użytkownika) obejmuje *SPLFDTA.

Drukowanie (Print)
Odniesienie do definicji formularza podczas tworzenia zbioru buforowego

Operacje na segmentach stron (*PAGSEG)

Poniżej znajduje sie lista działań, które można wykonać na segmentach stron (*PAGSEG) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Drukowanie (Print)
  Drukowanie zbioru buforowego, który odnosi się do segmentu strony

- Operacja zmiany

  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 na grupie deskryptorów wydruków (*PDG)

Poniżej znajduje sie lista działań, które można wykonać na grupie deskryptorów wydruków (*PDG) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Otwarcie (Open)
  Gdy grupa deskryptorów wydruków jest otwierana do odczytu za pomocą funkcji API PrintManager lub słowa CPI.

- Operacja zmiany

  Otwarcie (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 na programie (*PGM)

Poniżej znajduje sie lista działań, które można wykonać na programie (*PGM) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  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)

- Operacja zmiany

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 na panelach grupowych (*PNLGRP)

Poniżej znajduje sie lista działań, które można wykonać na panelach grupowych (*PNLGRP) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  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

- Operacja zmiany

  Brak

- Operacje, które nie są kontrolowane

  WRKPNLGRP
  Praca z panelami grupowymi (Work with Panel Group)

Operacje dla dostępności produktu (*PRDAVL)

Poniżej znajduje się lista działań, które można wykonać dla dostępności produktu (*PRDAVL) oraz informacje, które z tych operacji są kontrolowane.

- Operacja zmiany

  WRKSPTPRD
  Praca z obsługiwanymi produktami (Work with Supported Products), podczas dodawania lub usuwania obsługi

- Operacje, które nie są kontrolowane

  Odczyt (Read)
  Żadne operacje odczytu nie są kontrolowane

Operacje na definicji produktu (*PRDDFN)

Poniżej znajduje się lista działań, które można wykonać na definicji produktu (*PRDDFN) oraz informacje, które z tych operacji są kontrolowane.

- Operacja zmiany

  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

Odczyt (Read)
Żadne operacje odczytu nie są kontrolowane

Operacje na ładowaniu produktu (*PRDLOD)

Poniżej znajduje się lista działań, które można wykonać na ładowaniu produktu (*PRDLOD) oraz informacje, które z tych operacji są kontrolowane.

- Operacja zmiany

Zmiana (Change)
Stan ładowania produktu, lista bibliotek dla ładowania produktu, lista folderów dla ładowania produktu, język podstawowy

- Operacje, które nie są kontrolowane

Odczyt (Read)
Żadne operacje odczytu nie są kontrolowane

Operacje na formularzu menedżera zapytań(*QMFORM)

Poniżej znajduje się lista działań, które można wykonać na formularzu menedżera zapytań (*QMFORM) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

STRQMQRY
Uruchomienie zapytania menedżera zapytań (Start Query Management Query)

RTVQMFORM
Odtworzenie formularza menedżera zapytań (Retrieve Query Management Form)

Uruchamianie (Run)
Uruchomienie zapytania

Eksportowanie
Eksportowanie formularza menedżera zapytań

Drukowanie (Print)
Drukowanie formularza menedżera zapytań

Drukowanie raportu menedżera zapytań za pomocą formularza

Używanie (Use)
Przejdź do formularza za pomocą opcji 2, 5, 6, lub 9, albo funkcji F13 programu DB2 Query Manager and SQL Development Kit for i5/OS.

- Operacja zmiany

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 na zapytaniu menedżera zapytań(*QMQRY)

Poniżej znajduje się lista działań, które można wykonać na zapytaniu menedżera zapytań (*QMQRY) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  RTVQMQRY
  Odtworzenie zapytania menedżera zapytań (Retrieve Query Manager Query)

  Uruchamianie (Run)
  Uruchomienie zapytania menedżera zapytań

  STRQMQRY
  Uruchomienie zapytania menedżera zapytań (Start Query Manager Query)

  Eksportowanie
  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)

- Operacja zmiany

  CRTQMQRY
  Tworzenie zapytania menedżera zapytań (Create Query Management Query)

  Konwertowanie (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 na definicji zapytania (*QRYDFN)

Poniżej znajduje się lista działań, które można wykonać na definicji zapytania (*QRYDFN) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  ANZQRY
  Analiza zapytania (Analyze Query)

Zmiana (Change)
Zmiana zapytania za pomocą ekranu podpowiedzi komendy WRKQRY lub QRY.

Wyświetlanie (Display)
Wyświetlenie zapytania za pomocą ekranu podpowiedzi WRKQRY

Eksportowanie
Eksportowanie formularza za pomocą menedżera zapytań

Eksportowanie
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)

Uruchamianie (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)

- Operacja zmiany

  Zmiana (Change)
  Składowanie zmienionego zapytania za pomocą programu licencjonowanego Query/400

- Operacje, które nie są kontrolowane

  Kopiowanie (Copy)
  Skopiuj zapytanie używając opcji 3 ekranu “Praca z zapytaniami”

  Tworzenie (Create)
  Stwórz zapytanie używając opcji 1 ekranu “Praca z zapytaniami”

  Usunięcie (Delete)
  Usuń zapytanie używając opcji 4 ekranu “Praca z zapytaniami”

  Uruchamianie (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 na tabelach konwersji kodów odniesienia (*RCT)

Poniżej znajduje sie lista działań, które można wykonać na tabelach konwersji kodów odniesienia (*RCT) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Brak
- Operacja zmiany

  Brak
- Operacje, które nie są kontrolowane

  Brak

Operacje na liście odpowiedzi

Poniżej znajduje się lista działań, które można wykonać na liście odpowiedzi oraz informacje, które z tych operacji są kontrolowane.

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.

- Operacje kontrolowane

  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 na opisach podsystemu (*SBSD)

Poniżej znajduje sie lista działań, które można wykonać na opisach podsystemu (*SBSD) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  ENDSBS
  Zakończenie pracy podsystemu (End Subsystem)

  STRSBS
  Uruchomienie podsystemu (Start Subsystem)
- Operacja zmiany

  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 na indeksie wyszukiwania informacji (*SCHIDX)

Poniżej znajduje się lista działań, które można wykonać na indeksie wyszukiwania informacji(*SCHIDX) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  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 na gnieździe lokalnym (*SOCKET)

Poniżej znajduje się lista działań, które można wykonać na gnieździe lokalnym (*SOCKET) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  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)

- Operacja zmiany

  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

  dowiązanie
  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

odczyt 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

zapis Funkcja API Write to File

writev Funkcja API Write to File (Vector)

Operacje na słowniku sprawdzania pisowni (*SPADCT)

Poniżej znajduje się lista działań, które można wykonać na słowniku sprawdzania pisowni (*SPADCT) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Weryfikowanie (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)
  Wykorzystanie słownika jako podstawy przy tworzeniu nowego słownika.

  Weryfikowanie (Verify)
  Wykorzystanie słownika do sprawdzania podczas tworzenia nowego słownika.

  Odtwarzanie (Retrieve)
  Odtwarzanie źródła listy słów zatrzymania (Retrieve Stop Word List Source)

  Drukowanie (Print)
  Drukowanie listy słów zatrzymania (Print Stop Word List Source)

- Operacja zmiany

  CRTSPADCT
  Tworzenie słownika pisowni (Create Spelling Aid Dictionary) za pomocą opcji REPLACE(*YES)

- Operacje, które nie są kontrolowane

Brak

Operacje na plikach buforowych

Poniżej znajduje sie lista działań, które można wykonać na plikach buforowych oraz informacje, które z tych operacji są kontrolowane.

Uwaga: Działania na zbiorach buforowych są kontrolowane, jeśli wartość systemowa kontroli działania (QAUDLVL) lub parametr kontroli działania (AUDLVL) w profilu użytkownika zawiera wartość *SPLFDTA.

- Operacje kontrolowane

  Dostęp (Access)
  Każdy dostęp przez użytkownika, który nie jest właścicielem zbioru buforowego, w tym:
  - CPYSPLF,
  - DSPSPLF,
  - SNDNETSPLF,
  - SNDTCPSPLF,
  - STRRMTWTR,
  - funkcja API QSPOPNSP.

  Zmiana (Change)
  Zmiana dowolnego z wymienionych atrybutów zbioru buforowego za pomocą komendy CHGSPLFA:
  - COPIES,
  - DEV,
  - FORMTYPE,
  - RESTART,
  - PAGERANGE.
  - OUTQ
  - DRAWER
  - PAGDFN
  - FORMDF
  - USRDFNOPT
  - USRDFNOBJ
  - USRDFNDTA
  - EXPDATE
  - SAVE

  Zmiana dowolnego innego atrybutu zbioru buforowego za pomocą komendy CHGSPLFA:

  Tworzenie (Create)
  Tworzenie zbioru buforowego za pomocą operacji drukowania

  Tworzenie zbioru buforowego za pomocą funkcji API QSPCRTSP

  Usunięcie (Delete)
  Usunięcie zbioru buforowego za pomocą dowolnej z wymienionych operacji:
  - 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.
– Usunięcie zbiorów buforowych, które utraciły ważność, za pomocą komendy DLTEXPSPLF
– Usunięcie zbiorów buforowych za pomocą wspomagającej funkcji czyszczenia.

Wstrzymanie (Hold)
Wstrzymanie zbioru buforowego za pomocą dowolnej z wymienionych operacji:
– 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.

Odczyt (Read)
Odczytywanie zbioru buforowego przez drukarkę lub program piszący dyskietek.

Zwalnianie (Release)
Zwalnianie zbioru buforowego

Odtwarzanie (Restore)
Odtwarzanie zbioru buforowego

Składowanie (Save)
Składowanie zbioru buforowego

Operacje na pakiecie SQL (*SQLPKG)

Poniżej znajduje sie lista działań, które można wykonać na pakiecie SQL (*SQLPKG) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Uruchamianie (Run)
  Gdy obiekt *SQLPKG jest uruchomiony

- Operacja zmiany

  Brak

- Operacje, które nie są kontrolowane

  PRTSQLINF
  Drukowanie informacji SQL (Print SQL Information)

Operacje na programie usługowym (*SRVPGM)

Poniżej znajduje sie lista działań, które można wykonać na programie usługowym (*SRVPGM) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  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 konsolid.

UPDPGM
Pozycja kontroli dla każdego programu usługowego używanego podczas wykonywania komendy UPDPGM

UPDSRVPGM
Pozycja kontroli dla każdego programu usługowego używanego podczas wykonywania komendy UPDSRVPGM

- Operacja tworzenia

CRTSRVPGM
Tworzenie programu usługowego (Create Service Program)

UPDSRVPGM
Aktualizacja programu usługowego (Update Service Program)

- Operacja zmiany

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 na opisach sesji (*SSND)

Poniżej znajduje sie lista działań, które można wykonać na opisach sesji (*SSND) oraz informacje, które z tych operacji są kontrolowane.

Dla obiektów typu *SSND operacje odczytu lub zmiany nie są kontrolowane.

Operacje na przestrzeni pamięci serwera (*SVRSTG)

Poniżej znajduje się lista działań, które można wykonać na przestrzeni pamięci serwera (*SVRSTG) oraz informacje, które z tych operacji są kontrolowane.

Dla obiektu typu *SVRSTG operacje odczytu lub zmiany nie są kontrolowane.

Operacje na pliku strumieniowym (*STMF)

Poniżej znajduje się lista działań, które można wykonać na pliku strumieniowym (*STMF) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

CPY Kopiowanie obiektu (Copy Object)

DSPLNK
Wyświetlenie dowiązań obiektów

givedescriptor
Funkcja API Give File Access

MOV Przeniesienie obiektu (Move Object)

open, open64, QlgOpen, QlgOpen64, Qp0lOpen
Funkcje API Open File

SAV Składowanie obiektu (Save Object)

WRKLNK
Praca z dowiązaniami obiektów

- Operacja zmiany

ADDLNK
Dodanie dowiązania (Add Link)

CHGAUD
Zmiana kontroli (Change Auditing)

CHGAUT
Zmiana uprawnień (Change Authority)

CHGOWN
Zmiana właściciela (Change Owner)

CHGPGP
Zmiana grupy podstawowej (Change Primary Group)

CHKIN
Zwrócenie obiektu

CHKOUT
Pobranie obiektu

chmod, QlgChmod
Funkcje API Change File Authorizations

chown, QlgChown
Funkcje API Change Owner and Group

CPY Kopiowanie obiektu (Copy Object)

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

dowiązanie
Funkcja API Create Link to File

MOV Przeniesienie obiektu (Move Object)

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
Zmiana nazwy zbioru lub katalogu, zachowanie nowych API

Qp0lRenameUnlink, QlgRenameUnlink
Zmiana nazwy pliku lub katalogu, usunięcie dowiązań nowych API

RMVLNK
Usuwanie dowiązania (Remove Link)

RNM Zmiana nazwy obiektu (Rename Object)

RST Odtworzenie obiektu (Restore Object)

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

odczyt 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

zapis Funkcja API Write to File

writev Funkcja API Write to File (Vector)

Operacje na dowiązaniach symbolicznych (*SYMLNK)

Poniżej znajduje się lista działań, które można wykonać na obiektach dowiązańsymbolicznych (*SYMLNK) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  CPY Kopiowanie obiektu (Copy Object)

  DSPLNK
  Wyświetlenie dowiązań obiektów

  MOV Przeniesienie obiektu (Move Object)

  readlink
  Funkcja API Read Value of Symbolic Link

  SAV Składowanie obiektu (Save Object)

  WRKLNK
  Praca z dowiązaniami obiektów

- Operacja zmiany

  CHGOWN
  Zmiana właściciela (Change Owner)

  CHGPGP
  Zmiana grupy podstawowej (Change Primary Group)

  CPY Kopiowanie obiektu (Copy Object)

  MOV Przeniesienie obiektu (Move Object)

  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 obiektu (Rename Object)

  RST Odtworzenie obiektu (Restore Object)

symlink, QlgSymlink
Funkcje API Make Symbolic Link

unlink, QlgUnlink
Funkcje API Remove Link to File

WRKLNK
Praca z dowiązaniami obiektów

- Operacje, które nie są kontrolowane

lstat, lstat64, QlgLstat, QlgLstat64
Funkcje API Link Status

Operacje na opisach maszyny S/36(*S36)

Poniżej znajduje sie lista działań, które można wykonać na opisach maszyny S/36 (*S36) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

Brak

- Operacja zmiany

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 na tabelach (*TBL)

Poniżej znajduje sie lista działań, które można wykonać na tabelach (*TBL) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

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

Odczyt (Read)
Tabeli kolejności sortowania należy używać podczas uruchamiania dowolnej komendy, która może określić kolejność sortowania

- Operacja zmiany

  Brak

- Operacje, które nie są kontrolowane

  WRKTBL
  Praca z tabelami (Work with tables)

Operacje na indeksach użytkownika (*USRIDX)

Poniżej znajduje się lista działań, które można wykonać na indeksach użytkownika (*USRIDX) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  QUSRTVUI
  Funkcja API Retrieve user index entries

- Operacja zmiany

  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 na profilach użytkownika(*USRPRF)

Poniżej znajduje się lista działań, które można wykonać na profilach użytokwnika (*USRPRF) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  RCLOBJOWN
  Odzyskiwanie obiektów przez właściciela

- Operacja zmiany

  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 na kolejce użytkowników (*USRQ)

Poniżej znajduje sie lista działań, które można wykonać na kolejce użytkowników (*USRQ) oraz informacje, które z tych operacji są kontrolowane.

- 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 na przestrzeni użytkowników (*USRSPC)

Poniżej znajduje się lista działań, które można wykonać na przestrzeni użytkowników (*USRSPC) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  QUSRTVUS
  Funkcja API Retrieve User Space

- Operacja zmiany

  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 na liście sprawdzania (*VLDL)

Poniżej znajduje się lista działań, które można wykonać na liście sprawdzania (*VLDL) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  QSYFDVLE
  Funkcja API Find Validation List Entry

- Operacja zmiany

  QSYADVLE
  Funkcja API Add Validation List Entry

  QSYCHVLE
  Funkcja API Change Validation List Entry

  QSYRMVLE
  Funkcja API Remove Validation List Entry

Operacje na obiektach dostosowania stacji roboczej (*WSCST)

Poniżej znajduje sie lista działań, które można wykonać na obiektach dostosowania stacji roboczej (*WSCST) oraz informacje, które z tych operacji są kontrolowane.

- Operacja odczytu

  Aktywowanie (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

- Operacja zmiany

  Brak

- Operacje, które nie są kontrolowane

  Brak

Dodatek F. Układ pozycji kroniki kontroli

Ta sekcja 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.

Opisane w tym dodatku układy pozycji kroniki przypominają sposób definiowania zbioru fizycznego za pomocą języka DDS. Na przykład zgodnie z definicją, w układzie binarnym (4) można przechowywać informacje liczące od 1 do 4 cyfr wymagające składowania dwubajtowego, podczas gdy w układzie binarnym (5) można przechowywać informacje liczące od 1 do 5 cyfr, co wymaga 4 bajtów. Definicje te są wykorzystywane i egzekwowane przez takie języki, jak język RPG. System zapisuje w kronice kontroli dodatkowe pozycje, dla zdarzeń takich jak IPL systemu lub składowanie dziennika. Układy dla tych typów pozycji są opisane w sekcji Zarządzanie kroniką.

"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585 zawiera rozmieszczenie pól, które są wspólne dla wszystkich typów pozycji, gdy dla komendy DSPJRN podano parametr OUTFILFMT(*TYPE2). Taki układ, o nazwie QJORDJE2, zdefiniowany jest w zbiorze QADSPJR2 w bibliotece QSYS.

"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 zawiera rozmieszczenie pól, które są wspólne dla wszystkich typów pozycji, gdy dla komendy DSPJRN podano parametr OUTFILFMT(*TYPE4). Taki układ, o nazwie 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.

Uwaga: Ponieważ formaty wyjściowe TYPE2 i *TYPE4 nie są już aktualizowane, więc zaleca się zaprzestanie korzystania z formatów *TYPE2 i *TYPE4 i używanie tylko formatów *TYPE5.

"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" zawiera rozmieszczenie pól, które są wspólne dla wszystkich typów pozycji, gdy dla komendy DSPJRN podano parametr OUTFILFMT(*TYPE5). Taki układ, o nazwie QJORDJE5, zdefiniowany jest w zbiorze QADSPJR5 w bibliotece QSYS. Format wyjściowy *TYPE5 obejmuje wszystkie informacje formatu *TYPE4, wraz z informacjami dotyczącymi biblioteki programu, nazwy urządzenia ASP, numeru urządzenia ASP, dziennika, biblioteki dziennika, nazwy urządzenia ASP dziennika, numeru urządzenia ASP dziennika, numeru ramienia, ID wątku, rodziny adresów, portu zdalnego i adresu zdalnego.

Tabele od "Pozycje kroniki AD (Auditing Change - zmiana kontroli)" na stronie 588 do "Pozycje kroniki ZR (Odczyt obiektu)" na stronie 729 prezentują układy dla modelowych zbiorów wyjściowych bazy danych udostępniane w celu definiowania danych wejściowych. Za pomocą komendy CRTDUPOBJ można utworzyć 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 zapytania lub programu" na stronie 306 udostępnia przykłady używania modelowych zbiorów wyjściowych bazy danych. Można także zapoznać się z tematem Zarządzanie kroniką.

Uwaga: Te tabele pozycji kroniki czasami zawierają pustą kolumnę pod kolumną przesunięcia, JE lub J4. Oznacza to, że nie istnieje modelowy zbiór wyjściowy dla danego typu kroniki kontroli.

Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)

Niniejsza tabela zawiera wszystkie dopuszczalne wartości pól, które są wspólne dla wszystkich typów pozycji, gdy przy komendzie DSPJRN określono parametr OUTFILFMT(*TYPE5).

Tabela 156. Standardowe pola nagłówków 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)	Stosowane do każdej pozycji kroniki. Początkowa wartość w każdej nowej lub odtworzonej kronice wynosi 1. Opcjonalnie resetowana do 1, gdy podłączany jest nowy dziennik.
26	Kod kroniki	Char(1)	Zawsze T.
27	Typ pozycji	Char(2)	Listę typów pozycji oraz opisy zawiera “Typy pozycji kroniki kontroli (Audit Journal - QAUDJRN)” na stronie 586.
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.
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. Pole posiada 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	Liczba/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. Nieużywana 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)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
215	Ograniczenie referencyjne	Char(1)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
216	Wyzwalacz	Char(1)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
217	Dane niepełne	Char(1)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
218	Ignorowanie przez APY/ RMVJRNCHG	Char(1)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.

Tabela 156. Standardowe pola nagłówków pozycji kroniki kontroli (kontynuacja). Format rekordu QJORDJE5 (*TYPE5)

Pozycja (Offset)	Pole	Format	Opis
219	Zminimalizowane ESD	Char(1)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
220	Indykator obiektu	Char(1)	Używana dla obiektów kronikowanych. Nieużywana 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 zawierającej dziennik, w którym znajduje się pozycja kroniki.
261	Urządzenie ASP dziennika	Char(10)	Nazwa urządzenia puli ASP, w której przechowywany jest dziennik.
271	Numer ASP dziennika	Zoned(5,0)	Numer urządzenia ASP zawierającego dziennik, w którym znajduje się pozycja 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 dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
396	ID transakcji	Char(140)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
536	Zastrzeżone	Char(20)	Używana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
556	Indykatory wartości pustej (Null)	Char(50)	Używana dla obiektów kronikowanych. Nieużywana 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 wymiany profili użytkownika użyto funkcji API, pole nazwy profilu użytkownika będzie zawierać nazwę nowego (wymienionego) profilu.

Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)

Niniejsza tabela zawiera wszystkie dopuszczalne wartości pól, które są wspólne dla wszystkich typów pozycji, gdy przy komendzie OUTFILFMT określono parametr (*TYPE4).

Tabela 157. Standardowe pola nagłówków 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)	Stosowane do każdej pozycji kroniki. Początkowa wartość w każdej nowej lub odtworzonej kronice wynosi 1. Opcjonalnie resetowana do 1, gdy podłączany jest nowy dziennik.
16	Kod kroniki	Char(1)	Zawsze T.
17	Typ pozycji	Char(2)	Listę typów pozycji oraz opisy zawiera “Typy pozycji kroniki kontroli (Audit Journal - QAUDJRN)” na stronie 586.
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. Pole 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)	Wykorzystywana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
91	Nazwa biblioteki	Char(10)	Wykorzystywana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
101	Nazwa podzbioru	Char(10)	Wykorzystywana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
111	Liczba/RRN	Zoned(10)	Wykorzystywana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
121	Flaga	Char(1)	Wykorzystywana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
122	Identyfikator cyklu zatwierdzania	Zoned(10)	Wykorzystywana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
132	Profil użytkownika	Char(10)	Nazwa bieżącego profilu użytkownika[1].
142	Nazwa systemu	Char(8)	Nazwa systemu.
150	Identyfikator kroniki	Char(10)	Wykorzystywana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
160	Ograniczenie referencyjne	Char(1)	Wykorzystywana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
161	Wyzwalacz	Char(1)	Wykorzystywana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
162	(Obszar zastrzeżony)	Char(8)	
170	Indykatory wartości pustej (Null)	Char(50)	Wykorzystywana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
220	Długość danych pozycji	Binary (4)	Długość danych pozycji.

Tabela 157. Standardowe pola nagłówków pozycji kroniki kontroli (kontynuacja). Format rekordu QJORDJE4 (*TYPE4)

Pozycja (Offset)	Pole	Format	Opis
	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 wymiany profili użytkownika użyto funkcji API, pole nazwy profilu użytkownika będzie zawierać nazwę nowego (wymienionego) profilu.		

Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)

Niniejsza tabela zawiera wszystkie dopuszczalne wartości pól, które są wspólne dla wszystkich typów pozycji, gdy przy komendzie DSPJRN określono parametr OUTFILFMT(*TYPE2).

Tabela 158. Standardowe pola nagłówków 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)	Stosowane do każdej pozycji kroniki. Początkowa wartość w każdej nowej lub odtworzonej kronice wynosi 1. Opcjonalnie resetowana do 1, gdy podłączany jest nowy dziennik.
16	Kod kroniki	Char(1)	Zawsze T.
17	Typ pozycji	Char(2)	Listę typów pozycji oraz opisy zawiera “Typy pozycji kroniki kontroli (Audit Journal - QAUDJRN)” na stronie 586.
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. Pole ma wartość *NONE, gdy spełniony jest jeden z poniższych warunków: • nazwa programu nie odnosi się do tego typu pozycji, • nazwa programu nie jest dostępna.
67	Nazwa obiektu	Char(10)	Wykorzystywana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
77	Nazwa biblioteki	Char(10)	Wykorzystywana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
87	Nazwa podzbioru	Char(10)	Wykorzystywana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
97	Liczba/RRN	Zoned(10)	Wykorzystywana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.

Tabela 158. Standardowe pola nagłówków pozycji kroniki kontroli (kontynuacja). Format rekordu QJORDJE2 (*TYPE2)

Pozycja (Offset)	Pole	Format	Opis
107	Flaga	Char(1)	Wykorzystywana dla obiektów kronikowanych. Nieużywana dla pozycji kroniki kontroli.
108	Identyfikator cyklu zatwierdzania	Zoned(10)	Wykorzystywana dla obiektów kronikowanych. Nieużywana 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 wymiany profili użytkownika użyto funkcji API, pole *Nazwa profilu użytkownika* będzie zawierać nazwę nowego (wymienionego) profilu.

Typy pozycji kroniki kontroli (Audit Journal - QAUDJRN)

Niniejsza tabela zawiera wszystkie dostępne typy pozycji kroniki kontroli.

Tabela 159. Typy pozycji kroniki kontroli (Audit Journal - 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
IM	Wykrywanie włamań
IP	Komunikacja między procesami

Tabela 159. Typy pozycji kroniki kontroli (Audit Journal - QAUDJRN) (kontynuacja)

Typ pozycji	Opis
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
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

Tabela 159. Typy pozycji kroniki kontroli (Audit Journal - QAUDJRN) (kontynuacja)

Typ pozycji	Opis
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
X1	Token identyfikacyjny
XD	Rozszerzenie serwera katalogów
YC	Dostęp do obiektu DLO (zmiana)
YR	Dostęp do obiektu DLO (odczyt)
ZC	Dostęp do obiektu (zmiana)
ZR	Dostęp do obiektu (odczyt)

Pozycje kroniki AD (Auditing Change - zmiana kontroli)

Niniejsza tabela opisuje format pozycji kroniki AD (Auditing Change - zmiana kontroli)

Tabela 160. Pozycje kroniki AD (Auditing Change - zmiana kontroli). Zbiór opisów pól QASYADJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	J4	J5			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
156	224	610	Typ pozycji	Char(1)	**D** Komenda CHGDLOAUD **O** Komenda CHGOBJAUD lub 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.

Tabela 160. Pozycje kroniki AD (Auditing Change - zmiana kontroli) (kontynuacja). Zbiór opisów pól QASYADJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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.
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	CHGUSRAUD *AUTFAIL	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik wywoła niepowodzenie autoryzacji.
		663	CHGUSRAUD *JOBBAS	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik wykona podstawową funkcję zadania.
		664	CHGUSRAUD *JOBCHGUSR	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik zmieni aktywny profil użytkownika dla wątku lub jego zbiór grupy.
		665	CHGUSRAUD *NETBAS	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik wykona podstawową funkcję sieci.
		666	CHGUSRAUD *NETCLU	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik wykona funkcje klastra lub grupy zasobów klastra.
		667	CHGUSRAUD *NETCMN	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik wykona funkcję komunikacji sieciowej.
		668	CHGUSRAUD *NETFAIL	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik wywoła niepowodzenie sieci.
		669	CHGUSRAUD *NETSCK	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik wykona zadania gniazda.

Tabela 160. Pozycje kroniki AD (Auditing Change - zmiana kontroli) (kontynuacja). Zbiór opisów pól QASYADJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
		670	CHGUSRAUD *PGMFAIL	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik wywoła niepowodzenie programu.
		671	CHGUSRAUD *PRTDTA	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik wykona funkcję drukowania z parametrem SPOOL(*NO).
		672	CHGUSRAUD *SECCFG	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik wykona konfigurację bezpieczeństwa.
		673	CHGUSRAUD *SECDIRSRV	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik dokona zmian lub aktualizacji przy pomocy funkcji usług katalogowych.
		674	CHGUSRAUD *SECIPC	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik dokona zmian w komunikacji międzyprocesowej.
		675	CHGUSRAUD *SECNAS	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik wykona akcje usługi uwierzytelniania sieciowego.
		676	CHGUSRAUD *SECRUN	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik wykona funkcje wykonawcze bezpieczeństwa.
		677	CHGUSRAUD *SECSCKD	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik wykona funkcje deskryptora gniadza.
		678	CHGUSRAUD *SECVFY	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik skorzysta z funkcji weryfikacji.
		679	CHGUSRAUD *SECVLDL	Char(1)	Y = Zapisz rekord kontroli, gdy ten użytkownik manipuluje listami sprawdzania.
		680	(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]	Binarne(4)	Długość nazwy obiektu.
330	398	784	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	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)	

Tabela 160. Pozycje kroniki AD (Auditing Change - zmiana kontroli) (kontynuacja). Zbiór opisów pól QASYADJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
342	410	796	Identyfikator pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
358	426	812	ID zbioru obiektu[1,2]	Char(16)	Identyfikator zbioru dla obiektu.
374	442	828	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	954	1340	ID zbioru obiektu[1]	Char(16)	Identyfikator zbioru dla obiektu.
	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[1]	Binary(5)	Identyfikator kodowanego zestawu znaków dla nazwy ścieżki.
	989	1375	Identyfikator kraju lub regionu nazwy ścieżki[1]	Char(2)	Identyfikator kraju lub regionu nazwy ścieżki.
	991	1377	Identyfikator języka nazwy ścieżki[1]	Char(3)	Identyfikator języka dla nazwy ścieżki.
	994	1380	Długość nazwy ścieżki[1]	Binary(4)	Długość nazwy ścieżki.
	996	1382	Indykator nazwy ścieżki[1]	Char(1)	Indykator nazwy ścieżki: **Y** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	997	1383	Identyfikator zbioru katalogu względnego[1, 3]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[3]
	1013	1399	Nazwa ścieżki[1, 4]	Char(5002)	Nazwa ścieżki obiektu.

[1] Niniejsze pola są używane wyłącznie dla obiektów w katalogu ″root″(/), systemie plików QOpenSys lub systemach plików użytkownika.

[2] Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

[3] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

[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 puli ASP obiektu.

Pozycje kroniki AF (Authority Failure - błąd uprawnień)

Niniejsza tabela opisuje format pozycji kroniki AF (Authority Failure - błąd uprawnień)

Tabela 161. Pozycje kroniki AF (Authority Failure - błąd uprawnień). Zbiór opisów pól QASYAFJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.

Tabela 161. Pozycje kroniki AF (Authority Failure - błąd uprawnień) (kontynuacja). Zbiór opisów pól QASYAFJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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 **K** Naruszenie uprawnień specjalnych **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, 12, 17]	Char(10)	Nazwa obiektu.
167	235	621	Nazwa biblioteki[13]	Char(10)	Nazwa biblioteki, w której składowany jest obiekt, lub numer licencjonowanej poprawki kodu wewnętrznego, której instalacja nie powiodła się.[11]
177	245	631	Typ obiektu[14, 17]	Char(8)	Typ obiektu.

Tabela 161. Pozycje kroniki AF (Authority Failure - błąd uprawnień) (kontynuacja). Zbiór opisów pól QASYAFJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
185	253	639	Działanie błędu sprawdzania	Char(1)	Działanie podjęte po wykryciu błędu sprawdzania, 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 został zapisany w formacie i5/OS. **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** Program obsługi wyjścia skanowania zmodyfikował skanowany obiekt **X** Program obsługi wyjścia skanowania żądał obiektu oznaczonego jako mającego błąd podczas skanowania

Tabela 161. Pozycje kroniki AF (Authority Failure - błąd uprawnień) (kontynuacja). Zbiór opisów pól QASYAFJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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.
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. **AAC** Brak uprawnień do komendy Zaawansowana analiza SST (SST Advanced Analysis). **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[15, 16]	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]	Binarne(4)	Długość nazwy obiektu.

Tabela 161. Pozycje kroniki AF (Authority Failure - błąd uprawnień) (kontynuacja). Zbiór opisów pól QASYAFJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
395	463	849	Identyfikator CCSID nazwy obiektu[3]	Binary(5)	Identyfikator kodowanego zestawu znaków nazwy obiektu
399	467	853	Identyfikator kraju lub regionu nazwy obiektu[3]	Char(2)	Identyfikator kraju lub regionu 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	ID zbioru obiektu[3,4]	Char(16)	Identyfikator zbioru dla obiektu.
439	507	893	Nazwa obiektu[3,6]	Char(512)	Nazwa obiektu.
	1019	1405	ID zbioru obiektu[3]	Char(16)	Identyfikator zbioru dla 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[3]	Binary(5)	Identyfikator kodowanego zestawu znaków nazwy ścieżki
	1054	1440	Identyfikator kraju lub regionu nazwy ścieżki[3]	Char(2)	Identyfikator kraju lub regionu nazwy ścieżki.
	1056	1442	Identyfikator języka nazwy ścieżki[3]	Char(3)	Identyfikator języka dla nazwy ścieżki.
	1059	1445	Długość nazwy ścieżki[3]	Binarne(4)	Długość nazwy ścieżki.
	1061	1447	Indykator nazwy ścieżki[3]	Char(1)	Indykator nazwy ścieżki: **Y** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwa ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	1062	1448	Identyfikator zbioru w katalogu względnym[3, 8]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie, pole zawiera zera heksadecymalne.[8]

Tabela 161. Pozycje kroniki AF (Authority Failure - błąd uprawnień) (kontynuacja). Zbiór opisów pól QASYAFJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1078	1464	Nazwa ścieżki[3, 9]	Char(5002)	Nazwa ścieżki 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

[1] Jeśli typ naruszenia dotyczy opisu G, nazwa obiektu zawiera nazwę *SRVPGM, który zawierał wyjście wykrywające błąd. Więcej informacji na temat rodzajów naruszeń zawiera “Pozycje kroniki dotyczące kontroli bezpieczeństwa” na stronie 278.

[2] To pole zawiera nazwę użytkownika, który spowodował powstanie pozycji. QSYS może być użytkownikiem dla następujących pozycji:

- dla rekordów *TYPE2 pozycje 41 i 118,
- dla rekordów *TYPE4 pozycje 55 i 132,
- dla rekordów *TYPE5 pozycje 65 i 187.

[3] Te pola są używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanych przez użytkownika.

[4] Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

[5] Jeśli typ naruszenia dotyczy opisu G, nazwa obiektu zawiera port TCP/IP, do którego użytkownik nie posiada uprawnień. 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 zbioru obiektu będą puste.

[7] Tworzony obiekt klasy Java nie może rozszerzyć klasy bazowej, ponieważ klasa bazowa posiada atrybuty systemowe Java .

[8] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

[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 puli ASP obiektu.

[11] Gdy typ naruszenia wynosi X, a wartość kodu naruszenia operacji wynosi LIC, oznacza to błąd niezastosowania poprawki do Licencjonowanego Kod Wewnętrzny ze względu na naruszenie sygnatury. To pole zawiera numer poprawki do Licencjonowanego Kodu Wewnętrznego, której zastosowanie nie powiodło się.

[12] Jeśli typ naruszenia wynosi G, nazwa obiektu zawiera nazwę komendy lub programu, które wykryły błąd. Jeśli komenda ma kilka różnych nazw, to nazwa komendy w rekordzie kontroli może nie zgadzać się z dokładną użytą nazwą komendy, ale z jedną z jej alternatywnych nazw. Specjalna wartość *INSTR oznacza, że błąd został wykryty przez instrukcję maszynową.

[13] Jeśli typ naruszenia wynosi K, nazwa biblioteki zawiera nazwę biblioteki programu lub *N biblioteki programu, które wykryły błąd.

[14] Jeśli typ naruszenia wynosi K, nazwa obiektu zawiera typ obiektu komendy lub programu, które wykryły błąd.

[15] Jeśli typ naruszenia wynosi K, ścieżka folderu może zawierać pełną nazwę API lub nazwę punktu wyjścia, które wykryły błąd.

Tabela 161. Pozycje kroniki AF (Authority Failure - błąd uprawnień) (kontynuacja). Zbiór opisów pól QASYAFJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	J4	J5			
[16]			Gdy typ naruszenia wynosi X, a wartość kodu naruszenia operacji wynosi AAC, ścieżka folderu będzie zawierać 30-znakową nazwę zaawansowanej komendy analizy.		
[17]			Jeśli typ obiektu to *LIC, a biblioteka obiektów to *N, nazwa obiektu będzie nazwąLicencjonowanego Kod Wewnętrznego Ru.		

Pozycje kroniki AP (Adopted Authority - uprawnienie adoptowane)

Niniejsza tabela opisuje format pozycji kroniki AP (Adopted Authority - uprawnienie adoptowane)

Tabela 162. Pozycje kroniki AP (Adopted Authority - uprawnienie adoptowane). Zbiór opisów pól QASYAPJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	J4	J5			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
156	224	610	Typ pozycji	Char(1)	**S** Uruchomienie (Start) **E** Zakończenie (End) **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.
195	263	649	ID zbioru obiektu	Char(16)	Identyfikator zbioru dla 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 puli ASP obiektu.		

Pozycje kroniki AU (Attribute Changes - zmiany atrybutów)

Niniejsza tabela opisuje format pozycji kroniki AU (Attribute Changes - zmiany atrybutów)

Tabela 163. Pozycje kroniki AU (Attribute Changes - zmiany atrybutów). 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	Nowa długość wartości	Binarne(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	Binarne(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.			

Pozycje kroniki CA (Authority Changes - zmiana uprawnień)

Niniejsza tabela opisuje format pozycji kroniki CA (Authority Changes - zmiana uprawnień)

Tabela 164. Pozycje kroniki CA (Authority Changes - zmiana uprawnień). Zbiór opisów pól QASYCAJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.

Tabela 164. Pozycje kroniki CA (Authority Changes - zmiana uprawnień) (kontynuacja). Zbiór opisów pól QASYCAJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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 składowany jest 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 (Grant) **RPL** Nadanie z zastąpieniem **RVK** Odwołanie (Revoke) **USR** Operacja GRTUSRAUT

Tabela 164. Pozycje kroniki CA (Authority Changes - zmiana uprawnień) (kontynuacja). Zbiór opisów pól QASYCAJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
225	293	679	Nazwa pola	Char(10)	Nazwa pola.
235	303		(Obszar zastrzeżony)	Char(10)	
		689	Atrybut obiektu	Char(10)	Atrybut obiektu.
245	313	699	Użytkownik biurowy	Char(10)	Nazwa użytkownika biurowego.
255	323	709	Nazwa DLO	Char(12)	Nazwa DLO.
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]	Binarne(4)	Długość nazwy obiektu.
374	442	828	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	Identyfikator kodowanego zestawu znaków nazwy obiektu
378	446	832	Identyfikator kraju lub regionu nazwy obiektu[1]	Char(2)	Identyfikator kraju lub regionu 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	ID zbioru obiektu[1,2]	Char(16)	Identyfikator zbioru dla obiektu.
418	486	872	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	998	1384	ID zbioru obiektu	Char(16)	Identyfikator zbioru dla obiektu.
	1014	1400	Nazwa puli ASP [5]	Char(10)	Nazwa urządzenia puli ASP.

Tabela 164. Pozycje kroniki CA (Authority Changes - zmiana uprawnień) (kontynuacja). Zbiór opisów pól QASYCAJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1024	1410	Numer puli ASP [5]	Char(5)	Numer urządzenia puli ASP.
	1029	1415	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków nazwy ścieżki
	1033	1419	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu nazwy ścieżki.
	1035	1421	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	1038	1424	Długość nazwy ścieżki	Binarne(4)	Długość nazwy ścieżki.
	1040	1426	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **Y** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwa ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	1041	1427	Identyfikator zbioru w katalogu względnym[3]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[3]
	1057	1443	Nazwa ścieżki[4]	Char(5002)	Nazwa ścieżki obiektu.

[1] Te pola są używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanych przez użytkownika.

[2] Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

[3] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

[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 puli ASP obiektu.

Pozycje kroniki CD (Command String - łańcuch komendy)

Niniejsza tabela opisuje format pozycji kroniki CD (Command String - łańcuch komendy)

Tabela 165. Pozycje kroniki CD (Command String - łańcuch komendy). Zbiór opisów pól QASYCDJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
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 składowany jest obiekt.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253	639	Uruchom z programu CL	Char(1)	**Y** Tak **N** Nie
186	254	640	Łańcuch komendy	Char(6000)	Komenda, która została uruchomiona, razem z parametrami.
		6640	Nazwa puli ASP biblioteki komendy	Char(10)	Nazwa puli ASP dla biblioteki komendy
		6650	Numer puli ASP biblioteki komendy	Char(5)	Numer puli ASP dla biblioteki komendy

Pozycje kroniki CO (Create Object - tworzenie obiektu)

Niniejsza tabela opisuje format pozycji kroniki CO (Create Object - tworzenie obiektu)

Tabela 166. Pozycje kroniki CO (Create Object - tworzenie obiektu). Zbiór opisów pól QASYCOJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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		(Obszar zastrzeżony)	Char(20)	
		639	Atrybut obiektu	Char(10)	Atrybut obiektu.
		649	(Obszar zastrzeżony)	Char(10)	
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	Binarne(4)	Długość nazwy obiektu.
328	396	782	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	Identyfikator kodowanego zestawu znaków nazwy obiektu
332	400	786	Identyfikator kraju lub regionu nazwy obiektu[1]	Char(2)	Identyfikator kraju lub regionu nazwy obiektu.
334	402	788	Identyfikator języka nazwy obiektu[1]	Char(3)	Identyfikator języka dla nazwy obiektu.
337	405	791	(Obszar zastrzeżony)	Char(3)	

Tabela 166. Pozycje kroniki CO (Create Object - tworzenie obiektu) (kontynuacja). Zbiór opisów pól QASYCOJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
340	408	794	Identyfikator pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
356	424	810	ID zbioru obiektu[1,2]	Char(16)	Identyfikator zbioru dla obiektu.
372	440	826	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	952	1338	ID zbioru obiektu	Char(16)	Identyfikator zbioru dla 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 nazwy ścieżki
	987	1373	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu nazwy ścieżki.
	989	1375	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	992	1378	Długość nazwy ścieżki	Binarne(4)	Długość nazwy ścieżki.
	994	1380	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **Y** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwa ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	995	1381	Identyfikator zbioru w katalogu względnym[3]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[3]
	1011	1397	Nazwa ścieżki[4]	Char(5002)	Nazwa ścieżki obiektu.

[1] Te pola są używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanych przez użytkownika.

[2] Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

[3] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

[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 puli ASP obiektu.

Pozycje kroniki CP (User Changes - zmiany użytkowników)

Niniejsza tabela opisuje format pozycji kroniki CP (User Changes - zmiany użytkowników)

Tabela 167. Pozycje kroniki CP (User Changes - zmiany użytkowników). Zbiór opisów pól QASYCPJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Zmiana w profilu użytkownika
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 wykonywanej 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** Uprawnienia specjalne *SECADM.

Tabela 167. Pozycje kroniki CP (User Changes - zmiany użytkowników) (kontynuacja). Zbiór opisów pól QASYCPJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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.
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 użytkownika.
493	561	947	Identyfikator grupy	Char(10)	GID użytkownika.

Tabela 167. Pozycje kroniki CP (User Changes - zmiany użytkowników) (kontynuacja). Zbiór opisów pól QASYCPJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
503	571	957	Zarządzanie hasłem lokalnym	Char(10)	Wartość parametru LCLPWDMGT.
		967	Zgodność kompozycji hasła	Char(10)	Określa, czy nowe hasło jest zgodne z zasadami kompozycji hasła. ***PASSED** Sprawdzone i zgodne. ***SYSVAL** Sprawdzone, ale niezgodne ze względu na regułę związaną z wartością systemową. ***EXITPGM** Sprawdzone, ale niezgodne ze względu na odpowiedź programu wyjściowego. ***NONE** Niesprawdzone; jako hasło określono *NONE. ***NOCHECK** Niesprawdzone; hasło zostało zmienione. Pole to ma znaczenie tylko w przypadku, gdy pole Zmieniono hasło zawiera wartość *Y*.
		977	Okres ważności hasła	Char (7)	Określa wartość, na jaką zmieniony został okres ważności hasła. ***NOMAX** Brak okresu ważności. ***SYSVAL** Używana jest wartość systemowa QPWDEXPITV. **numer** Okres ważności w dniach.
		984	Blokada zmiany hasła	Char(10)	Określa wartość, na jaką została zmieniona blokada zmiany hasła. ***SYSVAL** Wykorzystywana jest wartość systemowa QPWDCHGBLK. ***NONE** Brak okresu blokady. **1-99** Zablokowana liczba godzin.

Pozycje kroniki CQ (*CRQD - zmiany opisów CRQD)

Niniejsza tabela opisuje format pozycji kroniki CQ (*CRQD - zmiany opisów CRQD)

*Tabela 168. Pozycje kroniki CQ (*CRQD - zmiany opisów CRQD).* Zbiór opisów pól QASYCQJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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

Pozycje kroniki CU (Cluster Operations - operacje klastrów)

Niniejsza tabela opisuje format pozycji kroniki CU (Cluster Operations - operacje klastrów)

Tabela 169. Pozycje kroniki CU (Cluster Operations - operacje klastrów). Zbiór opisów pól QASYCUJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583.
	224	610	Typ pozycji	Char(1)	Typ pozycji. **M** Sterowanie klastrem **R** Zarządzanie grupą zasobów klastra (*GRP)

Tabela 169. Pozycje kroniki CU (Cluster Operations - operacje klastrów) (kontynuacja). Zbiór opisów pól QASYCUJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	225	611	Pozycja działania	Char(3)	Typ działania. **ADD** Dodanie (Add) **CRT** Tworzenie (Create) **DLT** Usunięcie (Delete) **DST** Dystrybucja **END** Zakończenie (End) **FLO** Przełączanie awaryjne **LST** Informacje o liście **RMV** Usuwanie (Remove) **STR** Uruchomienie (Start) **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.
		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

Pozycje kroniki CV (Connection Verification - weryfikacja połączenia)

Niniejsza tabela opisuje format pozycji kroniki CV (Connection Verification - weryfikacja połączenia)

Tabela 170. Pozycje kroniki CV (Connection Verification - weryfikacja połączenia). Zbiór opisów pól QASYCVJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583.
	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** Niepoprawne hasło. 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 połączenia punkt z punktem.
	236	622	Protokół	Char(10)	Typ pozycji. **L2TP** Protokół Layer Two Tunneling protocol (L2TP) **PPP** Protokół Point-to-Point protocol (PPP). **SLIP** Protokół Serial Line Internet Protocol.

Tabela 170. Pozycje kroniki CV (Connection Verification - weryfikacja połączenia) (kontynuacja). Zbiór opisów pól QASYCVJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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 170. Pozycje kroniki CV (Connection Verification - weryfikacja połączenia) (kontynuacja). Zbiór opisów pól QASYCVJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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	Binarne(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. Używane dla typu pozycji E lub R.
	637	1023	Zastrzeżone	Binarne(4)	Zawsze zerowe
		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

Pozycje kroniki CY (Konfigurowanie szyfrowania)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki CY (Konfigurowanie szyfrowania).

Tabela 171. Pozycje kroniki CY (Konfigurowanie szyfrowania). Zbiór opisów pól QASYCYJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.

Tabela 171. Pozycje kroniki CY (Konfigurowanie szyfrowania) (kontynuacja). Zbiór opisów pól QASYCYJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Funkcja kontroli dostępu koprocesora szyfrującego **F** Funkcja kontroli udogodnień koprocesora szyfrującego **K** Funkcja klucza głównego usług szyfrujących **M** Funkcja klucza głównego koprocesora szyfrującego
	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 lub czyszczenie FCV. **INI** Reinicjowanie karty. **LOD** Ładowanie klucza głównego. **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. **TST** Testowanie klucza głównego.
	228	614	Profil karty	Char(8)	Nazwa profilu karty.[2]
	236	622	Rola karty	Char(8)	Rola profilu karty.[2]
	244	630	Nazwa urządzenia	Char(10)	Nazwa urządzenia szyfrującego.[2]

Tabela 171. Pozycje kroniki CY (Konfigurowanie szyfrowania) (kontynuacja). Zbiór opisów pól QASYCYJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
		640	Identyfikator klucza głównego[1]	Binary(4)	Identyfikator klucza głównego usług szyfrujących[3]. Możliwe są następujące wartości: **-2** Składowanie/odtwarzanie klucza głównego **-1** Klucz główny ASP **1** Klucz główny 1 **2** Klucz główny 2 **3** Klucz główny 3 **4** Klucz główny 4 **5** Klucz główny 5 **6** Klucz główny 6 **7** Klucz główny 7 **8** Klucz główny 8
		644	Szyfrowanie klucza głównego	Char(1)	Klucz główny zaszyfrowany przy użyciu domyślnego klucza głównego składowania i odtwarzania. **T** Klucz główny został ustawiony i zaszyfrowany domyślnym kluczem głównym składowania i odtwarzania. **N** Klucz główny został ustawiony i zaszyfrowany kluczem głównym składowania i odtwarzania ustawionym przez użytkownika.
		645	Wersja klucza głównego	Char(8)	Wersja klucza głównego, którego zawartość została usunięta. **NOWA** Została usunięta zawartość nowej wersji. **BIEŻĄCA** Została usunięta zawartość bieżącej wersji. **STARA** Została usunięta zawartość starej wersji. **OCZEKUJĄCA** Została usunięta zawartość oczekującej wersji.

[1] Jeśli typem pozycji (J5 przesunięcie 610) jest K, to profil karty (J5 przesunięcie 614), rola karty (J5 przesunięcie 622) i nazwa urządzenia (J5 przesunięcie 630) ustawiane są na puste.

[2] Jeśli typem pozycji jest K, to pole jest puste.

[3] Jeśli typem pozycji jest K, to pole jest puste.

Pozycje kroniki DI (Serwer katalogów)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki DI (Serwer katalogów).

Tabela 172. Pozycje kroniki DI (Serwer katalogów). Zbiór opisów pól QASYDIJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
	224	610	Typ pozycji	Char(1)	Typ pozycji. **L** Operacja LDAP
	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. **CI** Tworzenie instancji **CO** Tworzenie obiektu. **CP** Zmiana hasła. **DI** Usunięcie instancji **DO** Usunięcie obiektu. **EX** Eksportowanie katalogu LDAP. **IM** Importowanie katalogu LDAP. **OM** Zarządzanie obiektem (zmiana nazwy). **OW** Zmiana prawa własności. **PO** Zmiana strategii. **PW** Awaria hasła. **RM** Zarządzanie replikacją **UB** Odłączanie powiodło się. **ZC** Zmiana obiektu. **ZR** Odczytanie obiektu.

Tabela 172. Pozycje kroniki DI (Serwer katalogów) (kontynuacja). Zbiór opisów pól QASYDIJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	227	613	Kod błędu uprawnień	Char(1)	Kod dla błędów uprawnień. Pole to wykorzystywane jest tylko wówczas, gdy typ operacji (J5 przesunięcie 611) 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 zaplecza, repliki, publikowanie). **G** Nieuprawniona próba zarządzania replikacją. **I** Nieuprawniona próba importu. **M** Nieuprawniona próba zmiany. **P** Nieuprawniona próba zmiany strategii. **R** Nieuprawniona próba odczytu (wyszukiwania). **U** Nieuprawniona próba odczytu konfiguracji kontroli. **X** Nieuprawniona próba autoryzacji proxy.
	228	614	Zmiana konfiguracji	Char(1)	Zmiany konfiguracji. Pole to wykorzystywane jest tylko wówczas, gdy typ operacji (J5 przesunięcie 611) to CF. **A** Zmiana ND administratora. **C** Włączenie lub wyłączenie protokołu zmian. **L** Zmiana nazwy biblioteki zaplecza. **P** Zmiana agenta publikacji. **R** Zmiana serwera replik. Jeśli typ operacji (J5 przesunięcie 611) to RM, wystąpić mogą następujące wartości: **U** Wstrzymanie replikacji. **V** Wznowienie replikacji. **W** Replikacja oczekujących zmian. **X** Pominięcie co najmniej jednej oczekującej zmiany. **Y** Wyciszenie kontekstu replikacji. **Z** Wyłączenie wyciszenia kontekstu replikacji.

Tabela 172. Pozycje kroniki DI (Serwer katalogów) (kontynuacja). Zbiór opisów pól QASYDIJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	229	615	Kod zmiany konfiguracji	Char(1)	Kod zmian konfiguracji. Pole to wykorzystywane jest tylko wówczas, gdy typ operacji (J5 przesunięcie 611) 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. Pole to wykorzystywane jest tylko wówczas, gdy typ operacji (J5 przesunięcie 611) to CA lub OW. **T** Prawda **F** Fałsz
	231	617	Wybór uwierzytelniania połączenia	Char(20)	Wybór uwierzytelniania połączenia. Pole to wykorzystywane jest tylko wówczas, gdy typ operacji (J5 przesunięcie 611) to BN.
	251	637	Wersja LDAP	Char(4)	Wersja klienta żądającego. Pole to wykorzystywane jest wyłącznie wówczas, gdy operacja została wykonana przez serwer 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. Pole to wykorzystywane jest wyłącznie wówczas, gdy operacja została wykonana przez serwer LDAP. **A** Uwierzytelnione **N** Anonimowe **U** Nieuwierzytelnione
	257	643	Identyfikator połączenia	Char(20)	Identyfikator połączenia żądania. Pole to wykorzystywane jest wyłącznie wówczas, gdy operacja została wykonana przez serwer LDAP.
	277	663	Adres IP klienta	Char(50)	Adres IP i numer portu klienta. Pole to wykorzystywane jest wyłącznie wówczas, gdy operacja została wykonana przez serwer 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.

Tabela 172. Pozycje kroniki DI (Serwer katalogów) (kontynuacja). Zbiór opisów pól QASYDIJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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.
	4343	4729	Identyfikator CCSID nazwy właściciela	Bin(5)	Identyfikator kodowanego zestawu znaków (CCSID) nazwy właściciela. Pole to wykorzystywane jest tylko wówczas, gdy typ operacji (J5 przesunięcie 611) 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. Pole to wykorzystywane jest tylko wówczas, gdy typ operacji (J5 przesunięcie 611) to OW.
	6351	6737	Identyfikator CCSID nowej nazwy	Bin(5)	Identyfikator kodowanego zestawu znaków (CCSID) nowej nazwy. Pole to wykorzystywane jest tylko wówczas, gdy typ operacji (J5 przesunięcie 611) to OM, OW, PO, ZC, AF+M, lub AF+P . • 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 operacji typu PO, ZC, AF+M lub AF+P, pole to zawierać będzie identyfikator CCSID listy zmienionych typów atrybutów w polu Nowa nazwa.
	6355	6741	Długość nowej nazwy	Bin(4)	Długość nowej nazwy. Pole to wykorzystywane jest tylko wówczas, gdy typ operacji (J5 przesunięcie 611) to OM, OW, PO, ZC, AF+M, lub AF+P . • 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 operacji typu PO, ZC, AF+M lub AF+P, pole to zawierać będzie długość listy zmienionych typów atrybutów w polu Nowa nazwa.
	6357	6743	Nowa nazwa[1]	Char(2002)	Nowa nazwa. Pole to wykorzystywane jest tylko wówczas, gdy typ operacji (J5 przesunięcie 611) to OM, OW, PO, ZC, AF+M lub AF+P. • Dla typu operacji OM, to pole będzie zawierało nową nazwę obiektu. • Dla typu operacji OW, to pole będzie zawierało nową nazwę właściciela. • Dla operacji typu PO, ZC, AF+M lub AF+P, pole to zawierać będzie listę zmienionych typów atrybutów.
	8359	8745	ID zbioru obiektu[2]	Char(16)	Identyfikator zbioru dla obiektu do eksportowania.
	8375	8761	Nazwa puli ASP[2]	Char(10)	Nazwa urządzenia puli ASP.

Tabela 172. Pozycje kroniki DI (Serwer katalogów) (kontynuacja). Zbiór opisów pól QASYDIJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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 nazwy ścieżki.
	8394	8780	Identyfikator kraju lub regionu nazwy ścieżki[2]	Char(2)	Identyfikator kraju lub regionu nazwy ścieżki.
	8396	8782	Identyfikator języka nazwy ścieżki[2]	Char(3)	Identyfikator języka nazwy ścieżki.
	8399	8785	Długość nazwy ścieżki[2]	Bin(4)	Długość nazwy ścieżki.
	8401	8787	Idndykator nazwy ścieżki[2]	Char(1)	Indykator nazwy ścieżki. **T** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	8402	8788	Identyfikator zbioru w katalogu względnym[2,3]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[3]
	8418	8804	Nazwa ścieżki[1,2]	Char(5002)	Nazwa ścieżki 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). **T** Użytkownik LDAP jest administratorem. **N** Użytkownik LDAP nie jest administratorem. **U** W tym momencie nie wiadomo, czy użytkownik LDAP jest administratorem.
		13817	Identyfikator CCSID identyfikatora proxy	Bin(5)	Identyfikator kodowanego zestawu znaków (CCSID) identyfikatora proxy.
		13821	Długość identyfikatora proxy	Bin(4)	Długość identyfikatora proxy.

Tabela 172. Pozycje kroniki DI (Serwer katalogów) (kontynuacja). Zbiór opisów pól QASYDIJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
		13823	Identyfikator proxy[1]	Char(2002)	Nazwa identyfikatora proxy. Pole to wykorzystywane jest wówczas, gdy kontrola autoryzacji proxy wykorzystywana jest do żądania wykonania operacji o uprawnieniach identyfikatora proxy, lub do powiązania SASL, w którym klient określił inny identyfikator autoryzowanego użytkownika różniący się od identyfikatora powiązania.
		15825	Asercja grupy	Char(1)	Asercja przypisania do grupy **0** Grupy nie zostały określone przez klienta. **1** Grupy zostały określone przez klienta.
		15826	Odniesienie	Char(36)	Łańcuch odniesienia użyty do korelacji tej pozycji z pozycją/pozycjami XD listingu grup.
		15862	Nazwa instancji	Char(8)	Nazwa instancji
		15870	Identyfikator CCSID trasy	Bin(5)	Identyfikator CCSID trasy
		15874	Długość trasy	Bin(4)	Długość trasy
		15876	Trasa	Char(502)	Trasa żądania

[1] Jest to pole o zmiennej długości. Pierwsze dwa bajty zawierają długość wartości znajdującej się w polu.

[2] Pola te wykorzystywane są tylko wówczas, gdy typ operacji (J5 przesunięcie 611) to EX lub IM.

[3] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

Pozycje kroniki DO (Operacja usunięcia)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki DO (Operacja usunięcia).

Tabela 173. Pozycje kroniki DO (Operacja usunięcia). Zbiór opisów pól QASYDOJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.

Tabela 173. Pozycje kroniki DO (Operacja usunięcia) (kontynuacja). Zbiór opisów pól QASYDOJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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 **I** Inicjowanie obszaru zmiennej środowiskowej **P** Oczekiwanie na usunięcie obiektu (usuwanie zostało przeprowadzone za pomocą kontroli transakcji) **R** Oczekujące usuwanie obiektu zostało wycofane
157	225	611	Nazwa obiektu	Char(10)	Nazwa obiektu.
167	235	621	Nazwa biblioteki	Char(10)	Nazwa biblioteki, w której składowany jest obiekt.
177	245	631	Typ obiektu	Char(8)	Typ obiektu.
185	253		(Obszar zastrzeżony)	Char(20)	
		639	Atrybut obiektu	Char(10)	Atrybut obiektu.
		649	(Obszar zastrzeżony)	Char(10)	
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 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.

Tabela 173. Pozycje kroniki DO (Operacja usunięcia) (kontynuacja). Zbiór opisów pól QASYDOJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
337	405	791	(Obszar zastrzeżony)	Char(3)	
340	408	794	Identyfikator pliku nadrzędnego[1,2]	Char(16)	Identyfikator pliku katalogu nadrzędnego.
356	424	810	ID zbioru obiektu[1,2]	Char(16)	Identyfikator zbioru dla obiektu.
372	440	826	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	952	1338	ID zbioru obiektu	Char(16)	Identyfikator zbioru dla 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 nazwy ścieżki.
	987	1373	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.
	989	1375	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	992	1378	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.
	994	1380	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	995	1381	Identyfikator zbioru w katalogu względnym[3]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[3]
	1011	1397	Nazwa ścieżki[4]	Char(5002)	Nazwa ścieżki obiektu.

Tabela 173. Pozycje kroniki DO (Operacja usunięcia) (kontynuacja). Zbiór opisów pól QASYDOJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
[1]			Te pola są używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanych przez użytkownika.		
[2]			Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.		
[3]			Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.		
[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 puli ASP obiektu.		

Pozycje kroniki DS (Resetowanie identyfikatora użytkownika narzędzi serwisowych IBM)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki DS (Resetowanie identyfikatora użytkownika narzędzi serwisowych IBM).

Tabela 174. Pozycje kroniki DS (Resetowanie identyfikatora użytkownika narzędzi serwisowych IBM). Zbiór opisów pól QASYDSJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Resetowanie hasła identyfikatora użytkownika narzędzi serwisowych. **C** Zmiana identyfikatora użytkownika narzędzi serwisowych. **P** Hasło identyfikatora użytkownika narzędzi serwisowych zostało zmienione.
157	225	611	Resetowanie identyfikatora użytkownika IBM narzędzi SST	Char(1)	**T** 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 174. Pozycje kroniki DS (Resetowanie identyfikatora użytkownika narzędzi serwisowych IBM) (kontynuacja). Zbiór opisów pól QASYDSJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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 serwisowych. **T** Żądanie zmiany hasła identyfikatora użytkownika narzędzi serwisowych.
	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.

Pozycje kroniki EV (Zmienna środowiskowa)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki EV (Zmienna środowiskowa).

Tabela 175. Pozycje kroniki EV (Zmienna środowiskowa). Zbiór opisów pól QASYEVJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Dodanie (Add) **C** Zmiana (Change) **D** Usunięcie (Delete) **I** Inicjowanie obszaru zmiennej środowiskowej

Tabela 175. Pozycje kroniki EV (Zmienna środowiskowa) (kontynuacja). Zbiór opisów pól QASYEVJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	225	611	Obcięta nazwa	Char(1)	Określa, czy nazwa zmiennej środowiskowej (przesunięcie 232) jest obcięta. **T** 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.
	1234	1620	Nowa obcięta nazwa[1]	Char(1)	Określa, czy nazwa nowej zmiennej środowiskowej (przesunięcie 1241) jest obcięta. **T** Wartość zmiennej środowiskowej jest obcięta. **N** Wartość zmiennej środowiskowej nie jest obcięta.
	1235	1621	Identyfikator CCSID nowej nazwy zmiennej środowiskowej[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.

Pozycje kroniki GR (Rekord ogólny)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki GR (Rekord ogólny).

Tabela 176. Pozycje kroniki GR (Rekord ogólny). Zbiór opisów pól QASYGRJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583.

Tabela 176. Pozycje kroniki GR (Rekord ogólny) (kontynuacja). Zbiór opisów pól QASYGRJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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 (Change) **ZR** Odczyt (Read)
	227	613	Nazwa użytkownika	Char(10)	Nazwa profilu użytkownika Dla typu pozycji F, pole to 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 176. Pozycje kroniki GR (Rekord ogólny) (kontynuacja). Zbiór opisów pól QASYGRJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	243	629	Pole 1	Char(102)[1]	Dane pola 1 Dla typu pozycji F, pole to zawiera opis wykonanej operacji rejestrowania funkcji. Możliwe wartości to: ***REGISTER:** Funkcja została zarejestrowana ***REREGISTER:** Funkcja została zaktualizowana ***DEREGISTER:** Funkcja została wyrejestrowana ***CHGUSAGE:** Informacje dotyczące korzystania z 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, pole to 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 176. Pozycje kroniki GR (Rekord ogólny) (kontynuacja). Zbiór opisów pól QASYGRJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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, pole to zawiera nazwę funkcji, na której wykonywano działanie. Dla typu pozycji C, pole to 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 176. Pozycje kroniki GR (Rekord ogólny) (kontynuacja). Zbiór opisów pól QASYGRJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	459	845	Pole 3	Char(102)[1]	Dane pola 3. Dla typu pozycji F, pole to zawiera ustawienia użycia dla użytkownika. Dla pola tego istnieje wartość tylko wówczas, gdy operacja rejestracji funkcji posiada jedną z następujących wartości: ***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 pole to 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, pole to zawiera ustawienie *ALLOBJ dla funkcji. Dla pola tego istnieje wartość tylko wówczas, gdy operacja rejestracji funkcji posiada jedną z następujących wartości: ***REGISTER** ***REREGISTER**

Tabela 176. Pozycje kroniki GR (Rekord ogólny) (kontynuacja). Zbiór opisów pól QASYGRJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
[1]	Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość pola.				

Pozycje kroniki GS (Nadanie deskryptora)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki GS (Nadanie deskryptora).

Tabela 177. Pozycje kroniki GS (Nadanie deskryptora). Zbiór opisów pól QASYGSJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
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	Nieupakowane (6,0)	Numer zadania.
183	251	637	Nazwa profilu użytkownika	Char(10)	Nazwa profilu użytkownika.
	261	647	JUID	Char(10)	Identyfikator użytkownika zadania dla zadania docelowego. (Ta wartość stosowana jest tylko dla podtypu G rekordów kontroli.)

Pozycje kroniki IM (Monitor włamań)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki IM (Monitor włamań).

Tabela 178. Pozycje kroniki IM (Monitor włamań). Zbiór opisu pola QASYIMJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
		1			Pola nagłówka wspólne dla wszystkich typów pozycji.
		610	Typ pozycji	Char(1)	Typ pozycji. **P** Wykryto możliwe naruszenie systemu
		611	Godzina zdarzenia	TIMESTAMP	Godzina, o której wykryto zdarzenie, w formacieSAA.

Tabela 178. Pozycje kroniki IM (Monitor włamań) (kontynuacja). Zbiór opisu pola QASYIMJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
		637	Identyfikator punktu wykrycia	Char(4)	Unikalny identyfikator miejsca przetwarzania, które wykryło naruszenie systemu. Pole to przeznaczone jest dla personelu serwisowego.
		641	Rodzina adresów lokalnych	Char(1)	Rodzina lokalnych adresów IP związanych z wykrytym zdarzeniem.
		642	Numer portu lokalnego	Nieupakowane (5, 0)	Numer portu lokalnego związanego z wykrytym zdarzeniem.
		647	Lokalny adres IP	Char(46)	Lokalny adres IP związany z wykrytym zdarzeniem.
		693	Rodzina adresów zdalnych	Char(1)	Rodzina zdalnych adresów IP związanych z wykrytym zdarzeniem.
		694	Numer portu zdalnego	Nieupakowane (5, 0)	Numer portu zdalnego związanego z wykrytym zdarzeniem.
		699	Zdalny adres IP	Char(46)	Zdalny adres IP związany z wykrytym zdarzeniem.
		745	Identyfikator typu badania	Char(6)	Określa typ badania wykorzystany do wykrycia możliwego naruszenia systemu. Możliwe są następujące wartości: **ATTACK** Zdarzenie wykrycia ataku **TR-TCP** Zdarzenie wykrycia kontroli ruchu przez TCP. **TR-UDP** Zdarzenie wykrycia kontroli ruchu przez UDP. **SCANE** Zdarzenie wykrycia skanowania **SCANG** Zdarzenie wykrycia globalnego skanowania **XATTACK** Możliwy atak z wewnątrz **XTRTCP** Zdarzenie wykrycia kontroli ruchu wychodzącego (TCP) **XTRUDP** Zdarzenie wykrycia kontroli ruchu wychodzącego (UDP) **XSCAN** Zdarzenie wykrycia skanowania ruchu wychodzącego
		751	Korelator zdarzeń	Char(4)	Unikalny identyfikator danego naruszenia systemu. Identyfikator może być użyty w korelacji tego rekordu kontroli z innymi informacjami o wykrytych włamaniach.

Tabela 178. Pozycje kroniki IM (Monitor włamań) (kontynuacja). Zbiór opisu pola QASYIMJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
		755	Typ zdarzenia	Char(8)	Określa typ możliwego wykrytego włamania. Możliwe wartości są następujące: **ACKSTORM** Zalew pakietów ACK TCP **ADRPOISN** Zatruwanie adresu **FLOOD** Atak typu flood **FRAGGLE** Atak typu fraggle **ICMPRED** Przekierowanie ICMP (Internet Control Message Protocol) **IPFRAG** Fragmentacja IP **MALFPKT** Zniekształcony pakiet **OUTRAW** Jawny atak z wewnątrz **PERPECH** Bezterminowe echo **PNGDEATH** Atak typu ping of death **RESTOPT** Zastrzeżone opcje IP **RESTPROT** Zastrzeżony protokół IP **SMURF** Atak typu smurf
		763	Protokół	Char(3)	Numer protokołu
		766	Warunek	Char(4)	Numer warunku ze zbioru strategii IDS
		770	Przytłumianie	Char(1)	• 0 = nieaktywne • 1 = aktywne
		771	Odrzucone pakiety	Nieupakowane (5, 0)	Liczba pakietów odrzuconych w trakcie przytłumiania
		776	Docelowy stos TCP/IP	Char(1)	**P** Stos produkcji **S** Stos usług
		777	Zarezerwowane	Char(6)	Zarezerwowane do wykorzystania w przyszłości
		783	Podejrzany pakiet	Char(1002)[1]	Zmienna długość pola, która może zawierać do 1000 początkowych bajtów pakietu IP związanego z wykrytym zdarzeniem. Pole to zawiera dane binarne i powinno być traktowane jakby posiadało identyfikator CCSID 65 535.

Tabela 178. Pozycje kroniki IM (Monitor włamań) (kontynuacja). Zbiór opisu pola QASYIMJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
[1]	Jest to pole o zmiennej długości. Pierwsze 2 bajty zawierają długość informacji o podejrzanym pakiecie.				

Pozycje kroniki IP (Komunikacja między procesami)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki IP (Komunikacja między procesami)

Tabela 179. Pozycje kroniki IP (Komunikacja między procesami). Zbiór opisów pól QASYIPJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Zmiany prawa własności i/lub uprawnień **C** Tworzenie (Create) **D** Usunięcie (Delete) **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
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

Tabela 179. Pozycje kroniki IP (Komunikacja między procesami) (kontynuacja). Zbiór opisów pól QASYIPJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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. Pierwsze dwa znaki zawierają długość nazwy semaforu.

Pozycje kroniki IR (Działania reguł IP)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki IR (Działania reguł IP).

Tabela 180. Pozycje kroniki IR (Działania reguł IP). Zbiór opisów pól QASYIRJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583.
	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).

Tabela 180. Pozycje kroniki IR (Działania reguł IP) (kontynuacja). Zbiór opisów pól QASYIRJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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.
	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	ID zbioru obiektu[1,2]	Char(16)	Identyfikator zbioru dla obiektu.
	309	695	Nazwa zbioru[1]	Char(512)	Nazwa zbioru.
	821	1207	Sekwencja połączenia	Char(40)	Nazwa połączenia.
	861	1247	ID zbioru dla obiektu	Char(16)	Identyfikator zbioru dla 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 nazwy ścieżki.
	896	1282	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.
	898	1284	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	901	1287	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.

Tabela 180. Pozycje kroniki IR (Działania reguł IP) (kontynuacja). Zbiór opisów pól QASYIRJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	903	1289	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	904	1290	Identyfikator zbioru w katalogu względnym[3]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[3]
	920	1306	Nazwa ścieżki[4]	Char(5002)	Nazwa ścieżki obiektu.

[1] Te pola są używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanym przez użytkownika.

[2] Jeśli identyfikator ma ustawiony ostatni lewy bit i resztę bitów zerowych oznacza to, że identyfikator nie jest ustawiony.

[3] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

[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 puli ASP obiektu.

Pozycje kroniki IS (Zarządzanie bezpieczeństwem internetowym)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki IS (Zarządzanie bezpieczeństwem internetowym).

Tabela 181. Pozycje kroniki IS (Zarządzanie bezpieczeństwem internetowym). Zbiór opisów pól QASYISJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583.

Tabela 181. Pozycje kroniki IS (Zarządzanie bezpieczeństwem internetowym) (kontynuacja). Zbiór opisów pól QASYISJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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[1]	Char(15)	Lokalny adres IP.
	240	626	Port identyfikatora klienta lokalnego	Char(5)	Port identyfikatora klienta lokalnego.
	245	631	Zdalny adres IP[1]	Char(15)	Zdalny adres IP.
	260	646	Port identyfikatora klienta zdalnego	Char(5)	Port identyfikatora klienta zdalnego (poprawny dla fazy 2).
	265	651	Rodzina lokalnych adresów IP	Char(1)	Rodzina lokalnych adresów IP **4** IPv4 **6** IPv6
		652	Lokalny adres IP	Char(46)	Lokalny adres IP
		698	Rodzina zdalnych adresów IP	Char(1)	Rodzina zdalnych adresów IP **4** IPv4 **6** IPv6
		699	Zdalny adres IP	Char(46)	Zdalny adres IP
		745	Zarezerwowane	Char(162)	Zarezerwowane
	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** i5/OSBłędy programu VPN Key Manager
	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

Tabela 181. Pozycje kroniki IS (Zarządzanie bezpieczeństwem internetowym) (kontynuacja). Zbiór opisów pól QASYISJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	785	1171	Typ identyfikatora klienta lokalnego,	Char(2)	Typ identyfikatora klienta (poprawny dla fazy 2): **1** adres IP wersja 4 **2** pełna nazwa domeny **3** Pełna nazwa domeny użytkownika **4** podsieć IP wersja 4 **5** Adres IP wersja 6 **6** Podsieć IP wersja 6 **7** zakres adresów IP wersja 4 **8** Zakres adresów IP wersja 6 **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 wersja 4 **2** pełna nazwa domeny **3** Pełna nazwa domeny użytkownika **4** podsieć IP wersja 4 **5** Adres IP wersja 6 **6** Podsieć IP wersja 6 **7** zakres adresów IP wersja 4 **8** Zakres adresów IP wersja 6 **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)
[1] To pole obsługuje jedynie adresy IPv4.					

Pozycje kroniki JD (Zmiana opisu zadania)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki JD (Zmiana opisu zadania).

Tabela 182. Pozycje kroniki JD (Zmiana opisu zadania). Zbiór opisów pól QASYJDJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
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 składowany jest 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

Pozycje kroniki JS (Zmiana zadania)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki JS (Zmiana zadania)

Tabela 183. Pozycje kroniki JS (Zmiana zadania). Zbiór opisów pól QASYJSJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.

Tabela 183. Pozycje kroniki JS (Zmiana zadania) (kontynuacja). Zbiór opisów pól QASYJSJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Komenda ENDJOBABN **B** Wprowadzenie (Submit) **C** Zmiana (Change) **E** Zakończenie (End) **H** Wstrzymanie (Hold) **I** Odłączenie **J** Bieżące zadanie usiłuje przerwać pracę innego zadania **K** Bieżące zadanie zostanie przerwane **L** Nastąpiło przerwanie bieżącego zadania **M** Zmiana profilu lub profilu grupowego **N** Komenda ENDJOB **P** Podłączenie zadania prestartu lub natychmiastowego zadania wsadowego **Q** Zmiana atrybutów zapytania **R** Zwalnianie (Release) **S** Uruchomienie (Start) **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

Tabela 183. Pozycje kroniki JS (Zmiana zadania) (kontynuacja). Zbiór opisów pól QASYJSJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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 (Query) **T** MRT **U** Alternatywny użytkownik buforu
159	227	613	Nazwa zadania	Char(10)	Pierwsza część pełnej nazwy zadania
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.

Tabela 183. Pozycje kroniki JS (Zmiana zadania) (kontynuacja). Zbiór opisów pól QASYJSJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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. **T** Tak **N** Nie
	985	1371	Zmiana użytkownika efektywnego[3]	Char(1)	Efektywny profil użytkownika został zmieniony. **T** Tak **N** Nie
	986	1372	Zmiana zeskładowanego użytkownika[3]	Char(1)	Zeskładowany profil użytkownika został zmieniony **T** Tak **N** Nie
	987	1373	Zmiana rzeczywistej grupy[3]	Char(1)	Rzeczywisty profil grupowy został zmieniony. **T** Tak **N** Nie
	988	1374	Zmiana grupy efektywnej[3]	Char(1)	Efektywny profil grupowy został zmieniony **T** Tak **N** Nie
	989	1375	Zmiana zeskładowanej grupy[3]	Char(1)	Zeskładowany profil grupowy został zmieniony. **T** Tak **N** Nie
	990	1376	Zmiana grup dodatkowych[3]	Char(1)	Dodatkowe profile grupowe zostały zmienione. **T** Tak **N** Nie
	991	1377	Numer listy bibliotek[4]	Bin(4)	Liczba bibliotek w polu rozszerzenia listy bibliotek (pozycja 993).

Tabela 183. Pozycje kroniki JS (Zmiana zadania) (kontynuacja). Zbiór opisów pól QASYJSJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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
		3656	Nazwa strefy czasowej	Char(10)	Nazwa opisowa strefy czasowej
		3666	Nazwa zadania wyjściowego	Char(10)	Nazwa zadania, które przerwało pracę bieżącego zadania, lub nazwa zadania, którego praca została przerwana przez bieżące zadanie.
		3676	Użytkownik zadania wyjściowego	Char(10)	Nazwa użytkownika zadania, które przerwało pracę bieżącego zadania, lub nazwa użytkownika zadania, którego praca została przerwana przez bieżące zadanie.
		3686	Numer zadania wyjściowego[6, 7]	Char(6)	Numer zadania, które przerwało pracę bieżącego zadania, lub numer zadania, którego praca została przerwana przez bieżące zadanie.
		3692	Nazwa programu wyjściowego[6]	Char(10)	Nazwa programu wyjściowego użytego do przerwania pracy zadania
		3702	Biblioteka programu wyjściowego[6]	Char(10)	Nazwa biblioteki programu wyjściowego użytego do przerwania pracy zadania
		3712	Nazwa ASP biblioteki JOBQ	Char(10)	Nazwa ASP biblioteki JOBQ
		3722	Numer ASP biblioteki JOBQ	Char(5)	Numer ASP biblioteki JOBQ

[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] Pole to wykorzystywane jest tylko wówczas, gdy typ pozycji (przesunięcie 610) to M lub T.

[4] Pole to wykorzystywane jest tylko wówczas, gdy ilość bibliotek na liście bibliotek przekracza długość pola pod przesunięciem 729.

[5] Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość danych w tym polu.

[6] Pole to wykorzystywane jest tylko wówczas, gdy typ pozycji (przesunięcie 610) to J, K, lub L.

[7] Jeśli typ pozycji to J, pole to zawiera informacje o zadaniu, które zostanie przerwane. Jeśli typ pozycji to K lub L, pole to zawiera informacje o zadaniu, które zażądało przerwania bieżącego zadania.

Pozycje kroniki KF (Plik bazy kluczy)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki KF (Plik bazy kluczy).

Tabela 184. Pozycje kroniki KF (Plik bazy kluczy). Zbiór opisów pól QASYKFJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583.
	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

Tabela 184. Pozycje kroniki KF (Plik bazy kluczy) (kontynuacja). Zbiór opisów pól QASYKFJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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)	
	266	652	Identyfikator pliku nadrzędnego	Char(16)	Identyfikator pliku katalogu nadrzędnego kluczy.
	282	668	ID zbioru 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	ID zbioru 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	ID zbioru 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.

Tabela 184. Pozycje kroniki KF (Plik bazy kluczy) (kontynuacja). Zbiór opisów pól QASYKFJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	2445	2831	Identyfikator CCSID nazwy ścieżki	Binary(5)	Identyfikator kodowanego zestawu znaków dla nazwy ścieżki.
	2449	2835	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.
	2451	2837	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	2454	2840	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.
	2456	2842	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do pliku bazy kluczy. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	2457	2843	Identyfikator zbioru w katalogu względnym[2]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[2]
	2473	2859	Bezwzględna nazwa ścieżki[1]	Char(5002)	Bezwzględna nazwa ścieżki do pliku bazy kluczy.
	7475	7861	ID zbioru obiektu	Char(16)	Identyfikator pliku zbioru źródłowego lub docelowego.
	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 nazwy ścieżki.
	7510	7896	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.
	7512	7898	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	7515	7901	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.

Tabela 184. Pozycje kroniki KF (Plik bazy kluczy) (kontynuacja). Zbiór opisów pól QASYKFJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	7517	7903	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną bezwzględną nazwę ścieżki do zbioru źródłowego lub docelowego. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	7518	7904	Identyfikator zbioru w katalogu względnym[3]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[2]
	7534	7920	Bezwzględna nazwa ścieżki[1]	Char(5002)	Bezwzględna nazwa ścieżki do zbioru źródłowego lub docelowego.

[1] Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

[2] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

[3] Kiedy 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.

Pozycje kroniki LD (Dowiązanie, usunięcie dowiązania, wyszukiwanie katalogu)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki LD (Dowiązanie, usunięcie dowiązania, wyszukiwanie katalogu).

Tabela 185. Pozycje kroniki LD (Dowiązanie, usunięcie dowiązania, wyszukiwanie katalogu). Zbiór opisów pól QASYLDJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.

Tabela 185. Pozycje kroniki LD (Dowiązanie, usunięcie dowiązania, wyszukiwanie katalogu) (kontynuacja). Zbiór opisów pól QASYLDJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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 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	ID zbioru obiektu[1,2]	Char(16)	Identyfikator zbioru dla obiektu.
221	289	675	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	801	1187	ID zbioru obiektu	Char(16)	Identyfikator zbioru dla 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 nazwy ścieżki.
	836	1222	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.
	838	1224	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	841	1227	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.

Tabela 185. Pozycje kroniki LD (Dowiązanie, usunięcie dowiązania, wyszukiwanie katalogu) (kontynuacja). Zbiór opisów pól QASYLDJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	843	1229	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	844	1230	Identyfikator zbioru katalogu względnego[1]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[1]
	860	1246	Nazwa ścieżki[2]	Char(5002)	Nazwa ścieżki obiektu.

[1] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

[2] Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

Pozycje kroniki ML (Działanie poczty)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki ML (Działanie poczty).

Tabela 186. Pozycje kroniki ML (Działanie poczty). Zbiór opisów pól QASYMLJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
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 NA (Zmiana atrybutu)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki NA (Zmiana atrybutu).

Tabela 187. Pozycje kroniki NA (Zmiana atrybutu). Zbiór opisów pól QASYNAJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
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.

Pozycje kroniki ND (Filtr przeszukiwania katalogów APPN)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki ND (Filtr przeszukiwania katalogów APPN).

Tabela 188. Pozycje kroniki ND (Filtr przeszukiwania katalogów APPN). Zbiór opisów pól QASYNDJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
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

Tabela 188. Pozycje kroniki ND (Filtr przeszukiwania katalogów APPN) (kontynuacja). Zbiór opisów pól QASYNDJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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. **T** To jest sesja przychodząca **N** To nie jest sesja przychodząca
206	274	660	Sesja wychodząca	Char(1)	Sesja wychodząca. **T** To jest sesja wychodząca **N** To nie jest sesja wychodząca

Szczegółowe informacje na temat filtru przeszukiwania katalogów APPN i punktów końcowych APPN zawiera sekcja Zabezpieczenie systemu w środowisku APPN i HPR.

Pozycje kroniki NE (Filtr punktów końcowych APPN)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki NE (Filtr punktów końcowych APPN).

Tabela 189. Pozycje kroniki NE (Filtr punktów końcowych APPN). Zbiór opisów pól QASYNEJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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. **T** To jest sesja przychodząca **N** To nie jest sesja przychodząca

Tabela 189. Pozycje kroniki NE (Filtr punktów końcowych APPN) (kontynuacja). Zbiór opisów pól QASYNEJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
182	250	636	Sesja wychodząca	Char(1)	Sesja wychodząca. **T** To jest sesja wychodząca **N** To nie jest sesja wychodząca

Szczegółowe informacje na temat filtru przeszukiwania katalogów APPN i punktów końcowych APPN zawiera sekcja Zabezpieczenie systemu w środowisku APPN i HPR.

Pozycje kroniki OM (Zmiana zarządzania obiektami)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki OM (Zmiana zarządzania obiektami).

Tabela 190. Pozycje kroniki OM (Zmiana zarządzania obiektami). Zbiór opisów pól QASYOMJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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 poprzedni obiekt.
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 przeniesiony został obiekt.
205	273		(Obszar zastrzeżony)	Char(20)	
		659	Atrybut obiektu	Char(10)	Atrybut obiektu.
		669	(Obszar zastrzeżony)	Char(10)	
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

Tabela 190. Pozycje kroniki OM (Zmiana zarządzania obiektami) (kontynuacja). Zbiór opisów pól QASYOMJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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 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.

Tabela 190. Pozycje kroniki OM (Zmiana zarządzania obiektami) (kontynuacja). Zbiór opisów pól QASYOMJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1583	1969	ID zbioru obiektu[1,2]	Char(16)	Identyfikator zbioru dla obiektu.
	1599	1985	Nazwa puli ASP[7]	Char(10)	Nazwa urządzenia puli ASP.
	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 nazwy ścieżki.
	1618	2004	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.
	1620	2006	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	1623	2009	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.
	1625	2011	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	1626	2012	Identyfikator zbioru w katalogu względnym[3]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[3]
	1642	2028	Bezwzględna nazwa ścieżki[5]	Char(5002)	Poprzednia bezwzględna nazwa ścieżki do obiektu.
	6644	7030	ID zbioru obiektu	Char(16)	Identyfikator zbioru dla 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 nazwy ścieżki.
	6679	7065	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.

Tabela 190. Pozycje kroniki OM (Zmiana zarządzania obiektami) (kontynuacja). Zbiór opisów pól QASYOMJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	6681	7067	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	6684	7070	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.
	6686	7072	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	6687	7073	Identyfikator zbioru w katalogu względnym[4]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[3]
	6703	7089	Bezwzględna nazwa ścieżki[5]	Char(5002)	Nowa bezwzględna nazwa ścieżki do obiektu.

[1] Te pola są używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanych przez użytkownika.

[2] Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

[3] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

[4] Kiedy 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.

Pozycje kroniki OR (Odtwarzanie obiektu)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki OR (Odtwarzanie obiektu).

Tabela 191. Pozycje kroniki OR (Odtwarzanie obiektu). Zbiór opisów pól QASYORJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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. **T** Odtworzony został program z atrybutem system-state. **N** Odtworzony został program z atrybutem user-state.
206	274	660	Komenda systemu[2]	Char(1)	**T** 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. **T** Bit trybu SETUID dla odtworzonego obiektu jest ustawiony. **N** Bit trybu SETUID dla odtworzonego obiektu nie jest ustawiony.

Tabela 191. Pozycje kroniki OR (Odtwarzanie obiektu) (kontynuacja). Zbiór opisów pól QASYORJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	276	662	Tryb SETGID	Char(1)	Indykator trybu SETGID. **T** 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 ma format inny niż i5/OS **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 **T** *YES **N** *NO **C** *CHGONLY Opisy tych wartości zawiera opis komendy CHGATR.
	279		(Obszar zastrzeżony)	Char(14)	
		665	Atrybut obiektu	Char(10)	Atrybut obiektu.
		675	(Obszar zastrzeżony)	Char(4)	
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.
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.

Tabela 191. Pozycje kroniki OR (Odtwarzanie obiektu) (kontynuacja). Zbiór opisów pól QASYORJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
401	469	855	Praca w imieniu użytkownika	Char(10)	Użytkownik pracujący w imieniu innego użytkownika.
411			(Obszar zastrzeżony)	Char(20)	
	479		(Obszar zastrzeżony)	Char(18)	
		865	Odtwórz uprawnienia prywatne	Char(1)	Zażądano odtworzenia uprawnień prywatnych (podano PVTAUT(*YES) w komendzie odtworzenia) **T** W komendzie odtworzenia podano PVTAUT(*YES) **N** W komendzie odtworzenia podano PVTAUT(*NO)
		866	Zapisano uprawnienia prywatne[8]	Binary(5)	Liczba zeskładowanych uprawnień prywatnych
		870	Liczba odtworzonych uprawnień prywatnych[8]	Binary(5)[8]	Liczba odtworzonych uprawnień prywatnych
		874	(Obszar zastrzeżony)	Char(9)	
	497	883	Długość nazwy obiektu	Binary(4)	Długość pola poprzedniej nazwy obiektu.
431	499	885	Identyfikator CCSID nazwy obiektu[3]	Binary(5)	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	ID zbioru obiektu[3,4]	Char(16)	Identyfikator zbioru dla obiektu.
475	543	929	Nazwa obiektu [3]	Char(512)	Nazwa obiektu.
	1055	1441	Identyfikator poprzedniego pliku	Char(16)	Identyfikator pliku dla poprzedniego obiektu.

Tabela 191. Pozycje kroniki OR (Odtwarzanie obiektu) (kontynuacja). Zbiór opisów pól QASYORJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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	ID zbioru obiektu	Char(16)	Identyfikator zbioru dla 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 nazwy ścieżki.
	1122	1508	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.
	1124	1510	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	1127	1513	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.
	1129	1515	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **Y** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	1130	1516	Identyfikator zbioru w katalogu względnym[5]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[5]
	1146	1532	Nazwa ścieżki[6]	Char(5002)	Nazwa ścieżki 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] To pole jest używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanych przez użytkownika.

[4] Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

[5] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

Tabela 191. Pozycje kroniki OR (Odtwarzanie obiektu) (kontynuacja). Zbiór opisów pól QASYORJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
[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 puli ASP obiektu.		
[8]			Jeśli wartość w polu Odtwórz uprawnienia prywatne (przesuniecie 865) to N, to pole ma wartość zero.		

Pozycje kroniki OW (Zmiana prawa własności)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki OW (Zmiana prawa własności).

Tabela 192. Pozycje kroniki OW (Zmiana prawa własności). Zbiór opisów pól QASYOWJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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 składowany jest 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)	
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.

Tabela 192. Pozycje kroniki OW (Zmiana prawa własności) (kontynuacja). Zbiór opisów pól QASYOWJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
348	416	802	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	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	ID zbioru obiektu[1,2]	Char(16)	Identyfikator zbioru dla obiektu.
392	460	846	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	972	1358	ID zbioru 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 nazwy ścieżki.
	1007	1393	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.
	1009	1395	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	1012	1398	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.
	1014	1400	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	1015	1401	Identyfikator zbioru w katalogu względnym[3]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[3]

Tabela 192. Pozycje kroniki OW (Zmiana prawa własności) (kontynuacja). Zbiór opisów pól QASYOWJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1031	1417	Nazwa ścieżki[4]	Char(5002)	Nazwa ścieżki obiektu.

[1] Te pola są używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanym przez użytkownika.

[2] Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

[3] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

[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 puli ASP obiektu.

Pozycje kroniki O1 (Dostęp optyczny)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki O1 (Dostęp optyczny).

Tabela 193. Pozycje kroniki O1 (Dostęp optyczny). zbiór opisu pola QASY01JE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
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

Tabela 193. Pozycje kroniki O1 (Dostęp optyczny) (kontynuacja). zbiór opisu pola QASY01JE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
169	237	623	Nazwa CSI	Char(8)	Nazwa obiektu pobocznego
177	245	631	Biblioteka CSI	Char(10)	Biblioteka obiektu pobocznego
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.					

Pozycje kroniki O2 (Dostęp optyczny)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki O2 (Dostęp optyczny).

Tabela 194. Pozycje kroniki O2 (Dostęp optyczny). zbiór opisu pola QASY02JE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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

Tabela 194. Pozycje kroniki O2 (Dostęp optyczny) (kontynuacja). zbiór opisu pola QASY02JE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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
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

Pozycje kroniki O3 (Dostęp optyczny)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki O3 (Dostęp optyczny).

Tabela 195. Pozycje kroniki O3 (Dostęp optyczny). zbiór opisu pola QASY03JE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Lista pól znajduje się w sekcjach “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581, “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.

Tabela 195. Pozycje kroniki O3 (Dostęp optyczny) (kontynuacja). zbiór opisu pola QASY03JE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
156	224	610	Typ pozycji	Char(1)	**A** Zmiana atrybutów woluminu **B** Tworzenie kopii zapasowej woluminu **C** Konwersja woluminu zapasowego na podstawowy **E** Eksportowanie **I** Inicjowanie (Initialize) **K** Sprawdzenie woluminu **L** Zmiana listy autoryzacji **M** Importowanie **N** Zmiana nazwy (Rename) **R** Odczyt bezwzględny
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
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).

Pozycje kroniki PA (Adoptowanie programu)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki PA (Adoptowanie programu).

Tabela 196. Pozycje kroniki PA (Adoptowanie programu). Zbiór opisów pól QASYPAJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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). **T** 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.
	283	669	Identyfikator CCSID nazwy obiektu[1]	Binary(5)	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.

Tabela 196. Pozycje kroniki PA (Adoptowanie programu) (kontynuacja). Zbiór opisów pól QASYPAJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	839	1225	Tryb SETUID	Char(1)	Indykator trybu ustawiania efektywnego identyfikatora użytkownika (Set effective user ID - SETUID). **T** 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). **T** 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	ID zbioru obiektu	Char(16)	Identyfikator zbioru dla 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 nazwy ścieżki.
	886	1272	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.
	888	1274	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	891	1277	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.
	893	1279	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	894	1280	Identyfikator zbioru w katalogu względnym[4]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[4]
	910	1296	Nazwa ścieżki[5]	Char(5002)	Nazwa ścieżki obiektu.

Tabela 196. Pozycje kroniki PA (Adoptowanie programu) (kontynuacja). Zbiór opisów pól QASYPAJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
[1]			Te pola są używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanych przez użytkownika.		
[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]			Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.		
[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 puli ASP obiektu.		

Pozycje kroniki PG (Zmiana grupy podstawowej)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki PG (Zmiana grupy podstawowej).

Tabela 197. Pozycje kroniki PG (Zmiana grupy podstawowej). Zbiór opisów pól QASYPGJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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)	**T** *OBJEXIST
206	274	660	Zarządzanie obiektami	Char(1)	**T** *OBJMGT
207	275	661	Operacyjne do obiektu	Char(1)	**T** *OBJOPR
208	276	662	Zmiana obiektu	Char(1)	**T** *OBJALTER

Tabela 197. Pozycje kroniki PG (Zmiana grupy podstawowej) (kontynuacja). Zbiór opisów pól QASYPGJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
209	277	663	Odniesienie do obiektu	Char(1)	**T** *OBJREF
210	278	664	(Obszar zastrzeżony)	Char(10)	
220	288	674	Zarządzanie listą autoryzacji	Char(1)	**T** *AUTLMGT
221	289	675	Uprawnienie do odczytu	Char(1)	**T** *READ
222	290	676	Uprawnienie do dodawania	Char(1)	**T** *ADD
223	291	677	Uprawnienie do aktualizacji	Char(1)	**T** *UPD
224	292	678	Uprawnienie do usuwania	Char(1)	**T** *DLT
225	293	679	Uprawnienie do uruchamiania	Char(1)	**T** *EXECUTE
226	294	680	(Obszar zastrzeżony)	Char(10)	
236	304	690	Uprawnienie na wyłączność	Char(1)	**T** *EXCLUDE
237	305	691	Odebranie poprzedniej grupy podstawowej	Char(1)	**T** 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 kodowanego zestawu znaków dla nazwy obiektu.

Tabela 197. Pozycje kroniki PG (Zmiana grupy podstawowej) (kontynuacja). Zbiór opisów pól QASYPGJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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	ID zbioru obiektu[1,2]	Char(16)	Identyfikator zbioru dla obiektu.
425	493	879	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	1005	1391	ID zbioru obiektu	Char(16)	Identyfikator zbioru dla 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 nazwy ścieżki.
	1040	1426	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.
	1042	1428	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	1045	1431	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.
	1047	1433	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	1048	1434	Identyfikator zbioru w katalogu względnym[3]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[3]
	1064	1450	Nazwa ścieżki[4]	Char(5002)	Nazwa ścieżki obiektu.

Tabela 197. Pozycje kroniki PG (Zmiana grupy podstawowej) (kontynuacja). Zbiór opisów pól QASYPGJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
[1]			Te pola są używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanych przez użytkownika.		
[2]			Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.		
[3]			Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.		
[4]			Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.		
[5]			Wartość *N oznacza, że wartość poprzedniej grupy podstawowej 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 puli ASP obiektu.		

Pozycje kroniki PO (Zbiór wydruku)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki PO (Zbiór wydruku).

Tabela 198. Pozycje kroniki PO (Zbiór wydruku). Zbiór opisów pól QASYPOJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**`J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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
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	Nieupakowane (6,0)	Trzecia część pełnej nazwy zadania.
184	252	638	Profil użytkownika	Char(10)	Profil użytkownika, który utworzył wydruk.

Tabela 198. Pozycje kroniki PO (Zbiór wydruku) (kontynuacja). Zbiór opisów pól QASYPOJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**`J4**	**J5**			
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).
		1164	Nazwa puli ASP	Char(10)	Nazwa puli ASP dla biblioteki urządzenia

Tabela 198. Pozycje kroniki PO (Zbiór wydruku) (kontynuacja). Zbiór opisów pól QASYPOJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**`J4**	**J5**			
		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.
		1194	Data utworzenia zbioru buforowego (UTC)	Char(7)	Data utworzenia zbioru buforowego (jest to ta sama data co data utworzenia zbioru buforowego (pozycja 1151), jednak w formacie czasu UTC).
		1201	Godzina utworzenia zbioru buforowego (UTC)	Char(6)	Godzina utworzenia zbioru buforowego (jest to ta sama godzina co godzina utworzenia zbioru buforowego (pozycja 1158), jednak w formacie czasu UTC).

[1] To pole jest puste, jeśli typem wydruku jest drukowanie bezpośrednie.

[2] To pole jest puste, jeśli typem wydruku jest drukowanie zdalne.

Pozycje kroniki PS (Przełączanie profilu)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki PS (Przełączanie profilu).

Tabela 199. Pozycje kroniki PS (Przełączanie profilu). Zbiór opisów pól QASYPSJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.

Tabela 199. Pozycje kroniki PS (Przełączanie profilu) (kontynuacja). Zbiór opisów pól QASYPSJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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.
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)	Czas ważności tokenu profilu, podany w sekundach.

Pozycje kroniki PW (Hasło)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki PW (Hasło).

Tabela 200. Pozycje kroniki PW (Hasło). Zbiór opisów pól QASYPWJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
156	224	610	Typ pozycji naruszenia	Char(1)	Typ naruszenia **A** Połączenie APPC nie powiodło się. **C** Uwierzytelnienie użytkownika za pomocą komendy CHKPWD nie powiodło się. **D** Niepoprawna nazwa identyfikatora użytkownika narzędzi serwisowych. **E** Niepoprawne hasło identyfikatora użytkownika narzędzi serwisowych. **P** Niepoprawne hasło. **Q** Próba wpisania się (uwierzytelnienia użytkownika) nie powiodła się, ponieważ profil użytkownika został wyłączony. **R** Próba wpisania się (uwierzytelnienia użytkownika) nie powiodła się, ponieważ upłynął termin ważności hasła. Ten rekord kontroli może nie działać w niektórych mechanizmach uwierzytelniania użytkowników. Niektóre z tych mechanizmów nie sprawdzają okresu ważności haseł. **S** Niepoprawne hasło deszyfrowania SQL. **U** Niepoprawna nazwa użytkownika. **X** Identyfikator użytkownika narzędzi serwisowych jest wyłączony. **T** Niepoprawny identyfikator użytkownika narzędzi serwisowych. **Z** Niepoprawne hasło identyfikatora użytkownika narzędzi serwisowych.
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.

Tabela 200. Pozycje kroniki PW (Hasło) (kontynuacja). Zbiór opisów pól QASYPWJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
223	291	677	ID sieci	Char(8)	ID sieci dla konsolidowania APPC.
		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.

Pozycje kroniki RA (Zmiana uprawnień dla odtworzonego obiektu)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki RA (Zmiana uprawnień dla odtworzonego obiektu).

Tabela 201. Pozycje kroniki RA (Zmiana uprawnień dla odtworzonego obiektu). Zbiór opisów pól QASYRAJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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 składowany jest 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)	**T** Uprawnienia publiczne ustawione na *EXCLUDE.
196	264	650	Uprawnienia prywatne	Char(1)	**T** Usunięto uprawnienia prywatne.

Tabela 201. Pozycje kroniki RA (Zmiana uprawnień dla odtworzonego obiektu) (kontynuacja). Zbiór opisów pól QASYRAJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
197	265	651	Usunięto AUTL	Char(1)	**T** 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 kodowanego zestawu znaków dla nazwy obiektu.
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	ID zbioru obiektu[1,2]	Char(16)	Identyfikator zbioru dla obiektu.
365	433	819	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	945	1331	ID zbioru obiektu	Char(16)	Identyfikator zbioru dla 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 nazwy ścieżki.
	980	1366	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.

Tabela 201. Pozycje kroniki RA (Zmiana uprawnień dla odtworzonego obiektu) (kontynuacja). Zbiór opisów pól QASYRAJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	982	1368	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	985	1371	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.
	987	1373	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	988	1374	Identyfikator zbioru w katalogu względnym[3]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[3]
	1004	1390	Nazwa ścieżki[4]	Char(5002)	Nazwa ścieżki obiektu.

[1] Te pola są używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanych przez użytkownika.

[2] Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

[3] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

[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 puli ASP obiektu.

Pozycje kroniki RJ (Odtwarzanie opisu zadania)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki RJ (Odtwarzanie opisu zadania).

Tabela 202. Pozycje kroniki RJ (Odtwarzanie opisu zadania). Zbiór opisów pól QASYRJJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.

Tabela 202. Pozycje kroniki RJ (Odtwarzanie opisu zadania) (kontynuacja). Zbiór opisów pól QASYRJJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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

Pozycje kroniki RO (Zmiana prawa własności do odtworzonego obiektu)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki RO (Zmiana prawa własności do odtworzonego obiektu).

Tabela 203. Pozycje kroniki RO (Zmiana prawa własności do odtworzonego obiektu). Zbiór opisów pól QASYROJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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.
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.

Tabela 203. Pozycje kroniki RO (Zmiana prawa własności do odtworzonego obiektu) (kontynuacja). Zbiór opisów pól QASYROJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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 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	ID zbioru obiektu[1,2]	Char(16)	Identyfikator zbioru dla obiektu.
372	440	826	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	952	1338	ID zbioru obiektu	Char(16)	Identyfikator zbioru dla 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 nazwy ścieżki.
	987	1373	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.
	989	1375	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	992	1378	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.

Tabela 203. Pozycje kroniki RO (Zmiana prawa własności do odtworzonego obiektu) (kontynuacja). Zbiór opisów pól QASYROJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	994	1380	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	995	1381	Identyfikator zbioru w katalogu względnym[3]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[3]
	1011	1397	Nazwa ścieżki[4]	Char(5002)	Nazwa ścieżki obiektu.

[1] Te pola są używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanych przez użytkownika.

[2] Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

[3] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

[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 puli ASP obiektu.

Pozycje kroniki RP (Odtwarzanie programów adoptujących uprawnienia)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki RP (Odtwarzanie programów adoptujących uprawnienia).

Tabela 204. Pozycje kroniki RP (Odtwarzanie programów adoptujących uprawnienia). Zbiór opisów pól QASYRPJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Odtwarzanie programów adoptujących uprawnienia właściciela

Tabela 204. Pozycje kroniki RP (Odtwarzanie programów adoptujących uprawnienia) (kontynuacja). Zbiór opisów pól QASYRPJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
157	225	611	Nazwa programu	Char(10)	Nazwa programu.
167	235	621	Biblioteka programu	Char(10)	Nazwa biblioteki, w której znajduje się obiekt.
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.
	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	ID zbioru obiektu[1,2]	Char(16)	Identyfikator zbioru dla obiektu.
	327	713	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	839	1225	ID zbioru obiektu	Char(16)	Identyfikator zbioru dla 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 nazwy ścieżki.
	874	1260	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.
	876	1262	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	879	1265	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.

Tabela 204. Pozycje kroniki RP (Odtwarzanie programów adoptujących uprawnienia) (kontynuacja). Zbiór opisów pól QASYRPJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	881	1267	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	882	1268	Identyfikator zbioru w katalogu względnym[3]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[3]
	898	1284	Nazwa ścieżki[4]	Char(5002)	Nazwa ścieżki obiektu.

[1] Te pola są używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanym przez użytkownika.

[2] Jeśli identyfikator ma ustawiony ostatni lewy bit i resztę bitów zerowych oznacza to, że identyfikator nie jest ustawiony.

[3] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

[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 puli ASP obiektu.

Pozycje kroniki RQ (Odtwarzanie obiektu deskryptora żądania zmiany)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki RQ (Odtwarzanie obiektu deskryptora żądania zmiany).

Tabela 205. Pozycje kroniki RQ (Odtwarzanie obiektu deskryptora żądania zmiany). Zbiór opisów pól QASYRQJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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.

Tabela 205. Pozycje kroniki RQ (Odtwarzanie obiektu deskryptora żądania zmiany) (kontynuacja). Zbiór opisów pól QASYRQJE/J4/J5

Pozycja (Offset)					
JE	**J4**	**J5**	**Pole**	**Format**	**Opis**
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

Pozycje kroniki RU (Odtwarzanie uprawnień dla profilu użytkownika)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki RU (Odtwarzanie uprawnień dla profilu użytkownika).

Tabela 206. 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 nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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

Pozycje kroniki RZ (Zmiana grupy podstawowej dla odtworzonego obiektu)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki RZ (Zmiana grupy podstawowej dla odtworzonego obiektu).

Tabela 207. Pozycje kroniki RZ (Zmiana grupy podstawowej dla odtworzonego obiektu). Zbiór opisów pól QASYRZJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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.
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 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 207. Pozycje kroniki RZ (Zmiana grupy podstawowej dla odtworzonego obiektu) (kontynuacja). Zbiór opisów pól QASYRZJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
356	424	810	ID zbioru obiektu[1,2]	Char(16)	Identyfikator zbioru dla obiektu.
372	440	826	Nazwa obiektu[1]	Char(512)	Nazwa obiektu.
	952	1338	ID zbioru obiektu	Char(16)	Identyfikator zbioru dla 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 nazwy ścieżki.
	987	1373	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.
	989	1375	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	992	1378	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.
	994	1380	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	995	1381	Identyfikator zbioru w katalogu względnym[3]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[3]
	1011	1397	Nazwa ścieżki[4]	Char(5002)	Nazwa ścieżki obiektu.

[1] Te pola są używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanych przez użytkownika.

[2] Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

[3] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

[4] Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.

Pozycje kroniki SD (Zmiana katalogu dystrybucyjnego systemu)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki SD (Zmiana katalogu dystrybucyjnego systemu).

Tabela 208. Pozycje kroniki SD (Zmiana katalogu dystrybucyjnego systemu). Zbiór opisów pól QASYSDJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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
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

Tabela 208. Pozycje kroniki SD (Zmiana katalogu dystrybucyjnego systemu) (kontynuacja). Zbiór opisów pól QASYSDJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
212	280	666	Identyfikator użytkownika sieci	Char(47)	Zmieniony identyfikator użytkownika sieci

Pozycje kroniki SE (Zmiana pozycji routingu podsystemu)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki SE (Zmiana pozycji routingu podsystemu).

Tabela 209. Pozycje kroniki SE (Zmiana pozycji routingu podsystemu). Zbiór opisów pól QASYSEJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
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 składowany jest 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
		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

Tabela 209. Pozycje kroniki SE (Zmiana pozycji routingu podsystemu) (kontynuacja). Zbiór opisów pól QASYSEJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
		691	Numer puli ASP dla biblioteki programu	Char(5)	Numer puli ASP dla biblioteki programu

Pozycje kroniki SF (Działanie na zbiorze buforowym)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki SF (Działanie na zbiorze buforowym).

Tabela 210. Pozycje kroniki SF (Działanie na zbiorze buforowym). Zbiór opisów pól QASYSFJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
156	224	610	Typ dostępu	Char(1)	Typ pozycji **A** Zbiór buforowy został odczytany przez kogoś innego niż właściciel tego zbioru. **C** Utworzenie zbioru buforowego. **D** Usunięcie zbioru buforowego. **H** Wstrzymanie zbioru buforowego. **I** Tworzenie zbioru wstawianego. **R** Zwolnienie zbioru buforowego. **S** Zbiór buforowy zapisany. **T** Zbiór buforowy wczytany. **U** Atrybuty zbioru buforowego dotyczące ochrony zostały zmienione. **V** Tylko atrybuty zbioru buforowego nie dotyczące ochrony zostały zmienione.
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].

Tabela 210. Pozycje kroniki SF (Działanie na zbiorze buforowym) (kontynuacja). Zbiór opisów pól QASYSFJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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.
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.

Tabela 210. Pozycje kroniki SF (Działanie na zbiorze buforowym) (kontynuacja). Zbiór opisów pól QASYSFJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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.
	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.

Tabela 210. Pozycje kroniki SF (Działanie na zbiorze buforowym) (kontynuacja). Zbiór opisów pól QASYSFJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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).
	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.

Tabela 210. Pozycje kroniki SF (Działanie na zbiorze buforowym) (kontynuacja). Zbiór opisów pól QASYSFJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
		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.
		1665	Poprzedni stan zbioru buforowego	Char(3)	Poprzedni stan zbioru buforowego.
		1668	Nowy stan zbioru buforowego	Char(3)	Nowy stan zbioru buforowego.
		1671	Oryginalna data utworzenia	Char(7)	Oryginalna data utworzenia.
		1678	Oryginalna godzina utworzenia	Char(6)	Oryginalna godzina utworzenia.
		1684	Poprzednia data ważności zbioru buforowego	Char(7)	Poprzednia data ważności zbioru buforowego
		1687	Nowa data ważności zbioru buforowego	Char(7)	Nowa data ważności zbioru buforowego
		1694	Data utworzenia zbioru buforowego (UTC)	Char(7)	Data utworzenia zbioru buforowego (jest to ta sama data co data utworzenia zbioru buforowego (pozycja 1097), jednak w formacie czasu UTC).
		1701	Godzina utworzenia zbioru buforowego (UTC)	Char(6)	Godzina utworzenia zbioru buforowego (jest to ta sama godzina co godzina utworzenia zbioru buforowego (pozycja 1104), jednak w formacie czasu UTC).
[1] Gdy typ pozycji to I (drukowanie wstawiane), wtedy to pole jest puste.					

Pozycje kroniki SG (Sygnały asynchroniczne)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki SG (Sygnały asynchroniczne).

Tabela 211. Pozycje kroniki SG (Sygnały asynchroniczne). Zbiór opisów pól QASYSGJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583.

Tabela 211. Pozycje kroniki SG (Sygnały asynchroniczne) (kontynuacja). Zbiór opisów pól QASYSGJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Przetworzono asynchroniczny sygnał systemu i5/OS **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 przetwarzania **U** Koniec żądania
	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 czasu w momencie utworzenia sygnału. **Uwaga:** Funkcji API QWCCVTDT można użyć do przekształcenia datownika *DTS na inne formaty.

Pozycje kroniki SK (Połączenia SSL)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki SK (Połączenia SSL).

Tabela 212. Pozycje kroniki SK (Połączenia SSL). Zbiór opisów pól QASYSKJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583.
	224	610	Typ pozycji	Char(1)	**A** Akceptowanie **C** Połączenie **D** Przypisano adres DHCP **F** Filtrowana poczta **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.
	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] Jeśli typ wpisu to D, pole to zawiera adres IP przypisany klientowi wysyłającemu żądanie przez serwer DHCP.

[3] Te pola obsługują jedynie adresy IPv4.

Pozycje kroniki SM (Zmiana zarządzania systemami)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki SM (Zmiana zarządzania systemami).

Tabela 213. Pozycje kroniki SM (Zmiana zarządzania systemami). Zbiór opisów pól QASYSMJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
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 odtworzenia ścieżek dostępu zostały zmienione
157	225	611	Typ dostępu	Char(1)	**A** Dodanie (Add) **C** Zmiana (Change) **D** Usunięcie (Delete) **R** Usuwanie (Remove) **S** Wyświetlanie (Display) **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
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

Tabela 213. Pozycje kroniki SM (Zmiana zarządzania systemami) (kontynuacja). Zbiór opisów pól QASYSMJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
227	295	681	Podzbiór zbioru sieciowego	Char(10)	Nazwa podzbioru zbioru sieciowego
237	305	691	Numer zbioru sieciowego	Nieupakowane (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

Pozycje kroniki SO (Działania na informacjach o użytkowniku dotyczących bezpieczeństwa serwera)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki SO (Działania na informacjach o użytkowniku dotyczących bezpieczeństwa serwera).

Tabela 214. Pozycje kroniki SO (Działania na informacjach o użytkowniku dotyczących bezpieczeństwa serwera). Zbiór opisów pól QASYSOJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
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. **T** Pozycja jest pozycją uwierzytelniania serwera.

Tabela 214. Pozycje kroniki SO (Działania na informacjach o użytkowniku dotyczących bezpieczeństwa serwera) (kontynuacja). Zbiór opisów pól QASYSOJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	236	622	Przechowywanie hasła	Char(1)	**N** Hasło nie jest przechowywane **S** Brak zmiany **T** 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.

Pozycje kroniki ST (Działanie narzędzi serwisowych)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki ST (Działanie narzędzi serwisowych).

Tabela 215. Pozycje kroniki ST (Działanie narzędzi serwisowych). Zbiór opisów pól QASYSTJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
156	224	610	Typ pozycji	Char(1)	Typ pozycji **A** Rekord usługi

Tabela 215. Pozycje kroniki ST (Działanie narzędzi serwisowych) (kontynuacja). Zbiór opisów pól QASYSTJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis	
JE	**J4**	**J5**				
157	225	611	Narzędzie serwisowe	Char(2)	Typ pozycji.	
					AN	ANZJVM
					AR	Śledzenie diagnostyczne ARM (parz komenda QShell ARMSRV)
					CD	QTACTLDV, QTADMPDV
					CE	QWTCTLTR
					CS	STRCPYSCN
					CT	DMPCLUTRC
					DC	DLTCMNTRC
					DD	DMPDLO
					DF	QWTDMPFR, QWTDMPLF
					DI	QSCDIRD
					DJ	DMPJVM, QPYRTJVM
					DM	DMPMEMINF
					DO	DMPOBJ
					DS	DMPSYSOBJ, QTADMPTS, QTADMPDV, QWTDMPLF
					DU	DMPUSRPRF
					DW	STRDW, ENDDW, ADDDWDFN, RMVDWDFN
					EC	ENDCMNTRC
					ER	ENDRMTSPT
					GS	QSMGSSTD
					HD	QYHCHCOP (DASD)
					HL	QYHCHCOP (LPAR)
					JW	STRJW, ENDJW, ADDJWDFN, RMVJWDFN
					LC	Utworzona tabela EPT
					LD	Usunięta tabela EPT
					LE	Nastąpiła zmiana tabeli EPT dla zadania
					LF	Uporządkowano tabelę EPT systemu
					LG	Punkty wejścia tabeli EPT zostały zmienione
					LH	Porównana tabela EPT

Tabela 215. Pozycje kroniki ST (Działanie narzędzi serwisowych) (kontynuacja). Zbiór opisów pól QASYSTJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis	
JE	**J4**	**J5**				
					LI	Wyświetlone punkty wejścia tabeli EPT
					MC	QWTMAINT (zmiana)
					MD	QWTMAINT (zrzut)
					MP	Zakończenie zadania systemowego
					MQ	Zrestartowanie zadania systemowego
					OP	Konsola Operations console
					PC	PRTCMNTRC
					PE	PRTERRLOG, QTADMPDV
					PI	PRTINTDTA, QTADMPDV
					PS	QP0FPTOS
					SC	STRCMNTRC
					SE	QWTSETTR
					SF	QWCCDSIC, QWVRCSTK (Wyświetlenie wpisu stosu wewnętrznego)
					SJ	STRSRVJOB
					SN	QPZSYNC
					SR	STRRMTSPT
					SS	QFPHPSF
					ST	STRSST
					SV	QSRSRV
					TA	TRCTCPAPP
					TC	TRCCNN (podano *FORMAT)
					TE	ENDTRC, ENDPEX, TRCJOB(określone *OFF lub *END)
					TI	TRCINT lub TRCCNN z SET(*ON), SET(*OFF) lub SET(*END)
					TO	QTOBSRV
					TQ	QWCTMQTM
					TS	STRTRC, STRPEX, TRCJOB(określony *ON)
					UD	QTAUPDDV
					WE	ENDWCH, QSCEWCH
					WS	STRWCH, QSCSWCH
					WT	WRKTRC
					WW	WRKWCH
159	227	613	Nazwa obiektu	Char(10)	Nazwa obiektu, do którego uzyskano dostęp	

Tabela 215. Pozycje kroniki ST (Działanie narzędzi serwisowych) (kontynuacja). Zbiór opisów pól QASYSTJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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	Nieupakowane (6,0)	Trzecia część pełnej nazwy zadania
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[8]	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. **A**[6] Aktywuj **D**[6] Dezaktywuj **T**[7] Zbieranie danych śledzenia zostało uruchomione **N**[7] Zbieranie danych śledzenia zostało zatrzymane, a informacje śledzenia zostały zapisane do zbioru buforowego **U**[7] 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

Tabela 215. Pozycje kroniki ST (Działanie narzędzi serwisowych) (kontynuacja). Zbiór opisów pól QASYSTJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
		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
		907	Typ konsoli [4]	Char(10)	Typ konsoli. Możliwe wartości to: • *DIRECT • *LAN • *HMC
		917	Działanie konsoli [4]	Char(10)	Działanie konsoli. Możliwe wartości to: • *RECOVERY • *TAKEOVER
		927	Rodzina adresów [4]	Char(10)	Rodzina adresów. • *IPv4 • *IPv6
		937	Poprzedni adres IP [4]	Char(46)	Adres IP poprzedniego urządzenia konsoli dla *LAN.
		938	Poprzedni identyfikator urządzenia [4]	Char(10)	Identyfikator narzędzi serwisowych poprzedniego urządzenia konsoli dla *LAN.
		993	Bieżący adres IP [4]	Char(46)	Bieżący adres IP urządzenia konsoli dla *LAN.
		1039	Bieżący identyfikator urządzenia [4]	Char(10)	Identyfikator narzędzi serwisowych bieżącego urządzenia konsoli dla *LAN.
		1049	Sesja podglądu[5]	Char(10)	Identyfikator sesji podglądu.
		1059	Pozycja[9]	Char(10)	Nazwa zmienionego punktu wejścia w tabeli punktów wejścia.
		1069	Obiekt pokrewny[10]	Char(10)	Nazwa obiektu pokrewnego. • Dla wartości LC w polu Narzędzie serwisowe to pole zawiera nazwę podstawowej tabeli punktów wejścia. • Dla wartości LG w polu Narzędzie serwisowe to pole zawiera nazwę programu wymiany. • Dla wartości LH w polu Narzędzie serwisowe to pole zawiera nazwę porównania tabeli punktów wejścia.

Tabela 215. Pozycje kroniki ST (Działanie narzędzi serwisowych) (kontynuacja). Zbiór opisów pól QASYSTJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	J4	J5			
		1079	Biblioteka obiektów pokrewnych[10]	Char(10)	Nazwa biblioteki obiektów pokrewnych. • Dla wartości LC w polu Narzędzie serwisowe to pole zawiera nazwę biblioteki podstawowej tabeli punktów wejścia. • Dla wartości LG w polu Narzędzie serwisowe to pole zawiera nazwę biblioteki programu wymiany. • Dla wartości LH w polu Narzędzie serwisowe to pole zawiera nazwę biblioteki porównania tabeli punktów wejścia.

[1] To pole jest wykorzystywane tylko wtedy, gdy wartość w polu Narzędzie serwisowe (pozycja 661) to CE.

[2] To pole jest wykorzystywane tylko wtedy, gdy wartość w polu Narzędzie serwisowe (pozycja 661) to AR lub TA.

[3] To pole jest wykorzystywane tylko wtedy, gdy wartość w polu Narzędzie serwisowe (pozycja 661) to ST lub OP.

[4] To pole jest wykorzystywane tylko wtedy, gdy wartość w polu Narzędzie serwisowe (pozycja 661) to OP.

[5] Pole to wykorzystywane jest wówczas, gdy typ pozycji (pozycja 661) to WS lub WE.

[6] To pole jest wykorzystywane wtedy, gdy wartość w polu Narzędzie serwisowe (pozycja 661) to AR.

[7] To pole jest wykorzystywane tylko wtedy, gdy wartość w polu Narzędzie serwisowe (pozycja 661) to TA.

[8] Kiedy wartość w polu Narzędzie serwisowe (pozycja 611) to GS, ścieżka folderu będzie zawierać 30 znakową nazwę komendy zaawansowanej analizy.

[9] To pole jest wykorzystywane tylko wtedy, gdy wartość w polu Narzędzie serwisowe (pozycja 661) to LG.

[10] To pole jest wykorzystywane tylko wtedy, gdy wartość w polu Narzędzie serwisowe (pozycja 661) to LC, LG lub LH.

Pozycje kroniki SV (Działanie na wartości systemowej)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki SV (Działanie na wartości systemowej).

Tabela 216. Pozycje kroniki SV (Działanie na wartości systemowej). Zbiór opisów pól QASYSVJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	J4	J5			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.

Tabela 216. Pozycje kroniki SV (Działanie na wartości systemowej) (kontynuacja). Zbiór opisów pól QASYSVJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
156	224	610	Typ pozycji	Char(1)	Typ pozycji. **A** Zmiana wartości systemowych **B** Zmiana atrybutów usługi **C** Zmiana zegara systemowego **D** Ustawienie czasu na czas uniwersalny (UTC) **E** Zmiana opcji **F** Zmiana systemowego atrybutu kroniki
157	225	611	Wartość systemowa lub atrybut usługi	Char(10)	**JRNRCVCNT** Zmieniona wartości licznika odzyskiwania kroniki **MAXCCHWAIT** Zmieniony maksymalny czas oczekiwania pamięci podręcznej kroniki **QINPIDCO** Zmiana bieżącej opcji konfiguracji instalowania dysku przez interfejs API QINPIDCO.
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 przed jego zmianą.
		1621	Rozszerzenie nowej wartości kontynuowanej	Char(1000)	Druga kontynuacja wartości, na jaką zmieniono wartość systemową lub atrybut usługi.
		2621	Rozszerzenie starej wartości kontynuowanej	Char(1000)	Druga kontynuacja zmienionej wartości dla wartości systemowej lub atrybutu usługi przed jego zmianą.

Pozycje kroniki VA (Zmiana listy kontroli dostępu)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki VA (Zmiana listy kontroli dostępu).

Tabela 217. Pozycje kroniki VA (Zmiana listy kontroli dostępu). Zbiór opisów pól QASYVAJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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	Nieupakowane (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 (Add) **C** Modyfikowanie **D** Usuwanie
198	266	652	Nazwa zasobu	Char(260)	Nazwa zasobu, który ma być zmieniony.

Pozycje kroniki VC (Uruchomienie i zakończenie połączenia)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki VC (Uruchomienie i zakończenie połączenia).

Tabela 218. Pozycje kroniki VC (Uruchomienie i zakończenie połączenia). Zbiór opisów pól QASYVCJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.

Tabela 218. Pozycje kroniki VC (Uruchomienie i zakończenie połączenia) (kontynuacja). Zbiór opisów pól QASYVCJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
156	224	610	Działanie połączenia	Char(1)	Działanie połączenia, które nastąpiło. **S** Uruchomienie (Start) **E** Zakończenie (End) **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	Nieupakowane (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)	Powód odrzucenia połączenia: **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.

Pozycje kroniki VF (Zamknięcie plików serwera)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki VF (Zamknięcie plików serwera).

Tabela 219. Pozycje kroniki VF (Zamknięcie plików serwera). Zbiór opisów pól QASYVFJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.

Tabela 219. Pozycje kroniki VF (Zamknięcie plików serwera) (kontynuacja). Zbiór opisów pól QASYVFJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
156	224	610	Przyczyna zamknięcia	Char(1)	Powód 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.
173	241	627	Godzina serwera	Nieupakowane (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.

Pozycje kroniki VL (Przekroczenie limitu konta)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki VL (Przekroczenie limitu konta).

Tabela 220. Pozycje kroniki VL (Przekroczenie limitu konta). Zbiór opisów pól QASYVLJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
156	224	610	Przyczyna	Char(1)	Powód 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.

Tabela 220. Pozycje kroniki VL (Przekroczenie limitu konta) (kontynuacja). Zbiór opisów pól QASYVLJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
167	235	621	Data serwera	Char(6)	Data zaprotokołowania zdarzenia na serwerze sieciowym.
173	241	627	Godzina serwera	Nieupakowane (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.

Pozycje kroniki VN (Logowanie i wylogowanie z sieci)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki VN (Logowanie i wylogowanie z sieci).

Tabela 221. Pozycje kroniki VN (Logowanie i wylogowanie z sieci). Zbiór opisów pól QASYVNJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
156	224	610	Typ logowania	Char(1)	Typ zdarzenia, które wystąpiło: **F** Żądanie wylogowania **O** Żądanie logowania **R** Logowanie odrzucono
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	Nieupakowane (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

Tabela 221. Pozycje kroniki VN (Logowanie i wylogowanie z sieci) (kontynuacja). Zbiór opisów pól QASYVNJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
198	266	652	Przyczyna odrzucenia	Char(1)	Powód odrzucenia próby logowania: **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

Pozycje kroniki VO (Lista sprawdzania)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki VO (Lista sprawdzania).

Tabela 222. Pozycje kroniki VO (Lista sprawdzania). Zbiór opisów pól QASYVOJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583.
	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
	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 sprawdzania.

Tabela 222. Pozycje kroniki VO (Lista sprawdzania) (kontynuacja). Zbiór opisów pól QASYVOJ4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	246	632	Zaszyfrowane dane	Char(1)	Wartość danych do zaszyfrowania. **T** Dane do zaszyfrowania zostały podane w żądaniu. **N** W żądaniu nie określono danych do szyfrowania.
	247	633	Dane pozycji	Char(1)	Wartość danych pozycji. **T** 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

Pozycje kroniki VP (Błąd hasła sieciowego)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki VP (Błąd hasła sieciowego).

Tabela 223. Pozycje kroniki VP (Błąd hasła sieciowego). Zbiór opisów pól QASYVPJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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	Nieupakowane (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.

Pozycje kroniki VR (Dostęp do zasobu sieciowego)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki VR (Dostęp do zasobu sieciowego).

Tabela 224. Pozycje kroniki VR (Dostęp do zasobu sieciowego). Zbiór opisów pól QASYVRJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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	Nieupakowane (6,0)	Godzina zaprotokołowania zdarzenia na serwerze sieciowym.
179	247	633	Nazwa komputera	Char(8)	Nazwa komputera żądającego zasobu.

Tabela 224. Pozycje kroniki VR (Dostęp do zasobu sieciowego) (kontynuacja). Zbiór opisów pól QASYVRJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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.

Pozycje kroniki VS (Sesja serwera)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki VS (Sesja serwera).

Tabela 225. Pozycje kroniki VS (Sesja serwera). Zbiór opisów pól QASYVSJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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	Nieupakowane (6,0)	Godzina zaprotokołowania zdarzenia na serwerze sieciowym.
179	247	633	Nazwa komputera	Char(8)	Nazwa komputera żądającego sesji.

Tabela 225. Pozycje kroniki VS (Sesja serwera) (kontynuacja). Zbiór opisów pól QASYVSJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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

Pozycje kroniki VU (Zmiana profilu sieciowego)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki VU (Zmiana profilu sieciowego).

Tabela 226. Pozycje kroniki VU (Zmiana profilu sieciowego). Zbiór opisów pól QASYVUJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
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	Nieupakowane (6,0)	Godzina zaprotokołowania zdarzenia na serwerze sieciowym.
179	247	633	Nazwa komputera	Char(8)	Nazwa komputera żądającego zmiany profilu użytkownika.

Tabela 226. Pozycje kroniki VU (Zmiana profilu sieciowego) (kontynuacja). Zbiór opisów pól QASYVUJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
187	255	641	Użytkownik	Char(10)	Nazwa użytkownika żądającego zmiany profilu użytkownika.
197	265	651	Działanie	Char(1)	Żądane działanie: **A** Dodanie (Add) **C** Zmiana (Change) **D** Usuwanie **P** Niepoprawne hasło
198	266	652	Nazwa zasobu	Char(260)	Nazwa zasobu.

Pozycje kroniki VV (Zmiana statusu usługi)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki VV (Zmiana statusu usługi).

Tabela 227. Pozycje kroniki VV (Zmiana statusu usługi). Zbiór opisów pól QASYVVJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
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	Nieupakowane (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.

Tabela 227. Pozycje kroniki VV (Zmiana statusu usługi) (kontynuacja). Zbiór opisów pól QASYVVJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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.
290	358	744	Usługa	Char(20)	Usługa, która została zmieniona.

Pozycje kroniki X0 (Uwierzytelnianie sieciowe)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki X0 (Uwierzytelnianie sieciowe).

Tabela 228. Pozycje kroniki X0 (Uwierzytelnianie sieciowe). Zbiór opisów pól QASYX0JE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.

Tabela 228. Pozycje kroniki X0 (Uwierzytelnianie sieciowe) (kontynuacja). Zbiór opisów pól QASYX0JE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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 228. Pozycje kroniki X0 (Uwierzytelnianie sieciowe) (kontynuacja). Zbiór opisów pól QASYX0JE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	539	925	Indykator zaszyfrowanych adresów	Char(1)	Indykator zaszyfrowanych adresów IP **T** 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) **T** 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) **T** użytkownik serwera zakończony **N** użytkownik serwera nie zakończony **X** nie udostępniono

Tabela 228. Pozycje kroniki X0 (Uwierzytelnianie sieciowe) (kontynuacja). Zbiór opisów pól QASYX0JE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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)
	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) **T** 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) **T** 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) **T** 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

Tabela 228. Pozycje kroniki X0 (Uwierzytelnianie sieciowe) (kontynuacja). Zbiór opisów pól QASYX0JE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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 **T** użytkownik lokalny zakończony **N** użytkownik lokalny nie zakończony **X** nie udostępniono
	3198	3584	Użytkownik lokalny GSS	Char(512)	Użytkownik lokalny GSS
	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 **T** użytkownik zdalny zakończony **N** użytkownik zdalny nie zakończony **X** nie udostępniono
	3717	4103	Użytkownik zdalny GSS	Char(512)	Użytkownik zdalny GSS

Pozycje kroniki X1 (Znacznik tożsamości)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki X1 (Znacznik tożsamości).

Tabela 229. Pozycje kroniki X1 (Znacznik tożsamości). Zbiór opisów pól QASYX1JE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
		1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
		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

Tabela 229. Pozycje kroniki X1 (Znacznik tożsamości) (kontynuacja). Zbiór opisów pól QASYX1JE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
		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.
		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.

Tabela 229. Pozycje kroniki X1 (Znacznik tożsamości) (kontynuacja). Zbiór opisów pól QASYX1JE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
		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. Pole to zostanie obcięte, jeśli ciąg przekracza jego długość. 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.
		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.

Pozycje kroniki XD (Rozszerzenie serwera katalogów)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki XD (Rozszerzenie serwera katalogów).

Tabela 230. Pozycje kroniki XD (Rozszerzenie serwera katalogów). Zbiór opisów pól QASYXDJ5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
		1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
		610	Typ pozycji	Char(1)	Typ pozycji: **G** Nazwy grup. Pola od 1 do 5 zawierają nazwy grup.
		611	Odniesienie	Char(36)	Łańcuch odniesienia służący do korelacji tej pozycji z pozycją DI używającą tych grup. Jeśli wiele żądań LDAP używa tego samego zestawu grup, więcej niż jedna pozycja DI może odnosić się do tej pozycji XD.
		647	Zastrzeżone	Char(100)	
		747	Identyfikator CCSID pola 1	Bin(5)	Wartość identyfikatora CCSID dla pola 1.
		751	Długość pola 1	Bin(4)	Długość danych w polu 1.
		753	Pole 1	Char(2002)	Dane pola 1 Dla pozycji typu G to pole będzie zawierać nazwę grupy z asercji przypisania do grupy.
		2755	Identyfikator CCSID pola 2	Bin(5)	Wartość identyfikatora CCSID dla pola 2.
		2759	Długość pola 2	Bin(4)	Długość danych w polu 2.
		2761	Pole 2	Char(2002)	Dane pola 2 Dla pozycji typu G to pole będzie zawierać nazwę grupy z asercji przypisania do grupy.
		4763	Identyfikator CCSID pola 3	Bin(5)	Wartość identyfikatora CCSID dla pola 3.
		4767	Długość pola 3	Bin(4)	Długość danych w polu 3.
		4769	Pole 3	Char(2002)	Dane pola 3 Dla pozycji typu G to pole będzie zawierać nazwę grupy z asercji przypisania do grupy.
		6771	Identyfikator CCSID pola 4	Bin(5)	Wartość identyfikatora CCSID dla pola 4.
		6775	Długość pola 4	Bin(4)	Długość danych w polu 4.
		6777	Pole 4	Char(2002)	Dane pola 4 Dla pozycji typu G to pole będzie zawierać nazwę grupy z asercji przypisania do grupy.
		8779	Identyfikator CCSID pola 5	Bin(5)	Wartość identyfikatora CCSID dla pola 5.
		8783	Długość pola 5	Bin(4)	Długość danych w polu 5.

Tabela 230. Pozycje kroniki XD (Rozszerzenie serwera katalogów) (kontynuacja). Zbiór opisów pól QASYXDJ5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
		8785	Pole 5	Char(2002)	Dane pola 5 Dla pozycji typu G to pole będzie zawierać nazwę grupy z asercji przypisania do grupy.

Pozycje kroniki YC (Zmiana obiektu DLO)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki YC (Zmiana obiektu DLO).

Tabela 231. Pozycje kroniki YC (Zmiana obiektu DLO). Zbiór opisów pól QASYYCJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)" na stronie 581,"Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)" na stronie 583 i "Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)" na stronie 585.
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 "Kody liczbowe dla typów dostępu" na stronie 732.

Pozycje kroniki YR (Odczyt obiektu DLO)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki YR (Odczyt obiektu DLO).

Tabela 232. Pozycje kroniki YR (Odczyt obiektu DLO). Zbiór opisów pól QASYYRJE/J4/J5

Pozycje (Offsets)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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 “Kody liczbowe dla typów dostępu” na stronie 732.					

Pozycje kroniki ZC (Zmiana obiektu)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki ZC (Zmiana obiektu).

Tabela 233. Pozycje kroniki ZC (Zmiana obiektu). Zbiór opisów pól QASYZCJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
156	224	610	Typ pozycji	Char(1)	Dostęp do obiektu **C** Zmiana obiektu **U** Aktualizowanie dostępu otwartego do obiektu

Tabela 233. Pozycje kroniki ZC (Zmiana obiektu) (kontynuacja). Zbiór opisów pól QASYZCJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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 233. Pozycje kroniki ZC (Zmiana obiektu) (kontynuacja). Zbiór opisów pól QASYZCJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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. Kiedy typem obiektu jest obiekt zintegrowanego systemu plików, to pole zawiera dodatkowe informacje identyfikujące żądanie zmiany. Możliwe wartości znajdują się w pliku włączanym QP0LJRNL.H biblioteki QSYSINC.
238			(Obszar zastrzeżony)	Char(20)	

Tabela 233. Pozycje kroniki ZC (Zmiana obiektu) (kontynuacja). Zbiór opisów pól QASYZCJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	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 kodowanego zestawu znaków dla nazwy obiektu.
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	ID zbioru obiektu[2, 4]	Char(16)	Identyfikator zbioru dla obiektu.
302	370	756	Nazwa obiektu[2]	Char(512)	Nazwa obiektu.
	882	1268	ID zbioru obiektu	Char(16)	Identyfikator zbioru dla 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 nazwy ścieżki.
	917	1303	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.
	919	1305	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	922	1308	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.
	924	1310	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.

Tabela 233. Pozycje kroniki ZC (Zmiana obiektu) (kontynuacja). Zbiór opisów pól QASYZCJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
	925	1311	Identyfikator zbioru w katalogu względnym[4]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[4]
	941	1327	Nazwa ścieżki[5]	Char(5002)	Nazwa ścieżki obiektu.

[1] Listę kodów dla typów dostępu zawiera “Kody liczbowe dla typów dostępu” na stronie 732.

[2] Te pola są używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanych przez użytkownika.

[3] Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.

[4] Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.

[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 puli ASP obiektu.

Pozycje kroniki ZR (Odczyt obiektu)

W poniższej tabeli zamieszczono informacje na temat formatu pozycji kroniki ZR (Odczyt obiektu).

Tabela 234. Pozycje kroniki ZR (Odczyt obiektu). Zbiór opisów pól QASYZRJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
1	1	1			Pola nagłówka wspólne dla wszystkich typów pozycji. Informacje na temat listy pól zawiera sekcja “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE5 (*TYPE5)” na stronie 581,“Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE4 (*TYPE4)” na stronie 583 i “Standardowe pola nagłówków pozycji kroniki kontroli Formatu rekordu QJORDJE2 (*TYPE2)” na stronie 585.
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 234. Pozycje kroniki ZR (Odczyt obiektu) (kontynuacja). Zbiór opisów pól QASYZRJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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. **T** 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 kodowanego zestawu znaków dla nazwy obiektu.

Tabela 234. Pozycje kroniki ZR (Odczyt obiektu) (kontynuacja). Zbiór opisów pól QASYZRJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
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	ID zbioru obiektu[2,3]	Char(16)	Identyfikator zbioru dla obiektu.
302	370	756	Nazwa obiektu[2]	Char(512)	Nazwa obiektu.
	882	1268	ID zbioru obiektu	Char(16)	Identyfikator zbioru dla 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 nazwy ścieżki.
	917	1303	Identyfikator kraju lub regionu nazwy ścieżki	Char(2)	Identyfikator kraju lub regionu dla nazwy ścieżki.
	919	1305	Identyfikator języka nazwy ścieżki	Char(3)	Identyfikator języka dla nazwy ścieżki.
	922	1308	Długość nazwy ścieżki	Binary(4)	Długość nazwy ścieżki.
	924	1310	Indykator nazwy ścieżki	Char(1)	Indykator nazwy ścieżki: **T** Pole Nazwa ścieżki zawiera pełną, bezwzględną nazwę ścieżki obiektu. **N** Pole Nazwa ścieżki zawiera względną ścieżkę dostępu do obiektu zamiast ścieżki bezwzględnej. Pole identyfikatora zbioru w katalogu względnym jest poprawne i można skorzystać z niego, aby utworzyć bezwzględną nazwę ścieżki, w odniesieniu do względnej nazwy ścieżki.
	925	1311	Identyfikator zbioru w katalogu względnym[4]	Char(16)	Jeśli pole Indykator nazwy ścieżki to N, pole to zawiera identyfikator zbioru katalogu zawierającego obiekt określony w polu Nazwa ścieżki. W przeciwnym razie zawiera ono zera szesnastkowe.[4]
	941	1327	Nazwa ścieżki[5]	Char(5002)	Nazwa ścieżki obiektu.

Tabela 234. Pozycje kroniki ZR (Odczyt obiektu) (kontynuacja). Zbiór opisów pól QASYZRJE/J4/J5

Pozycja (Offset)			Pole	Format	Opis
JE	**J4**	**J5**			
[1]	Listę kodów dla typów dostępu zawiera “Kody liczbowe dla typów dostępu”.				
[2]	Te pola są używane tylko dla obiektów w systemach plików: głównym (/), QOpenSys i zdefiniowanych przez użytkownika.				
[3]	Identyfikator, który ma ustawiony ostatni lewy bit i resztę bitów zerowych wskazuje, że identyfikator nie jest ustawiony.				
[4]	Jeśli pole Indykator nazwy ścieżki to N, ale identyfikator zbioru katalogu względnego składa się z zer szesnastkowych, to podczas określania nazwy ścieżki wystąpił błąd.				
[5]	Jest to pole o zmiennej długości. Dwa pierwsze bajty zawierają długość nazwy ścieżki.				

Kody liczbowe dla typów dostępu

Poniższa tabela 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 235. 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)

Tabela 235. Kody liczbowe dla typów dostępu (kontynuacja)

Kod	Typ dostępu	Kod	Typ dostępu	Kod	Typ dostępu
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)
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 bezpieczeństwa

Do skonfigurowania bezpieczeństwa systemu służą cztery narzędzia bezpieczeństwa: menu Narzędzia bezpieczeństwa (Security Tools - SECTOOLS) i Wprowadzenie raportów dotyczących zabezpieczeń do zadania wsadowego lub zaplanowanie ich (Submit or Schedule Security Reports to Batch - SECBATCH) oraz komendy Konfigurowanie bezpieczeństwa systemu (Configure System Security - CFGSYSSEC) i Odwołanie uprawnień publicznych (Revoke Public Authority - RVKPUBAUT).

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 bezpieczeństwa

Menu Narzędzia bezpieczeństwa (Security Tools - SECTOOLS) upraszcza zarządzanie bezpieczeństwem systemu oraz kontrolę nad nim dzięki dużej liczbie udostępnianych opcji i komend.

Rysunek przedstawia część menu SECTOOLS związaną z profilami użytkowników.

Aby uzyskać dostęp do tego menu, należy wpisać 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
     9. Drukowanie wewnętrznych danych profilu
```

Tabela 236 opisuje wymienione opcje menu i powiązane z nimi komendy:

Tabela 236. Komendy narzędzi dla profili użytkowników

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]

Tabela 236. Komendy narzędzi dla profili użytkowników (kontynuacja)

Opcja menu[1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
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]
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 (Display Activation Schedule) służy do wyświetlania lub drukowania informacji o harmonogramie aktywowania i wyłączania określonych profili użytkowników. Harmonogram można utworzyć komendą 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]

Tabela 236. Komendy narzędzi dla profili użytkowników (kontynuacja)

Opcja menu[1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
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]
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 237 opisuje opcje menu i powiązane z nimi komendy służące do kontroli ochrony:

Tabela 237. Komendy narzędzi dla kontroli bezpieczeństwa

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:** Jeśli kontrola ma zostać skonfigurowana za pomocą narzędzi ochrony, należy pamiętać, aby zaplanować zarządzanie odbiorcami kroniki kontroli. W przeciwnym przypadku wkrótce mogą 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.	
12	CPYAUDJRNE	Komenda Kopiowanie pozycji kroniki służy do kopiowania pozycji z kroniki kontroli ochrony do zbioru wyjściowego.	QASYxxJ5[2]

Tabela 237. Komendy narzędzi dla kontroli bezpieczeństwa (kontynuacja)

Opcja menu[1]	Nazwa komendy	Opis	Użyty zbiór bazy danych

[1] Są to opcje z menu SECTOOLS.

[2] xx to dwuznakowy typ pozycji kroniki. Na przykład modelowy plik wyjściowy pozycji kroniki AE to QSYS/QASYAEJ5. Modelowe pliki wyjściowe są opisane w sekcji Dodatek F, “Układ pozycji kroniki kontroli”, na stronie 581 niniejszej kolekcji tematów.

Jak używać menu Zadania wsadowe zabezpieczeń

Menu Zadania wsadowe zabezpieczeń pozwala na wprowadzenie do kolejki zadań jednego lub kilku raportów narzędzi zabezpieczeń, aby mogły zostać uruchomione później jako zadanie wsadowe. Można również wprowadzić do harmonogramu dowolny raport narzędzi zabezpieczeń jako zadanie wsadowe, które zostanie wykonane raz lub będzie wykonywane zgodnie z harmonogramem w ustalonych odstępach czasu. Przykłady zamieszczone w tej sekcji pokazują, w jaki sposób używać menu Zadania wsadowe zabezpieczeń.

Oto 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 menu pokaże się ekran Wprowadzania zadania (SBMJOB), jak przedstawiono w poniższym przykładzie:

```
                            Wprowadzenie zadania (Submit Job - SBMJOB)
Wpisz opcje i naciśnij klawisz Enter.

Komenda do uruchomienia  . . . . > 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 katalogu
```

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 opcje i naciśnij klawisz Enter.

Nazwa zadania  . . . . . _____                    Nazwa, *JOBD
Komenda do uruchomienia  . . . . > 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      Czas, *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 zadań wsadowych bezpieczeństwa

W tej tabeli opisane są opcje menu i powiązane komendy dla raportów bezpieczeństwa.

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 238. Komendy raportów bezpieczeństwa

Opcje 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[6]	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 238. Komendy raportów bezpieczeństwa (kontynuacja)

Opcje menu[1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
15, 54	PRTJOBDAUT	Komenda Drukowanie uprawnień opisu zadania (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 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. Raport usunięć zawiera użytkowników, których uprawnienia do obiektu zostały zmienione od ostatniego drukowania raportu.	QPVxxxxxx[5]

Tabela 238. Komendy raportów bezpieczeństwa (kontynuacja)

Opcje menu[1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
24, 63	PRTQAUT	Komenda Drukowanie uprawnień dla kolejki (Print Queue Authority) służy do drukowania ustawień bezpieczeństwa 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 238. Komendy raportów bezpieczeństwa (kontynuacja)

Opcje 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.	

[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. Opis modelowych plików wyjściowych zawiera Dodatek F, “Układ pozycji kroniki kontroli”, na stronie 581 w tej kolekcji tematów.

[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.

[6] Komenda DSPAUDJRNE nie przetwarza wszystkich typów rekordów kontroli bezpieczeństwa i nie wyświetla wszystkich pól dla rekordów, które obsługuje.

Komendy do konfigurowania bezpieczeństwa

Tabela zawiera opis komend, za pomocą których można skonfigurować bezpieczeństwo w systemie. komendy te znajdują w menu SECTOOLS.

Tabela 239. Komendy do konfigurowania 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 bezpieczeństwa systemu (Configure System Security)” 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 “Opis działania komendy Odwołanie uprawnień publicznych (Revoke Public Authority)” na stronie 747 zawiera listę czynności wykonywanych przez komendę RVKPUBAUT.	
[1] Są to opcje z menu SECTOOLS.			

Wartości ustawiane za pomocą komendy Konfigurowanie bezpieczeństwa systemu (Configure System Security)

W tej tabeli są wyświetlane wartości systemowe ustawiane podczas uruchamiania komendy Konfigurowanie bezpieczeństwa systemu (Configure System Security - CFGSYSSEC), która powoduje uruchomienie programu o nazwie QSYS/QSECCFGS.

Tabela 240. Wartości ustawiane przez komendę 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 czasu, po którym system podejmie działania dla 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

Tabela 240. Wartości ustawiane przez komendę CFGSYSSEC (kontynuacja)

Nazwa wartości systemowej	Ustawienie	Opis wartości systemowej
QMAXSGNACN	3 (Oba)	Określa, czy system wyłącza stację roboczą lub profil użytkownika, gdy osiągnięty zostanie limit wartości QMAXSIGN.
QPWDEXPITV	60	Określa częstotliwość zmiany haseł użytkowników
QPWDMINLEN	6 (Patrz uwagi 3 i 5)	Określa minimalną długość hasła
QPWDMAXLEN	8 (Patrz uwagi 4 i 5)	Określa maksymalną długość hasła
QPWDPOSDIF	1 (Tak) (Patrz uwaga 5)	Określa, czy każda pozycja nowego hasła musi różnić się od takiej samej pozycji poprzedniego hasła
QPWDLMTCHR	Patrz uwagi 2 i 5	Określa znaki, które są niedozwolone w haśle
QPWDLMTAJC	1 (Tak) (Patrz uwaga 5)	Określa, czy niedozwolone są przylegające numery w haśle
QPWDLMTREP	2 (Nie mogą być kolejno powtarzane) (Patrz uwaga 5)	Określa, czy powtarzanie znaków w haśle jest zabronione
QPWDRQDDGT	1 (Tak) (Patrz uwaga 5)	Określa, czy hasło powinno zawierać przynajmniej jedną liczbę
QPWDRQDDIF	1 (32 unikalne hasła)	Określa, ile unikalnych haseł należy podać, przed ponownym powtórzeniem hasła
QPWDRULES	• *MINLEN6 • *MAXLEN10 • *LMTSAMPOS • *LMTPRFNAME • *DGTMIN1 • *CHRLMTAJC • *DGTLMTAJC • *DGTLMTFST • *DGTLMTLST • *SPCCHRLMTAJC • *SPCCHRLMTFST • *SPCCHRLMTLST (patrz uwaga 6)	Reguły tworzenia poprawnego hasła.
QPWDVLDPGM	*NONE	Określa program użytkownika do obsługi wyjścia, który system wywołuje w celu sprawdzenia haseł
QRMTSIGN	*FRCSIGNON	Określa w jaki sposób system obsługuje próby zdalnego wpisania się (przez tranzyt lub TELNET).
QRMTSVRATR	0 (Wyłączone)	Umożliwia zdalne analizowanie systemu.
QSECURITY	50	Wymuszony poziom ochrony
QVFYOBJRST	3	Sprawdzenie obiektu podczas odtwarzania.

Tabela 240. Wartości ustawiane przez komendę CFGSYSSEC (kontynuacja)

Nazwa wartości systemowej	Ustawienie	Opis wartości systemowej
Uwagi: 1. Jeśli w systemie wartość QSECURITY jest ustawiona na 30 lub mniej, przed zmianą na wyższy poziom bezpieczeństwa należy zapoznać się z informacjami, które zawiera Rozdział 2, “Korzystanie z wartości systemowej Bezpieczeństwo systemu (System Security - QSecurity)”, na stronie 9. 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). 3. Jeśli minimalna długość haseł przekracza 6, wartość systemowa QPWDMINLEN nie zostanie zmieniona. 4. Jeśli maksymalna długość haseł przekracza 8, wartość systemowa QPWDMAXLEN nie zostanie zmieniona. 5. Ta wartość systemowa zostanie zmieniona tylko wtedy, gdy wartość systemowa QPWDRULES jest aktualnie ustawiona na *PWDSYSVAL. 6. Ta wartość systemowa nie zostanie zmieniona, jeśli jej bieżąca wartość wynosi *PWDSYSVAL.		

Komenda CFGSYSSEC ustawia także hasło na wartość *NONE dla wymienionych poniżej profili użytkowników IBM:

- QSYSOPR
- QPGMR
- QUSER
- QSRV
- QSRVBAS

Komenda CFGSYSSEC konfiguruje także kontrolę bezpieczeństwa według wartości podanych za pomocą komendy Zmiana kontroli bezpieczeństwa (Change Security Auditing - CHGSECAUD).

Zmienianie programu

Jeśli niektóre skonfigurowane wartości systemowe nie są odpowiednie dla instalacji użytkownika, można utworzyć własną wersję programu, która przetwarza komendę Konfigurowanie bezpieczeństwa systemu (Configure System Security - CFGSYSSEC).

Aby zmienić program, wykonaj następujące czynności:

1. Aby skopiować źródło programu uruchamianego podczas używania komendy CFGSYSSEC, użyj komendy Odtworzenie źródła CL (Retrieve CL Source - RTVCLSRC). Wczytywany program to QSYS/QSECCFGS. Po jego wczytaniu nadaj mu inną nazwę.
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.
3. Aby zmienić program do przetwarzania parametru komendy (PGM) dla komendy CFGSYSSEC, użyj komendy Zmiana komendy (Change Command - CHGCMD). Jako wartość PGM podaj nazwę swojego programu. Na przykład, aby utworzyć program o nazwie MYSECCFG w bibliotece QGPL, należy użyć następującej komendy:

   ```
   CHGCMD CMD(QSYS/CFGSYSSEC) PGM(QGPL/MOJ_PROG_SECCFG)
   ```

   Uwagi:

   a. 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.

   b. Podpis cyfrowy komendy RVKPUBAUT straci ważność, jeśli komenda ta zostanie zmieniona tak, aby korzystała z innego programu przetwarzania komend.

Opis działania komendy Odwołanie uprawnień publicznych (Revoke Public Authority)

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 241 oraz aplikacyjnych interfejsów programistycznych (API), które zawiera Tabela 242. W dostarczanym systemie uprawnienia publiczne dla tych komend i interfejsów API są ustawione na wartość *USE.

Komendy wymienione w sekcji Tabela 241 and the APIs that are listed in Tabela 242 dają możliwość poczynienia szkód w systemie. 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 241. Komendy, dla których uprawnienia publiczne ustawiane są za pomocą komendy RVKPUBAUT

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36FRSTS36FLRRSTS36LIBM
CHGCFGL	CRTDEVAPPC	STRRMTSPT
CHGCFGLE	CRTSBSD	STRSBS
CHGCMNE	ENDRMTSPT	WRKCFGL
CHGCTLAPPC	RMVAJE	
CHGDEVAPPC	RMVCFGLE	

Wszystkie interfejsy API, które zawiera Tabela 242 znajdują się w bibliotece QSYS:

Tabela 242. Programy dla których uprawnienia publiczne ustawiane są za pomocą komendy RVKPUBAUT

QTIENDSUP		
QTISTRSUP		
QWTCTLTR		
QWTSETTR		
QY2FTML		

Począwszy od wersji 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 ustawienia nie są odpowiednie dla instalacji użytkownika, można utworzyć własną wersję programu, która przetwarza komendę Odwołanie uprawnień publicznych (Revoke Public Authority - RVKPUBAUT).

Aby zmienić program, wykonaj następujące czynności:

1. Aby skopiować źródło programu uruchamianego podczas używania komendy RVKPUBAUT, użyj komendy Odtworzenie źródła CL (Retrieve CL Source - RTVCLSRC). Wczytywany program to QSYS/QSECRVKP. Po jego wczytaniu nadaj mu *inną nazwę*.

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.
3. Aby zmienić program do przetwarzania parametru komendy (PGM) dla komendy RVKPUBAUT, użyj komendy Zmiana komendy (Change Command - CHGCMD). Jako wartość PGM podaj nazwę swojego programu. Na przykład, aby utworzyć program o nazwie MYRVKPGM w bibliotece QGPL, należy użyć następującej komendy:

   ```
   CHGCMD CMD(QSYS/RVKPUBAUT) PGM(QGPL/MOJ_PROG_RVK)
   ```

   Uwagi:

   a. 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.

   b. Podpis cyfrowy komendy RVJPUDAUT straci ważność, jeśli komenda ta zostanie zmieniona tak, aby korzystała z innego programu przetwarzania komend.

Dodatek H. Informacje pokrewne dotyczące bezpieczeństwa systemu i5/OS

W niniejszej sekcji wymieniono podręczniki do produktów oraz dokumentację techniczną IBM Redbooks (w formacie PDF), serwisy WWW oraz tematy Centrum informacyjnego, które zawierają informacje pokrewne na temat bezpieczeństwa. Dokumenty w formacie PDF można wyświetlić lub wydrukować.

Podręczniki

- Podręcznik Recovering your system (około 8,42 MB) 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.
- Podręcznik Installing, upgrading, or deleting i5/OS and related software (3053 kB) udostępnia procedury przeprowadzające krok po kroku przez instalowanie początkowe, instalowanie programów licencjonowanych, poprawek PTF oraz języków dodatkowych z IBM.
- Podręcznik Remote Workstation Support  (1636 kB) udostępnia informacje dotyczące konfigurowania i używania obsługi zdalnych stacji roboczych, jak funkcji tranzytu terminalu, funkcji DHCF i zdalnych przyłączy 3270.
- Podręcznik Cryptographic Support/400  (448 kB) opisuje możliwości zabezpieczania danych za pomocą programu licencjonowanego Cryptographic Facility. Wyjaśnia, jak używać tego narzędzia oraz udostępnia informacje uzupełniające dla programistów.
- Podręcznik Local Device Configuration  (763 kB) udostępnia informacje dotyczące początkowej konfiguracji oraz jej zmiany. Zawiera także informacje dotyczące konfigurowania urządzeń.
- Podręcznik *SNA Distribution Services*, SC41-5410 (2259 kB) 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. (Podręcznik ten nie wchodzi w skład obecnego wydania Centrum informacyjnego i5/OS. Zawiera jednak przydatne informacje. Można go uzyskać za pośrednictwem Centrum publikacji IBM, zamawiając książkę drukowaną lub uzyskać wersję elektronicznej do bezpłatnego pobrania.
- Podręcznik *ADTS for AS/400: Source Entry Utility*, SC09-2605 (460 kB) 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. Podręcznik zawiera przykłady pomocne użytkownikom zarówno nowym jak i doświadczonych podczas wykonywania zadań edycji, od najprostszych komend wierszowych do korzystania z predefiniowanych zapytań dla języków wysokopoziomowych i formatów danych. (Podręcznik ten nie wchodzi w skład obecnego wydania Centrum informacyjnego i5/OS. Zawiera jednak przydatne informacje. Można go uzyskać za pośrednictwem Centrum publikacji IBM, zamawiając książkę drukowaną lub uzyskać wersję elektronicznej do bezpłatnego pobrania.

Dokumentacja techniczna IBM (Redbooks)

- Dokumentacja techniczna (Redbook) AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet  (2,1 MB) W tej dokumentacji technicznej IBM omówiono zagadnienia dotyczące bezpieczeństwa i czynników ryzyka związanych z podłączeniem produktu System i do Internetu. Udostępnia przykłady, zalecenia, wskazówki i techniki dla aplikacji.
- Podręcznik Cool Title About the AS/400 and Internet  (7,36 MB) - ta dokumentacja techniczna IBM Redbook umożliwia poznanie i naukę korzystania z Internetu (lub własnego intranetu) za pomocą produktu System i. 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.

Serwisy WWW

- Dokumentacja produktów Lotus  (http://www-10.lotus.com/ldd/doc)

  Ten serwis WWW zawiera informacje o produktach Lotus Notes, Domino i IBM Domino, przeznaczonych do systemu i5/OS. Z serwisu tego można pobrać informacje w formatach bazy danychDomino (.NSF) i Adobe Acrobat (.PDF), przeszukać bazy danych oraz uzyskać informacje na temat otrzymania podręczników w postaci wydrukowanej.

Inne informacje

- Książka Planning and setting up system security zawiera zestaw praktycznych porad dotyczących używania opcji zabezpieczających serwera iSeries i ustanawiania procedur obsługi dotyczących bezpieczeństwa. Podaje również informacje na temat konfiguracji i korzystania z narzędzi bezpieczeństwa, będących częścią systemu i5/OS.
- *Implementing AS/400 Security, wydanie 4* (15 października 2000 r.), Wayne Madden, Carol Woodbury. Loveland, Colorado: 29th Street Press. Zawiera wskazówki i praktyczne sugestie dotyczące planowania i konfigurowania bezpieczeństwa systemu oraz zarządzania nim.

  Numer zamówienia ISBN
  1583040730
- System i Access for Windows podaje informacje techniczne o programach System i Access for Windows do wszystkich wersji systemu System i Access for Windows
- Temat Konfiguracja TCP/IP podaje opis sposobu używania i konfigurowania protokołu TCP/IP.
- Temat Aplikacje, protokoły i usługi TCP/IP podaje opis używania aplikacji TCP/IP, takich jak FTP, SMTP i TELNET.
- Temat Podstawowe operacje systemowe informuje, jak uruchamiać i zatrzymywać system oraz radzić sobie z problemami w systemie.
- Temat Zintegrowany system plików zawiera przegląd zintegrowanego systemu plików. Opisuje, czym jest ten system, jak go używać i jakie są do niego interfejsy.
- Temat Serwer iSeries a bezpieczeństwo w Internecie ułatwia wykrycie potencjalnych problemów z bezpieczeństwem, występujących wskutek połączenia systemu iSeries z Internetem. Więcej informacji na ten temat zawiera strona główna serwisu IBM I/T (Information Technology) Security: http://www.ibm.com/security. Temat Optyczna pamięć masowa podaje informacje o funkcjach unikalnych dla *obsługi nośników optycznych*. Zawiera także informacje pomocne przy używaniu i zrozumieniu działania urządzeń CD, bezpośrednio podłączonych urządzeń biblioteki nośników optycznych oraz podłączonych za pomocą sieci LAN.
- Temat Drukowanie zawiera informacje na temat drukowania elementów i pojęcia dotyczące systemu, zbioru drukarkowego i obsługi buforowania drukarkowego dla operacji wydruku, oraz połączeń drukarek.
- Podręcznik Język CL udostępnia obszerny przegląd tematów dotyczących programowania, obejmujących ogólne omówienie obiektów i bibliotek, programowania w języku CL, sterowania przepływem oraz komunikowania 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.

  Podano tu także opis całego języka CL środowiska iSeries oraz jego komend dotyczących systemu i5/OS. Komendy i5/OS służą do wywoływania funkcji licencjonowanego programui5/OS (5722-SS1). Wszystkie komendy CL niebędące komendami i5/OS—te przypisane innym programom licencjonowanym, w tym różnym językom programowania i narzędziom—opisane są w podręcznikach dotyczących tych programów licencjonowanych.
- Temat Programowanie udostępnia informacje dotyczące wielu języków i narzędzi dostępnych w systemie iSeries. Zawiera podsumowanie:
  - Wszystkie komendy iSeries CL (w programie i5/OS i wszystkich innych programach licencjonowanych), pod różnymi postaciami.

  - 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).
- Temat Zarządzanie systemami zawiera informacje o gromadzeniu danych na temat wydajności, zarządzania wartościami systemowymi i zarządzania pamięcią masową.
- Temat Pojęcia dotyczące zbiorów bazy danych zawiera przegląd metod projektowania, pisania, uruchamiania i testowania instrukcji w narzędziach DB2 Query Manger i SQL Development Kit for i5/OS. Opisuje także interaktywny język SQL oraz udostępnia przykłady instrukcji SQL w programach COBOL, RPG, C, FORTRAN i PL/I. Ponadto podaje informacje na temat:
  - 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.

Zapisywanie plików PDF

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

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

Pobieranie programu Adobe Reader

Do przeglądania i drukowania plików PDF potrzebny jest program Adobe Reader zainstalowany na komputerze. Bezpłatną kopię programu można pobrać z serwisu WWW firmy Adobe

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

Dodatek I. Uwagi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Wszelkie ceny podawane przez IBM są propozycjami cen detalicznych; ceny te są aktualne i podlegają zmianom bez wcześniejszego powiadomienia. Ceny podawane przez dealerów mogą być inne.

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

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

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

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

Informacje na temat interfejsu programistycznego

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

Znaki towarowe

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

AIX
i5/OS
IBM
IBM (logo)
System i
z/OS

Intel, Intel Inside (logo), MMX oraz Pentium są znakami towarowymi Intel Corporation w Stanach Zjednoczonych i/lub w innych krajach.

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

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

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

UNIX jest zastrzeżonym znakiem towarowym Open Group w Stanach Zjednoczonych i w innych krajach.

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

Windows

Warunki

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

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

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

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

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

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

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

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

Drukowane w USA

SC85-0124-10