IBM

eserver

iSeries

Wskazówki i narzędzia dotyczące ochrony iSeries

Wersja 5

SC85-0032-07

IBM

@server

iSeries

Wskazówki i narzędzia dotyczące ochrony iSeries

Wersja 5

SC85-0032-07

Uwaga

Przed użyciem tych informacji oraz produktu, którego dotyczą, należy zapoznać się z informacjami zawartymi w sekcji “Uwagi” na stronie 161.

Wydanie ósme (kwiecień 2004)

To wydanie dotyczy wersji 5, wydania 3, modyfikacji 0 produktu IBM Operating System/400 (numer produktu 5722-SS1) i wszystkich kolejnych wydań i modyfikacji, chyba że zostanie to określone inaczej w kolejnych wydaniach. Ta wersja może nie pracować na wszystkich modelach komputerów o zredukowanej liczbie instrukcji (RISC) ani na modelach CISC.

Wydanie to zastępuje publikację SC85-0032-06.

Spis treści

Rysunki

Tabele

O książce Wskazówki i narzędzia dotyczące ochrony iSeries (SC85-0032-07)

Rola komputerów w organizacjach ulega gwałtownej zmianie. Menedżerowie IT, dostawcy oprogramowania, administratorzy ochrony i kontrolerzy potrzebują nowego spojrzenia na szereg obszarów, którymi zajmowali się już wcześniej. Wśród nich powinna znajdować się ochrona iSeries.

Systemy udostępniają wiele nowych funkcji, które niewiele różnią się od tradycyjnych aplikacji rozliczeniowych. Użytkownicy mają do dyspozycji nowe sposoby łączenia się z systemami: poprzez sieci LAN, linie komutowane (dial-up), sieci bezprzewodowe, a także poprzez inne typy sieci. Bardzo często jest tak, że użytkownicy nigdy nie widzą ekranu wpisywania się. Wiele organizacji staje się "rozległymi przedsiębiorstwami" z własnymi sieciami lub z Internetem.

Nagle okazało się, że systemy stały się łatwiej dostępne z zewnątrz. Menedżerowie systemów i administratorzy ochrony są skoncentrowani na tym, w jaki sposób chronić ważne informacje w szybko zmieniającym się środowisku.

Niniejsza publikacja zawiera one szereg praktycznych porad dotyczących korzystania z opcji ochrony iSeries i ustanawiania bezpiecznych procedur obsługi. Zalecenia znajdujące się w tej książce mają zastosowanie podczas instalacji z przeciętnymi wymaganiami dotyczącymi ochrony. Nie zawiera ona pełnego opisu dostępnych opcji ochrony iSeries. Opis dodatkowych opcji i szczegółowe informacje można znaleźć w publikacjach, których wykaz zawiera Rozdział 17, "Informacje pokrewne", na stronie 159.

Opisano tu także sposób instalacji i wykorzystania narzędzi będących częścią systemu OS/400. Informacje na temat narzędzi ochrony zawierają Rozdział 4, "Konfigurowanie iSeries do użycia narzędzi ochrony", na stronie 29 i sekcja "Komendy i menu dla komend ochrony" na stronie 30. Dodatkowo znajdują się tam przykłady używania tych narzędzi.

Do kogo adresowana jest ta książka

Za ochronę systemu odpowiedzialny jest **szef ochrony** lub **administrator ochrony**. Odpowiedzialność ta obejmuje zwykle następujące zadania:

- konfigurowanie i zarządzanie profilami użytkowników,
- ustawianie wartości systemowych mających wpływ na ochronę,
- administrowanie uprawnieniami do obiektów,
- wprowadzanie i monitorowanie strategii ochrony.

Jeśli jesteś odpowiedzialny za administrowanie ochroną jednego lub kilku systemów iSeries, informacje zawarte w tej książce są przeznaczone dla Ciebie. W instrukcjach zawartych w tej książce zakłada się, że:

- znasz podstawowe procedury systemu iSeries, takie jak wpisywanie się do systemu czy używanie komend,
- znasz podstawowe elementy ochrony iSeries: poziomy ochrony, wartości systemowe ochrony, profile użytkowników i ochronę obiektów.

  Uwaga: Rozdział 1, "Podstawowe elementy ochrony serwera iSeries", na stronie 3 zawiera przegląd tych elementów. Jeśli elementy te są dla Ciebie nowe,

przeczytaj sekcję *Podstawowa ochrona systemu i planowanie* w Centrum informacyjnym iSeries. Szczegóły znajdują się w sekcji "Informacje wstępne i pokrewne".

- Ustawienie wartości systemowej poziomu ochrony (QSECURITY) na przynajmniej 30 oznacza uaktywnienie ochrony systemu.

IBM ciągle rozwija możliwości ochrony w systemie iSeries. Aby wykorzystać nowe możliwości, należy regularnie analizować zbiorczy pakiet poprawek, dostępny dla danego wydania systemu. Należy sprawdzać, czy zawiera on poprawki związane z ochroną.

Jak używać tych informacji

Jeśli system nie został skonfigurowany tak, aby mógł używać narzędzi ochrony lub jeśli zainstalowano Security ToolKit for OS/400 dla wcześniejszego wydania, należy:

1. Przeczytać Rozdział 2, "Kreator ochrony iSeries i eServer Security Planner", na stronie 11. Opisuje on, w jaki sposób, korzystając z narzędzi ochrony, można określić zalecane narzędzia ochrony i jak rozpocząć pracę z nimi.
2. Więcej informacji na temat ochrony można znaleźć w książce Ochrona, umieszczonej online w Centrum informacyjnym iSeries.

Uwaga

Książka ta zawiera *wiele* wskazówek dotyczących ochrony iSeries. System może wymagać ochrony tylko niektórych obszarów. Ta pozycja może służyć jako źródło informacji o możliwych zagrożeniach ochrony i sposobach ich unikania. Można z niej też korzystać w konkretnych zagadnieniach ochrony tych obszarów, które są najbardziej newralgiczne w danym systemie.

Informacje wstępne i pokrewne

W Centrum informacyjnym można znaleźć dalsze odniesienia do informacji technicznych iSeries.

Dostęp do Centrum informacyjnego można uzyskać na dwa sposoby:

- Ze strony WWW

  `http://www.ibm.com/eserver/iseries/infocenter`
- Z dysku CD-ROM *Centrum informacyjne iSeries*, SK3T-4091-04. Ten dysk CD-ROM został dostarczony z nowym zamówieniem aktualizacji sprzętu iSeries lub oprogramowania IBM Operating System/400. Można również zamówić ten dysk CD-ROM z IBM Publications Center:

  `http://www.ibm.com/shop/publications/order`

Centrum informacyjne iSeries zawiera nowe i zaktualizowane informacje o serwerze iSeries, takie jak instalacja oprogramowania i sprzętu, Linux, WebSphere, Java, wysoka dostępność, baza danych, partycje logiczne, komendy CL oraz interfejsy API. Ponadto oferuje doradców i wyszukiwarki pomagające w planowaniu, rozwiązywaniu problemów i konfigurowaniu sprzętu oraz oprogramowania iSeries.

Z każdym zamówieniem sprzętu dostarczane są dyski *CD-ROM iSeries - Konfigurowanie i obsługa*, SK3T-4098-02. Ten dysk CD-ROM zawiera IBM **@server** IBM e(logo)server iSeries Access for Windows i kreatora EZ-Setup. iSeries Access Family oferuje bogaty

zestaw funkcji klienta i serwera, służących do łączenia komputerów PC z serwerami iSeries. Kreator EZ-Setup umożliwia automatyzację wielu czynności związanych z konfigurowaniem serwerów iSeries.

Jak wysyłać uwagi

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

- Aby wysłać komentarz pocztą, należy użyć formularza komentarzy czytelników i adresu wydrukowanego po jego drugiej stronie. Przy wysyłaniu formularza komentarzy czytelników spoza terenu Stanów Zjednoczonych, można przekazać formularz lokalnemu działowi firmy IBM lub przedstawicielowi firmy IBM.
- wysłać uwagi faksem pod jeden z poniższych numerów:
  - Stany Zjednoczone i Kanada: 1-800-937-3430
  - Inne kraje: 1-507-253-5192
- wysłać uwagi w postaci elektronicznej pod jeden z poniższych adresów poczty elektronicznej:
  - uwagi dotyczące książek:

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

    RCHINFOC@us.ibm.com

Uwagi powinny zawierać:

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

Część 1. Podstawowa ochrona serwera iSeries

Rozdział 1. Podstawowe elementy ochrony serwera iSeries

Ten temat zawiera krótki opis podstawowych elementów, które współpracując ze sobą, zapewniają ochronę systemu iSeries. W innych częściach książki podane są bardziej szczegółowe informacje, zawierające wskazówki, jak używać tych elementów, aby zaspokoić potrzeby organizacji.

Poziomy ochrony

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

Poziom 10:
System nie wymaga ochrony. Nie jest potrzebne żadne hasło. Jeśli podczas wpisywania się profil użytkownika nie istnieje, zostanie utworzony.

UWAGA:

Począwszy od wersji V4R3 nie można ustawić poziomu ochrony 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. Ponieważ poziom ochrony 10 nie zapewnia żadnej ochrony, nie jest on zalecany przez IBM. **IBM nie będzie pomagać w rozwiązywaniu problemów, które wystąpią na poziomie ochrony 10, chyba że można będzie je odtworzyć na wyższym poziomie ochrony.**

Poziom 20:
System wymaga do wpisania się identyfikatora użytkownika i hasła. Poziom ochrony 20 określa się często mianem **ochrony na poziomie wpisywania się**.Domyślnie wszyscy użytkownicy mają dostęp do wszystkich obiektów, ponieważ mają uprawnienie specjalne *ALLOBJ.

Poziom 30:
System wymaga do wpisania się identyfikatora użytkownika i hasła. Użytkownicy muszą mieć uprawnienia do używania obiektów, ponieważ domyślnie nie mają żadnych uprawnień. Jest to **ochrona na poziomie zasobów**.

Poziom 40:
System wymaga do wpisania się identyfikatora użytkownika i hasła. Poza ochroną zasobów system zapewnia **zabezpieczenie integralności.**Funkcje zabezpieczenia integralności, takie jak sprawdzanie paramtetrów dla interfejsów systemu operacyjnego, służą do zabezpieczania zarówno systemu, jak i istniejących w nim obiektów, przed manipulowaniem nimi przez doświadczonych użytkowników. Poziom 40 jest zalecany dla większości instalacji. Nowy system iSeries w wersji V4R5 lub nowszej jest dostarczany z ustawionym poziomem ochrony 40.

Poziom 50:
System wymaga do wpisania się identyfikatora użytkownika i hasła. System wymusza zarówno ochronę zasobów, jak i zabezpieczenie integralności, podobnie jak w przypadku poziomu 40,ale dodaje **rozszerzone zabezpieczenia integralności**, takie jak ograniczenia przesyłania komunikatów pomiędzy programami systemowymi a programiami użytkowników. Poziom ochrony 50 jest przeznaczony dla systemów iSeries, którym stawia się duże wymagania w zakresie ochrony.

Uwaga: Poziom 50 jest wymagany do certyfikatów C2 (i FIPS-140).

Rozdział 2 książki *iSeries Ochrona* zawiera więcej informacji o poziomach ochrony i opisuje sposoby przechodzenia pomiędzy nimi.

Ustawienia globalne

W systemie są pewne ustawienia globalne, określające sposób pracy systemu i jego wygląd z punktu widzenia innych użytkowników. Ustawienia te obejmują:

Wartości systemowe dotyczące ochrony:
Wartości systemowe dotyczące ochrony służą do sterowania ochroną systemu. Dzielą się one na cztery grupy:
- ogólne wartości systemowe dotyczące ochrony,
- inne wartości systemowe dotyczące ochrony,
- wartości systemowe sterujące hasłami,
- wartości systemowe sterujące kontrolą.

Kilka tematów w tej książce omawia wpływ określonych wartości systemowych na ochronę. Rozdział 3 w książce *iSeries Ochrona* opisuje wszystkie wartości systemowe związane z ochroną.

Atrybuty sieciowe:
Atrybuty sieciowe sterują sposobem współistnienia (lub określają brak uczestnictwa) w sieci z innymi systemami. Więcej informacji o atrybutach sieciowych znajduje się w książce *Zarządzanie pracą w systemie AS/400*.

Opisy podsystemów i inne elementy do zarządzania pracą:
Elementy do zarządzania pracą określają sposób wprowadzania danych i środowisko systemu. Kilka tematów w tej książce omawia wpływ niektórych wartości związanych z zarządzaniem pracą na ochronę. Pełne informacje zawiera książka *Zarządzanie pracą w systemie AS/400*.

Konfiguracja komunikacji:
Konfiguracja komunikacji również wpływa na to, jak dane są wprowadzane do systemu. W kilku tematach w tej książce znajdują się sugestie dotyczące zabezpieczania systemu podłączonego do sieci.

Profile użytkowników

Każdy użytkownik systemu **musi** mieć profil użytkownika. Przed wpisaniem się użytkownika należy utworzyć profil użytkownika. Profile użytkowników mogą służyć także do kontroli praw dostępu do narzędzi serwisowych, takich jak DASD i narzędzie do wykonywania zrzutów pamięci głównej. Więcej informacji można znaleźć w sekcji “Zarządzanie narzędziami serwisowymi” na stronie 62.

Profil użytkownika jest skutecznym i elastycznym narzędziem. Określa, co użytkownik może zrobić, a także definiuje sposób, w jaki widzi on system. Książka *iSeries Ochrona* opisuje wszystkie parametry w profilu użytkownika.

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 można wykorzystać jako wzorzec przy tworzeniu indywidualnych profili użytkowników za pomocą funkcji kopiowania profilu lub, jeśli jest używany iSeries Navigator, za pomocą menu Strategie ochrony do edycji uprawnień użytkownika.

Rozdziały 5 i 7 w książce *iSeries Ochrona* zawierają więcej informacji o planowaniu i używaniu profili grupowych.

Ochrona zasobów

Ochrona zasobów w systemie umożliwia definiowanie, kto może używać obiektów i w jaki sposób mogą one być używane. Możliwość dostępu do obiektu nazywa się **uprawnieniem**. Podczas konfigurowania uprawnień do obiektów należy dać użytkownikom takie uprawnienia, które pozwolą im wykonywać swoją pracę, ale uniemożliwią przeglądanie i zmienianie systemu. Uprawnienie do obiektu daje użytkownikowi prawo do pracy z obiektem i określa, co użytkownik może z nim zrobić. Zasób obiektu może być ograniczony przez określenie szczegółowych uprawnień użytkowników, takich jak dodawanie lub zmienianie rekordów. Można wykorzystać zasoby systemu, dając użytkownikowi dostęp do określonych zdefiniowanych systemowo podzbiorów uprawnień: *ALL, *CHANGE, *USE i *EXCLUDE.

Zbiory, programy, biblioteki i katalogi są obiektami systemowymi, które najczęściej wymagają ochrony zasobów, ale można określić uprawnienia do każdego obiektu z osobna.

Rozdział 5, “Zabezpieczenie ważnych informacji poprzez uprawnienia do obiektu” zawiera uwagi opisujące, jak ważne jest skonfigurowanie uprawnień do obiektów w systemie. Rozdział 5 książki *iSeries Ochrona* opisuje opcje służące do konfigurowania ochrony zasobów.

Ograniczenie dostępu do funkcji programu

Ograniczenie dostępu do funkcji programu zapewnia jego ochronę, gdy nie ma chroniącego go obiektu iSeries. Przed dodaniem tej funkcji w wersji V4R3, aby kontrolować prawa dostępu do funkcji programu, należało utworzyć listę autoryzacji lub inny obiekt, a następnie sprawdzać uprawnienia do tego obiektu. Teraz, aby łatwiej kontrolować prawa dostępu do aplikacji, części aplikacji lub różnych funkcji w ramach jednego programu, można używać ograniczenia dostępu do funkcji programu.

Aby zarządzać dostępem użytkowników do funkcji aplikacji za pomocą programu iSeries Navigator, można użyć jednej z dwóch metod. Pierwsza korzysta z obsługi Administracji aplikacji:

1. Kliknij prawym przyciskiem myszy system zawierający funkcje, do których chcesz zmienić ustawienia dostępu.
2. Zaznacz **Administrowanie aplikacjami**.
3. Jeśli znajdujesz się w systemie administracyjnym, zaznacz **Ustawienia lokalne**. W przeciwnym przypadku przejdź do następnego kroku.
4. Zaznacz funkcje, które mogą być administrowane.
5. Jeśli jest dostępna opcja **Dostęp domyślny**, zaznacz ją. Dzięki temu domyślnie wszyscy użytkownicy będa mieli dostęp do tej funkcji.
6. Jeśli jest dostępna opcja **Dostęp do wszystkich obiektów**, zaznacz ją. Dzięki temu wszyscy użytkownicy posiadający uprawnienia do obiektów systemowych będą mieli dostęp do tej funkcji.
7. Jeśli jest dostępny przycisk **Dostosuj**, kliknij go. W oknie dialogowym **Dostosowanie dostępu** użyj przycisków **Dodaj** i **Usuń**, aby dodać lub usunąć z list **Dostęp dozwolony** oraz **Brak dostępu** użytkowników lub grup.
8. Jeśli jest dostępny przycisk **Usuń dostosowanie**, kliknij go. Dzięki temu zostanie usunięty każdy skonfigurowany dostęp do wybranej funkcji.
9. Kliknij **OK**, aby zamknąć okno dialogowe **Administrowanie aplikacjami**.

Druga metoda zarządzania dostępem użytkowników wykorzystuje obsługę użytkowników i grup programu iSeries Navigator:

1. W programie iSeries Navigator, rozwiń **Użytkownicy i grupy**.
2. Zaznacz **Wszyscy użytkownicy**, **Grupy** lub **Użytkownik poza grupą**, aby wyświetlić listę użytkowników i grup.
3. Kliknij prawym przyciskiem myszy użytkownika lub grupę i zaznacz **Właściwości**.
4. Kliknij **Możliwości**.
5. Kliknij zakładkę **Aplikacje**.
6. Użyj tej strony, aby zmienić ustawienia dostępu dla użytkonika lub grupy.
7. Kliknij dwukrotnie **OK**, aby zamknąć okno dialogowe **Właściwości**.

Więcej informacji na temat programu iSeries Navigator i ochrony znajduje się w sekcji "Ochrona iSeries Navigator" na stronie 148.

Programiści mogą wykorzystać funkcje API ograniczenia dostępu do funkcji programu, aby:

- zarejestrować funkcję,
- pobrać informacje o funkcji,
- zdefiniować, kto może, a kto nie może korzystać z funkcji,
- sprawdzić, czy użytkownik ma uprawnienia do korzystania z funkcji.

Uwaga: Obsługa ta **nie** zastępuje ochrony zasobów. Nie zabezpiecza przed dostępem użytkownika do danego zasobu (na przykład zbioru lub programu) przy użyciu innego interfejsu.

Aby wykorzystać tę obsługę w ramach aplikacji, dostawca aplikacji musi zarejestrować funkcje podczas instalowania aplikacji. Zarejestrowana funkcja odpowiada blokowi kodu realizującemu określone funkcje w aplikacji. Gdy aplikacja jest uruchamiana przez użytkownika, przed wywołaniem tego bloku aplikacja wywołuje określoną funkcję API. Następnie jest wywoływana funkcja API sprawdzająca, czy użytkownik ma uprawnienia do korzystania z funkcji. Jeśli tak, uruchamiany jest blok kodu. Jeśli nie, użytkownik nie ma możliwości uruchomienia bloku kodu.

Uwaga: Funkcje API umożliwiają zarejestrowanie w bazie danych 30-znakowego identyfikatora funkcji (WRKREGINF). Ponieważ funkcje API obsługujące ograniczenia dostępu do funkcji programu nie używają punktów wyjścia związanych z identyfikatorami funkcji, same funkcje muszą mieć punkty wyjścia. Aby cokolwiek zarejestrować, **trzeba** podać nazwę formatu punktu wyjścia. W tym celu funkcja API Register Function tworzy fikcyjną nazwę i używa jej dla wszystkich zarejestrowanych funkcji. Ponieważ nazwa formatu jest fikcyjna, nie jest wywoływany żaden program zawierający punkt wyjścia.

Administrator systemu określa, kto ma lub nie ma dostępu do funkcji. Do zarządzania dostępem do funkcji programu może on użyć funkcji API lub interfejsu Administrowanie aplikacjami programu iSeries Navigator. Książka *iSeries server API Reference* zawiera informacje o funkcjach API umożliwiających ograniczenie dostępu do funkcji programu. Dodatkowe informacje o kontroli praw dostępu do funkcji znajdują się w sekcji "Ochrona iSeries Navigator" na stronie 148.

Kontrola ochrony

Kontrolowanie ochrony systemu może mieć kilka celów:

- Określenie, czy plan ochrony jest kompletny.

- Upewnienie się, że planowane elementy sterujące ochroną są na swoim miejscu i działają poprawnie. Ten typ kontroli jest zwykle realizowany przez szefa ochrony w ramach codziennych czynności administracyjnych. Może on także być wykonywany, czasami w sposób bardziej szczegółowy, w ramach okresowego badania ochrony przez pracowników przedsiębiorstwa lub firmy zewnętrzne.
- Upewnienie się, że ochrona systemu dotrzymuje kroku zmianom 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.

Opisane tu techniki są odpowiednie dla wszystkich powyższych sytuacji. Dobór kontrolowanych elementów oraz częstotliwość kontrolowania zależą od wielkości organizacji i potrzeb związanych z ochroną.

Kontrola ochrony wymaga użycia komend systemu i korzystania z informacji zawartych w protokołach i kronikach w systemie. Można utworzyć specjalny profil dla osoby, która będzie wykonywała kontrolę ochrony systemu. Profil kontrolera wymaga utworzenia uprawnienia specjalnego *AUDIT, aby można było zmieniać parametry kontroli systemu. Niektóre zadania kontroli zalecane w tym rozdziale wymagają profilu użytkownika z uprawnieniami specjalnymi *ALLOBJ i *SECADM. Po zakończeniu okresu kontroli należy upewnić się, że hasło tego profilu zostało ustawione na *NONE.

Szczegółowe informacje o kontroli ochrony zawiera Rozdział 9 książki *Ochrona*.

Przykład: raport dotyczący atrybutów ochrony systemu

Rys. 1 na stronie 8 przedstawia przykładowy wynik działania komendy Wydruk atrybutów ochrony systemu (Print System Security Attributes - PRTSYSSECA). Raport zawiera ustawienia wartości systemowych związanych z ochroną i atrybuty sieciowe zalecane dla systemu z typowymi wymaganiami odnośnie ochrony, a także bieżące ustawienia systemowe.

Uwaga: Kolumna *Wartość bieżąca* zawiera bieżące ustawienia systemowe. Aby sprawdzić, czy istnieje ryzyko naruszenia ochrony, należy je porównać z zalecanymi wartościami.

```
Atrybuty ochrony systemu

Nazwa wartości
systemowej       Wartość bieżąca        Wartość zalecana
QALWOBJRST       *NONE                  *NONE
QALWUSRDMN       *ALL                   QTEMP
QATNPGM          QEZMAIN   QSYS         *NONE
QAUDENDACN       *NOTIFY                *NOTIFY
QAUDFRCLVL       *SYS                   *SYS
QAUDCTL          *AUDLVL                *AUDLVL   *OBJAUD
QAUDLVL          *SECURITY              *AUTFAIL  *CREATE
                                        *DELETE   *SECURITY
                                        *SAVRST   *NOQTEMP
```

Rysunek 1. Wydruk artybutów ochrony systemu - przykład (Część 1 z 4)

```
QAUTOCFG         0                      0
QAUTORMT         1                      0
QAUTOVRT         9999                   0
QCMNRCYLMT       0 0                    0 0
QCRTAUT          *CHANGE                Sterowane z poziomu biblioteki.
QCRTOBJAUD       *NONE                  Sterowane z poziomu biblioteki.
QDEVRCYACN       *DSCMSG                *DSCMSG
QDSCJOBITV       120                    120
QDSPSGNINF       1                      1
QINACTITV        60                     60
QINACTMSGQ       *ENDJOB                *ENDJOB
QLMTDEVSSN       0                      1
QLMTSECOFR       0                      1
QMAXSGNACN       2                      3
QMAXSIGN         3                      3
```

Rysunek 1. Wydruk artybutów ochrony systemu - przykład (Część 2 z 4)

```
QPWDEXPITV       60                     60
QPWDLMTAJC       1                      1
QPWDLMTCHR       *NONE                  AEIOU@$#
QPWDLMTREP       1                      2
QPWDLVL          0
QPWDMAXLEN       8                      8
QPWDMINLEN       6                      6
QPWDPOSDIF       1                      1
QPWDRQDDGT       1                      1
QPWDRQDDIF       0                      1
QPWDVLDPGM       *NONE                  *NONE
QRETSVRSEC       0                      0
QRMTIPL          0                      0
QRMTSIGN         *FRCSIGNON             *FRCSIGNON
QSECURITY        50                     50
QSHRMEMCTL       1                      0
QSRVDMP          *DMPUSRJOB             *NONE
QUSEADPAUT       *NONE                  CRTAUTL AUTL(QUSEADPAUT) AUT(*EXCLUDE)
                                        CHGOBJOWN OBJ(QUSEADPAUT) OBJTYPE(*AUTL)
                                        CHGSYSVAL SYSVAL(QUSEADPAUT) VALUE(QUSEADPAUT)
QVFYOBJRST       1                      3
```

Rysunek 1. Wydruk artybutów ochrony systemu - przykład (Część 3 z 4)

```
Atrybuty ochrony systemu

Nazwa atrybutu
sieciowego       Wartość bieżąca        Wartość zalecana
DDMACC           *OBJAUT                *REJECT
JOBACN           *FILE                  *REJECT
PCSACC           *OBJAUT                *REJECT
```

Rysunek 1. Wydruk artybutów ochrony systemu - przykład (Część 4 z 4)

Rozdział 2. Kreator ochrony iSeries i eServer Security Planner

Kreator ochrony serwera iSeries i eSeries Security Planner pomagają w określeniu, jakie parametry ochrony mają obowiązywać w danym serwerze iSeries. Za pomocą Kreatora ochrony iSeries w programie iSeries Navigator można generować raporty określające na podstawie wybranych odpowiedzi wymagania ochrony. Informacje te można wykorzystać przy konfigurowaniu ochrony systemu.

Kreator ochrony iSeries i eServer Security Planner pomagają zaplanować i zaimplementować podstawowe założenia strategii ochrony dla serwerów iSeries servers. Celem obydwu tych narzędzi jest ułatwienie implementowania i zarządzania ochroną systemu. Kreator, który jest dostępny jako część systemu OS/400, zadaje kilka pytań wysokiego poziomu o środowisko serwera i w oparciu o odpowiedzi przedstawia zalecenia, które kreator może zastosować dla systemu.

Aplikacja eServer Security Planner jest wersją online Kreatora ochrony. Umożliwia ona użytkownikowi wybranie określonych opcji na podstawie wymagań stawianych ochronie, a następnie generuje raport sugerujący, jakie opcje będą wymagane, aby serwer był bezpieczny.

Aplikacja eServer Security Planner jest kreatorem działającym na stronie WWW. Podobnie jak kreator, dostarcza on zalecenia dotyczące implementacji ochrony systemu. Jednak doradca nie może zastosować tych zaleceń. Służy on raczej do utworzenia listy wartości ochrony systemu i innych atrybutów w oparciu o odpowiedzi na pytania doradcy, które powinny zostać zastosowane.

Kreator ochrony

Podjęcie decyzji, których wartości ochrony serwera iSeries należy użyć w danej firmie, może być skomplikowane. Kreator ochrony może w tym pomóc nowym użytkownikom systemu iSeries, a także użytkownikom zaawansowanym, jeśli implementacja ochrony lub środowisko, w którym pracuje iSeries, są im nieznane.

Co to jest kreator?

- Kreator jest to narzędzie przeznaczone dla nowych użytkowników, którzy instalują lub konfigurują w systemie dowolne oprogramowanie.
- Kreator uzyskuje od użytkownika informacje, zadając pytania. Odpowiedź na każde kolejne pytanie decyduje o tym, jakie będzie następne.
- Po udzieleniu odpowiedzi na wszystkie pytania jest wyświetlane okno zakończenia. Następnie użytkownik naciska przycisk **Zakończ**, aby zainstalować lub skonfigurować dany element.

Cele Kreatora ochrony

Na podstawie odpowiedzi użytkownika Kreator ochrony:

- konfiguruje wartości systemowe i atrybuty sieciowe dotyczące ochrony,
- konfiguruje związane z ochroną raporty służące do monitorowania systemu,
- generuje Raport informacyjny administratora i Raport informacyjny użytkownika:
  - Raport informacyjny administratora zawiera ustawienia związane z ochroną i wszelkie procedury, jakie mają być zrealizowane, zanim zalecenia zostaną zastosowane,
  - Raport informacyjny użytkownika zawiera informacje, które można wykorzystać podczas opracowywania strategii ochrony w firmie, między innymi reguły tworzenia haseł,

- zaleca określone konfiguracje różnych elementów systemu związanych z ochroną.

Zadania Kreatora ochrony

- Do zadań Kreatora ochrony należy:
  - określanie ustawień ochrony systemu na podstawie udzielonych odpowiedzi, a następnie ich wdrożenie tam, gdzie jest to odpowiednie;
  - generowanie szczegółowych raportów, takich jak:
    - raport wyjaśniający zalecenia kreatora;
    - raport zawierający szczegóły procedur, które powinny zostać zrealizowane przed rozpoczęciem implementacji;
    - raport zawierający listę informacji, jakie mają być przekazane użytkownikom systemu;
- elementy te wprowadzają w życie podstawową strategię ochrony systemu,
- kreator zaleca zaplanowanie regularnego generowania raportów kroniki kontroli; regularnie generowane raporty pomagają w:
  - zapewnieniu realizacji strategii ochrony;
  - zapewnieniu, że strategia ochrony jest zmieniana tylko za zgodą uprawnionych osób;
  - określeniu harmonogramu raportów umożliwiających monitorowanie w systemie zdarzeń związanych z ochroną;
- kreator umożliwia zapisanie zaleceń oraz zastosowanie w systemie wszystkich lub niektórych z nich.

Uwaga: W tym samym systemie można wielokrotnie używać Kreatora ochrony, umożliwiając użytkownikom posiadającym starszą instalację przeglądanie bieżących ustawień ochrony. Kreator ochrony może być używany od wersji V3R7 systemu (czyli od wprowadzenia programu iSeries Navigator).

Aby używać programu iSeries Navigator, na komputerze PC z systemem operacyjnym Windows 95/NT musi być zainstalowany IBM iSeries Access for Windows i komputer ten musi być połączony z serwerem iSeries. Użytkownik kreatora musi być wpisany do serwera iSeries. Jego identyfikator musi mieć uprawnienia specjalne *ALLOBJ, *SECADM, *AUDIT i *IOSYSCFG. Informacje dotyczące łączenia komputera PC z Windows 95/NT z systemem iSeries, można znaleźć w Centrum informacyjnym w artykule IBM iSeries Access for Windows (szczegóły znajdują w sekcji “Informacje wstępne i pokrewne” na stronie xii).

Aby uruchomić Kreator ochrony:

1. W programie iSeries Navigator, rozwiń dany server.
2. Kliknij prawym przyciskiem myszy **Ochrona** i zaznacz **Konfiguruj**.
   - Gdy użytkownik wybiera w aplikacji iSeries Navigator opcję **Ochrona**, do serwera iSeries jest wysyłane żądanie sprawdzenia jego uprawnień specjalnych.
   - Jeśli użytkownik nie ma wszystkich wymaganych uprawnień specjalnych (*ALLOBJ, *AUDIT, *IOSYSCFG, *SECADM), nie zobaczy opcji **Konfiguruj** i nie będzie miał dostępu do Kreatora ochrony.
3. Jeśli użytkownik ma wymagane uprawnienia:
   - wczytywane są poprzednie odpowiedzi,
   - wczytywane są bieżące ustawienia ochrony.

Kreator ochrony zaczyna się od jednego z trzech ekranów powitalnych. Wyświetlany ekran zależy od tego, który z poniższych warunków jest spełniony:

- kreator nie był jeszcze uruchamiany dla docelowego serwera iSeries,
- kreator był już uruchamiany, ale zmiany w ochronie zostały odroczone,
- kreator był już uruchamiany, a zmiany w ochronie zostały zastosowane.

Jeśli nie używasz programu iSeries Navigator, również możesz uzyskać pomoc w planowaniu ochrony. Aplikacja eServer Security Planner jest wersją online Kreatora ochrony, z jedną różnicą. Nie skonfiguruje on systemu automatycznie. Na podstawie odpowiedzi wygeneruje on jedynie raport zawierający zalecane opcje dotyczące ochrony. Aby uzyskać dostęp do aplikacji eServer Security Planner, należy przejść do Centrum informacyjnego eServer:

`http://publib.boulder.ibm.com/eserver/`

eServer Security Planner

Aplikacja eServer Security Planner jest wersją online Kreatora ochrony. Zadaje te same pytania, co Kreator ochrony i, na podstawie odpowiedzi, generuje te same zalecenia. Podstawowe różnice to:

- Aplikacja eServer Security Planner **nie**—
  - generuje raportów szczegółowych,
  - porównuje bieżących ustawień z zalecanymi,
  - ustawia automatycznie wartości systemowych.
- Z poziomu aplikacji eServer Security Planner nie można stosować zaleceń.

Aplikacja eServer Security Planner generuje program w języku CL, który można skopiować i edytować, aby zautomatyzować konfigurowanie ochrony. Z poziomu aplikacji eServer Security Planner można także przejść bezpośrednio do dokumentacji serwera iSeries. Dzięki temu można łatwo uzyskać informacje o danej wartości systemowej lub raporcie, które pomogą określić, czy wybrane ustawienia są odpowiednie dla danego środowiska.

Aby uzyskać dostęp do aplikacji eServer Security Planner, należy wpisać w przeglądarce poniższy adres URL:

`http://publib.boulder.ibm.com/eserver/`

Rozdział 3. Sterowanie interaktywnym wpisywaniem się

Ograniczanie dostępu do systemu należy zacząć od rzeczy oczywistej – ekranu Wpisanie się (Sign On). Można wykorzystać poniższe opcje, aby utrudnić osobie z zewnątrz wpisanie się do systemu za pomocą ekranu Wpisanie się (Sign On).

Ustawianie reguł tworzenia haseł

Aby zabezpieczyć wpisanie się do systemu, należy:
- określić strategię, która wymaga, aby hasła nie były proste i aby użytkownicy nie przekazywali ich sobie,
- ustawić wartości systemowe, tak aby pomagały w realizacji tej strategii; Tabela 1 zawiera zalecane ustawienia wartości systemowych.

Tabela 1 zawiera dość rygorystyczne wartości, które mają na celu radykalne zmniejszenie prawdopodobieństwa wyboru łatwego hasła. Jednak wybranie hasła spełniającego te kryteria może być trudne i denerwujące.

Warto udostępnić użytkownikom:
1. Listę kryteriów wyboru hasła.
2. Przykłady haseł poprawnych i niepoprawnych.
3. Rady, jak wymyślić dobre hasło.

Aby ustawić te wartości, trzeba uruchomić komendę Konfigurowanie ochrony systemu (Configure System Security - CFGSYSSEC). Należy użyć komendy Wydruk atrybutów ochrony systemu (Print System Security Attributes - PRTSYSSECA) .

Rozdział 3 książki *iSeries Ochrona*. Więcej informacji na temat komendy CFGSYSSEC zawiera sekcja “Wartości ustawiane przez komendę Konfigurowanie ochrony systemu” na stronie 38.

Tabela 1. Wartości systemowe dotyczące haseł

Nazwa wartości systemowej	Opis	Zalecana wartość
QPWDEXPITV	Jak często użytkownicy muszą zmieniać hasła. W każdym profilu użytkownika z osobna można podać inną wartość.	60 (dni)
QPWDLMTAJC	Czy system zabrania użycia tych samych przylegających znaków.	1 (tak)
QPWDLMTCHR	Jakich znaków nie można używać w hasłach.[2]	AEIOU#$@
QPWDLMTREP	Czy system zabrania wielokrotnego pojawienia się tego samego znaku w haśle.	2 (nie obok siebie)
QPWDLVL	Czy długość hasła dla profilu użytkownika jest ograniczona do 10 znaków, czy może mieć wartość maksymalną - 128.	0[3]
QPWDMAXLEN	Maksymalna liczba znaków w haśle.	8
QPWDMINLEN	Minimalna liczba znaków w haśle.	6
QPWDPOSDIF	Czy każdy znak w haśle musi być inny od tego samego znaku w poprzednim haśle.	1 (tak)
QPWDRQDDGT	Czy hasło musi zawierać przynajmniej jedną cyfrę.	1 (tak)
QPWDRQDDIF	Po jakim czasie użytkownik może ponownie użyć tego samego hasła.[2]	5 lub mniej (okresów ważności)[1]
QPWDVLDPGM	Jaki program obsługi wyjścia jest wywoływany, aby sprawdzić poprawność nowego hasła.	*NONE

Tabela 1. Wartości systemowe dotyczące haseł (kontynuacja)

Nazwa wartości systemowej	Opis	Zalecana wartość

Uwagi:

1. Wartość systemowa QPWDEXPITV określa, jak często należy zmieniać hasło, na przykład co 60 dni. Jest to **okres ważności**. Wartość systemowa QPWDRQDDIF określa, ile takich okresów musi upłynąć, aby można było ponownie użyć tego samego hasła. Rozdział 3 książki *iSeries Ochrona* zawiera więcej informacji o relacjach pomiędzy tymi wartościami systemowymi.
2. Wartość systemowa QPWDLMTCHR nie jest wymuszana na poziomie haseł 2 i 3. Szczegółowe informacje zawiera sekcja "Poziomy haseł".
3. Sekcja "Planowanie zmian poziomu haseł" zawiera informacje pomocne przy określaniu odpowiedniego poziomu.

Poziomy haseł

Od wersji V5R1 systemu operacyjnego, wartość systemowa QPWDLVL oferuje zwiększone zabezpieczenie hasłem. W poprzednich wydaniach użytkownicy musieli korzystać z haseł, których długość nie mogła przekraczać 10 znaków z ograniczonego zestawu. Obecnie można używać hasła (słowa lub kilku słów), zawierającego do 128 znaków, w zależności od ustawionego w systemie poziomu haseł. Poziomy haseł to:

- **Poziom 0:** systemy są dostarczane z tym poziomem. Na poziomie 0 hasła nie mogą mieć więcej niż 10 znaków i mogą zawierać tylko następujące znaki: A – Z, 0 – 9, #, @, $, i _. Poziom 0 jest najmniej bezpieczny.
- **Poziom 1:** takie same reguły, jak na poziomie 0, ale hasła dla iSeries Support for Windows Network Neighborhood (czyli iSeries NetServer) nie są zapisywane.
- **Poziom 2:** na tym poziomie hasła są bezpieczne. Poziom ten może być używany do celów testowych. Hasło użytkownika jest zachowywane, jeśli ma 10 znaków lub mniej i zawiera znaki z zestawu dopuszczalnego na poziomie 0 lub 1. Hasła (składające się z jednego lub więcej słów) na tym poziomie mają następującą charakterystykę:
  - ich długość może wynosić do 128 znaków;
  - mogą składać się z dowolnych znaków dostępnych na klawiaturze;
  - nie mogą składać się w całości z odstępów; wszystkie odstępy na końcu hasła są usuwane;
  - wielkość liter jest rozróżniana.
- **Poziom 3:** na tym poziomie hasła są najbezpieczniejsze, ponieważ wykorzystują najbardziej zaawansowane algorytmy szyfrowania. Hasła na tym poziomie mają taką samą charakterystykę, jak na poziomie 2. Na tym poziomie hasła dla iSeries NetServer nie są zapisywane.

Jeśli każdy system w sieci spełnia poniższe kryteria, powinno się używać haseł tylko z poziomu 2 i 3:

- system operacyjny jest w wersji V5R1 lub późniejszej,
- poziom haseł jest ustawiony na 2 lub 3.

Ponadto użytkownicy muszą wpisywać się przy użyciu tego samego poziomu haseł. Poziomy haseł są globalne; poszczególni użytkownicy nie mogą wybrać poziomu zabezpieczenia swoich haseł.

Planowanie zmian poziomu haseł

Zmiana poziomu haseł powinna być odpowiednio zaplanowana. Jeśli zmiany poziomu haseł nie zostaną odpowiednio zaplanowane, wymiana danych z innymi systemami może nie powieść się lub też użytkownicy nie będą mogli wpisać się do systemu. Przed zmianą wartości systemowej QPWDLVL należy się upewnić, że dane ochrony zostały zeskładowane

za pomocą komendy SAVSECDTA lub SAVSYS. Jeśli dostępna jest aktualna kopia zapasowa, można zresetować hasła dla wszystkich profili użytkowników w sytuacji, gdy konieczny będzie powrót do niższego poziomu haseł.

Programy wykorzystywane w systemie i w klientach, z którymi system się komunikuje, mogą stwarzać problemy, gdy poziom haseł (wartość systemowa QPWDLVL) jest ustawiony na 2 lub 3. Należy zaktualizować produkty i klientów wysyłających do systemu hasła w postaci zaszyfrowanej (czyli inne niż te, w których użytkownik wpisuje hasło na ekranie wpisywania się), aby obsługiwały nowe reguły szyfrowania haseł dla poziomu QPWDLVL równego 2 lub 3. Wysyłanie zaszyfrowanego hasła nazywa się **podstawieniem hasła**.

Podstawienie hasła zabezpiecza przed przechwyceniem hasła podczas przesyłania go przez sieć. Podstawienia haseł wygenerowane przez starszych klientów, którzy nie obsługują nowego algorytmu dla poziomu QPWDLVL 2 lub 3, nawet jeśli specyficzne znaki są poprawne, nie będą akceptowane. Dotyczy to także dostępu do serwera iSeries do równorzędnego serwera iSeries z użyciem szyfrowania w celu uwierzytelnienia systemów.

Problem jest bardziej złożony, ponieważ niektóre produkty, których to dotyczy (takie, jak Java Toolbox) są udostępniane jako oprogramowanie pośrednie. Produkty firm innych niż IBM wykorzystujące wcześniejszą wersję jednego z tych produktów nie będą pracowały poprawnie, dopóki nie zostaną odbudowane za pomocą zaktualizowanej wersji oprogramowania pośredniego.

Dlatego właśnie przed zmianą wartości systemowej QPWDLVL konieczne jest ostrożne planowanie.

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 0 na 1

Poziom haseł 1 pozwala wyeliminować hasła NetServer z systemu, który nie musi komunikować się z produktem Windows 95/98/ME AS/400 Client Support for Windows Network Neighborhood (iSeries 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. Prawdopodobieństwo włamania jest bardzo małe, z wyjątkiem funkcji wymagających hasła dla iSeries NetServer.

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 0 lub 1 na 2

Poziom haseł 2 oznacza użycie haseł z rozróżnianiem wielkości liter, o długości do 128 znaków (jedno lub kilka słów); powrót do poziomu QPWDLVL 0 lub 1 jest możliwy.

Niezależnie od poziomu haseł w systemie, hasła dla 2 i 3 poziomu są tworzone przy każdej zmianie hasła i za każdym razem, gdy użytkownik wpisuje się do systemu. Tworzenie haseł dla poziomów 2 i 3 w systemie, który jest na poziomie 0 lub 1, pomaga w przygotowaniu zmiany poziomu haseł na 2 lub 3.

Przed zmianą poziomu QPWDLVL na 2 administrator systemu powinien użyć komend DSPAUTUSR lub PRTUSRPRF TYPE(*PWDINFO), aby znaleźć wszystkie profile użytkowników, którzy nie mają haseł możliwych do wykorzystania na poziomie 2. W zależności od tego, jakie profile zostaną znalezione, administrator może wykonać jedną z poniższych czynności w celu dodania do profilu hasła na poziomie 2 i 3.

- Zmienić hasło profilu za pomocą komendy CHGUSRPRF lub CHGPWD, albo za pomocą funkcji API QSYCHGPW. Spowoduje to zmianę hasła użytecznego na poziomach 0 i 1. System utworzy także dwa odpowiednie hasła użyteczne na poziomach 2 i 3 (z rozróżnianiem wielkości liter). Zostaną także utworzone dwie wersje hasła do użycia na poziomach 2 i 3: w całości małymi i w całości wielkimi literami.

Na przykład zmiana hasła na C4D2RB4Y spowoduje wygenerowanie haseł C4D2RB4Y i c4d2rb4y dla poziomu 2.

- Wpisać się do systemu metodą wyświetlającą hasła w postaci niezaszyfrowanej (bez podstawienia). Jeśli hasło jest poprawne, a profil użytkownika nie ma hasła użytecznego na poziomach 2 i 3, system utworzy dwa odpowiednie hasła użyteczne na poziomach 2 i 3 (z rozróżnianiem wielkości liter). Zostaną także utworzone dwie wersje hasła do użycia na poziomach 2 i 3: w całości małymi i w całości wielkimi literami.

Brak hasła użytecznego na poziomie 2 lub 3 może być problemem w sytuacji, gdy profil użytkownika nie ma hasła użytecznego na poziomach 0 i 1, albo też gdy próbuje on wpisać się za pomocą produktu używającego podstawiania haseł. W takich sytuacjach, po zmianie poziomu haseł na 2, użytkownik nie będzie w stanie wpisać się do systemu.

Jeśli profil użytkownika nie ma hasła użytecznego na poziomach 2 i 3, ale ma hasło użyteczne na poziomach 0 i 1, to po wpisaniu się tego użytkownika za pomocą produktu wysyłającego hasła w postaci niezaszyfrowanej system uwierzytelnia użytkownika z użyciem hasła na poziomie 0 i tworzy dwa hasła dla poziomu 2 (w sposób opisany powyżej) dla tego profilu użytkownika. Następnie uwierzytelnianie będzie odbywało się z użyciem haseł dla poziomu 2.

Żaden klient ani usługa używająca podstawiania haseł nie będzie poprawnie działała na poziomie QPWDLVL 2, jeśli nie została zaktualizowana pod kątem użycia nowych reguł. Administrator powinien sprawdzić, czy wymagana jest aktualizacja klientów/usług.

Klienci/usługi używające podstawiania haseł to między innymi:

- TELNET
- iSeries Access
- iSeries Host Servers
- QFileSrv.400
- obsługa wydruków iSeries NetServer
- DDM
- DRDA
- SNA LU6.2

Zaleca się zeskładowanie danych ochrony przed zmianą poziomu na QPWDLVL 2. W razie potrzeby ułatwi to przejście z powrotem do poziomu QPWDLVL 0 lub 1.

Zaleca się także, aby inne wartości systemowe dotyczące haseł, takie jak QPWDMINLEN i QPWDMAXLEN, nie były zmieniane, dopóki poziom QPWDLVL 2 nie zostanie przetestowany. W razie potrzeby ułatwi to powrót do poziomu QPWDLVL 1 lub 0. Jednakże, aby system zezwolił na zmianę poziomu QPWDLVL na 2, wartość systemowa QPWDVLDPGM musi być równa *REGFAC lub *NONE. Dlatego, jeśli korzysta się z programu sprawdzającego hasła, może zaistnieć potrzeba napisania nowego, który za pomocą komendy ADDEXITPGM zostanie zarejestrowany dla punktu wyjścia QIBM_QSY_VLD_PASSWRD.

Na poziomie QPWDLVL równym 2 hasła iSeries NetServer są nadal obsługiwane, dlatego wszystkie funkcje i usługi wymagające haseł iSeries NetServer powinny nadal działać prawidłowo.

Gdy administrator jest zadowolony z działania systemu na poziomie QPWDLVL 2, może zacząć zmieniać odpowiednie Wartości systemowe, aby wykorzystać możliwość tworzenia dłuższych haseł. Musi jednak wiedzieć, że ma to następujące konsekwencje:

- Jeśli podane zostanie hasło dłuższe niż 10 znaków, hasła dla poziomów 0 i 1 zostaną usunięte. Dany profil użytkownika nie będzie mógł wpisać się do systemu, jeśli zostanie przywrócony poziom haseł 0 lub 1.
- Jeśli hasło zawiera znaki specjalne lub nie odpowiada regułom tworzenia prostych nazw obiektów (z wyjątkiem rozróżniania wielkości znaków), hasła dla poziomów 0 i 1 zostaną usunięte.
- Jeśli podane zostanie hasło dłuższe niż 14 znaków, hasło iSeries NetServer dla tego profilu użytkownika zostanie usunięte.
- Wartości systemowe dla haseł dotyczą tylko nowych haseł dla poziomu 2, a nie dotyczą wygenerowanych przez system haseł dla poziomu 0 i 1 lub haseł iSeries NetServer (jeśli zostały wygenerowane).

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 2 na 3

Gdy system przez jakiś czas pracuje na poziomie haseł QPWDLVL 2, administrator może rozważyć zmianę poziomu QPWDLVL na 3 w celu dalszego zwiększenia bezpieczeństwa haseł.

Na poziomie QPWDLVL 3 wszystkie hasła iSeries NetServer są usuwane, dlatego nie należy zmieniać poziomu QPWDLVL na 3, dopóki istnieje potrzeba używania haseł iSeries NetServer.

Na poziomie QPWDLVL 3, wszystkie hasła z poziomu 0 i 1 są usuwane. Administrator może użyć komend DSPAUTUSR lub PRTUSRPRF w celu znalezienia profili użytkowników, którzy nie mają haseł dla poziomu 2 lub 3.

Zmiana na niższy poziom haseł

Mimo iż powrót do niższej wartości QPWDLVL jest możliwy, z założenia jest on utrudniony. W zasadzie należy przyjąć, że zwiększenie wartości QPWDLVL jest nieodwracalne. Może jednak zaistnieć potrzeba przywrócenia poprzedniej wartości QPWDLVL.

Poniższe sekcje opisują czynności wymagane przy przejściu na niższy poziom haseł.

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 3 na 2: Zmiana ta jest względnie łatwa. Po ustawieniu wartości QPWDLVL na 2 administrator musi określić, czy jakiś profil użytkownika potrzebuje haseł iSeries NetServer lub haseł na poziomie 0 lub 1, a jeśli tak, zmienić hasło tego profilu na spełniające odpowiednie wymagania.

Ponadto może zaistnieć konieczność zmiany wartości systemowych dla haseł, aby były zgodne z hasłami iSeries NetServer i poziomu 0 lub 1, jeśli takie hasła są wymagane.

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 3 na 1 lub 0: Ze względu na wysokie ryzyko wystąpienia problemów z systemem (na przykład brak możliwości wpisania się do systemu przez kogokolwiek z powodu usunięcia wszystkich haseł dla poziomu 0 i 1), zmiana ta nie jest możliwa w sposób bezpośredni. Aby zmienić poziom QPWDLVL 3 na 1 lub 0, należy najpierw zmienić poziom QPWDLVL na 2.

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 2 na 1: Przed zmianą poziomu QPWDLVL na 1 administrator powinien użyć komendy DSPAUTUSR lub PRTUSRPRF TYPE(*PWDINFO) w celu odnalezienia wszystkich profili użytkowników, dla których brak haseł dla poziomu 0 lub 1. Jeśli profil użytkownika będzie wymagał hasła po zmianie poziomu QPWDLVL, administrator musi utworzyć dla tego profilu hasło dla poziomu 0 i 1 w jeden z poniższych sposobów:

- Zmienić hasło profilu za pomocą komendy CHGUSRPRF lub CHGPWD, albo za pomocą funkcji API QSYCHGPW. Spowoduje to zmianę hasła użytecznego na poziomach 2 i 3. System utworzy także odpowiednie hasło użyteczne na poziomach 0 i 1 (w całości wielkimi literami). System może utworzyć hasła dla poziomów 0 i 1 tylko wtedy, gdy:

– długość hasła wynosi do 10 znaków;
– hasło może zostać przekształcone do wielkich liter A-Z oraz znaków 0-9, @, #, $ i znaku podkreślenia w standardzie EBCDIC;
– hasło nie zaczyna się od cyfry ani znaku podkreślenia.

Na przykład zmiana hasła na RainyDay spowoduje wygenerowanie hasła RAINYDAY dla poziomów 0 i 1. Natomiast zmiana hasła na Rainy Days In April spowoduje usunięcie hasła dla poziomu 0 i 1, ponieważ podane hasło jest za długie i zawiera spacje.

Jeśli nie można utworzyć hasła dla poziomu 0 i 1, nie zostanie wygenerowany żaden komunikat.

- Wpisać się do systemu metodą wyświetlającą hasła w postaci niezaszyfrowanej (bez podstawienia). Jeśli hasło jest poprawne, a profil użytkownika nie ma hasła użytecznego na poziomach 0 i 1, system utworzy odpowiednie hasło użyteczne na poziomach 0 i 1 (w całości wielkimi literami). Jest to możliwe tylko wtedy, gdy zostaną spełnione opisane wyżej warunki.

Administrator może następnie zmienić poziom QPWDLVL na 1. Gdy zmiana poziomu QPWDLVL na 1 zacznie obowiązywać (następny IPL), wszystkie hasła iSeries NetServer zostaną usunięte.

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 2 na 0: Procedura nie różni się od zmiany poziomu QPWDLVL z 2 na 1 z wyjątkiem tego, że wszystkie hasła iSeries NetServer zostaną zachowane.

Uwagi dotyczące zmiany wartości systemowej QPWDLVL z 1 na 0: Po zmianie poziomu QPWDLVL na 0 administrator powinien użyć komendy DSPAUTUSR lub PRTUSRPRF w celu odnalezienia wszystkich profili użytkowników, które nie mają haseł iSeries NetServer. Jeśli profil użytkownika wymaga hasła iSeries NetServer, może ono zostać utworzone poprzez zmianę hasła użytkownika lub wpisanie się w sposób przesyłający hasła w postaci niezaszyfrowanej.

Następnie administrator może zmienić poziom QPWDLVL na 0.

Zmiana znanych haseł

Aby zabezpieczyć się przed znanymi sposobami uzyskania dostępu do serwera iSeries, które można jeszcze wykorzystać, wykonaj następujące czynności:

__ Krok 1. Upewnij się, że żaden profil użytkownika nie ma domyślnego hasła (takiego jak nazwa profilu). Możesz użyć komendy Analiza domyślnych haseł (Analyze Default Passwords - ANZDFTPWD). (Patrz sekcja “Unikanie domyślnych haseł” na stronie 26).

__ Krok 2. Spróbuj wpisać się do systemu za pomocą profili użytkownika i haseł, które zawiera Tabela 2 na stronie 21. Te hasła są opublikowane i od nich zaczyna każdy, kto próbuje włamać się do systemu. Jeśli możesz się wpisać, użyj komendy Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF), aby zmienić hasło na zalecaną wartość.

__ Krok 3. Uruchom narzędzia DST (Dedicated Service Tools) i spróbuj się wpisać używając hasła, tak jak to pokazujeTabela 2 na stronie 21. Więcej informacji na ten temat zawiera artykuł w Centrum informacyjnym iSeries —> Ochrona —> Narzędzia usług. Informacje na temat dostępu do Centrum informacyjnego iSeries zawiera sekcja “Informacje wstępne i pokrewne” na stronie xii.

__ Krok 4. Jeśli możesz wpisać się do DST przy użyciu jednego z tych haseł, zmień je korzystając ze sposobów pokazanych w: Centrum informacyjnym

iSeries—Ochrona—>Narzędzia usług. Informacje na temat dostępu do Centrum informacyjnego iSeries (patrz “Informacje wstępne i pokrewne” na stronie xii).

__ Krok 5. Na koniec upewnij się, że nie możesz się wpisać po prostu naciskając klawisz Enter na ekranie Wpisanie się (Sign On) bez podawania identyfikatora użytkownika lub hasła. Wypróbuj kilka różnych terminali. Jeśli możesz wpisać się bez podawania jakichkolwiek informacji na ekranie Wpisanie się (Sign On), wykonaj jedną z poniższych czynności:

- Zmień poziom ochrony na 40 lub 50 (wartość systemowa QSECURITY).

  Uwaga: Jeśli zwiększysz poziom ochrony na 40 lub 50, aplikacje mogą działać inaczej.

- Zmień wszystkie pozycje stacji roboczych dla podsystemów interaktywnych, aby wskazywały na opis zadania USER(*RQD).

Tabela 2. Hasła dla profili IBM

ID użytkownika	Hasło	Zalecana wartość
QSECOFR	QSECOFR[1]	Nietrywialna wartość znana tylko administratorowi ochrony. **Zapisz wybrane hasło i umieść je w bezpiecznym miejscu.**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2, 3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

Uwagi:

1. System jest dostarczany z wartością *Ustawienie jako wygasłe hasła* dla użytkownika QSECOFR ustawioną na *YES. Hasło użytkownika QSECOFR musi zostać zmienione podczas pierwszego wpisywania się do systemu.
2. Opisane profile użytkowników są niezbędne do funkcjonowania systemu, ale nie należy pozwalać użytkownikom wpisywać się z nimi. Nowe systemy w wersji V3R1 lub nowszej mają hasła dla tych profili ustawione na *NONE.

   Po uruchomieniu komendy CFGSYSSEC system ustawia te hasła na *NONE.
3. Aby uruchomić iSeries Access for Windows przez łącze TCP/IP, profil użytkownika QUSER musi być uaktywniony.

Tabela 3. Hasła dla narzędzi DST

Poziom DST	ID użytkownika	Hasło	Zalecana wartość
Podstawowy zakres	11111111	11111111	Nietrywialna wartość znana tylko administratorowi ochrony.[2]
Pełny zakres	22222222	22222222[3]	Nietrywialna wartość znana tylko administratorowi ochrony.[2]
Zakres ochrony	QSECOFR	QSECOFR[3]	Nietrywialna wartość znana tylko administratorowi ochrony.[2]
Zakres obsługi	QSRV	QSRV[3]	Nietrywialna wartość znana tylko administratorowi ochrony.[2]

Tabela 3. Hasła dla narzędzi DST (kontynuacja)

Poziom DST	ID użytkownika	Hasło	Zalecana wartość

Uwagi:

1. Identyfikator użytkownika jest wymagany tylko w wersjach PowerPC AS (RISC) systemu operacyjnego.
2. Jeśli inżynier serwisu sprzętu musi wpisać się z tym identyfikatorem użytkownika, zmień hasło po jego wyjściu.
3. Profil użytkownika narzędzi serwisowych utraci ważność w momencie pierwszego użycia.

Uwaga: Hasła DST mogą być zmieniane tylko z uwierzytelnionego urządzenia. Dotyczy to również wszystkich haseł i odpowiadających im identyfikatorów użytkowników, które są identyczne. Więcej informacji na temat uwierzytelniania urządzeń znajduje się w artykule dotyczącym konfiguracji Operations Console w Centrum informacyjnym iSeries.

Ustawianie wartości wpisania się

Tabela 4 zawiera opisy kilku wartości systemowych, które należy ustawić, aby utrudnić nieuprawnionej osobie wpisanie się do systemu. Po uruchomieniu, komenda CFGSYSSEC nadaje tym wartościom systemowym zalecane ustawienia. Więcej informacji o tych wartościach systemowych znajduje się w rozdziale 3 książki *iSeries Ochrona*.

Tabela 4. Wartości systemowe wpisania się

Nazwa wartości systemowej	Opis	Zalecane ustawienie
QAUTOCFG	Określa, czy system automatycznie konfiguruje nowe urządzenia.	0 (Nie)
QAUTOVRT	Liczba opisów urządzeń wirtualnych, które system automatycznie utworzy, jeśli nie ma dostępnego urządzenia.	0
QDEVRCYACN	Postępowanie systemu po ponownym połączeniu urządzenia po błędzie.[1]	*DSCMSG
QDSCJOBITV	Określa, jak długo system czeka przed zakończeniem zadania odłączonego.	120
QDSPSGNINF	Określa, czy podczas wpisywania się system wyświetla informacje o poprzednim wpisaniu się.	1 (tak)
QINACTITV	Określa, jak długo system czeka przed podjęciem działania, gdy zadanie interaktywne jest nieaktywne.	60
QINACTMSGQ	Określa, co system robi po upłynięciu czasu określonego w zmiennej QINACTITV.	*ENDJOB
QLMTDEVSSN	Określa, czy system zabrania użytkownikom wpisywać się z kilku stacji roboczych równocześnie.	1 (tak)
QLMTSECOFR	Określa, czy użytkownicy z uprawnieniami specjalnymi *ALLOBJ lub *SERVICE mogą wpisywać się tylko z określonych stacji roboczych.	1 (tak)
QMAXSIGN	Maksymalna liczba kolejnych nieprawidłowych prób wpisania się (niepoprawny profil użytkownika lub hasło).	3
QMAXSGNACN	Określa, co system robi po osiągnięciu limitu określonego w zmiennej QMAXSIGN.	3 (zablokowanie zarówno profilu użytkownika, jak i urządzenia)

Tabela 4. Wartości systemowe wpisania się (kontynuacja)

Nazwa wartości systemowej	Opis	Zalecane ustawienie
Uwagi: 1. System może odłączyć, a następnie ponownie połączyć sesje TELNET, gdy opis urządzenia dla danej sesji zostanie jawnie przypisany. 2. Jeśli ta wartość systemowa jest ustawiona na 1 (tak), należy jawnie nadać uprawnienia do urządzeń użytkownikom z uprawnieniami specjalnymi *ALLOBJ lub *SERVICE. Najprostszym sposobem jest nadanie profilowi użytkownika QSECOFR uprawnienia *CHANGE do określonych urządzeń.		

Zmiana komunikatów o błędzie przy wpisywaniu się

Hakerzy chcą wiedzieć, czy posuwają się do przodu, włamując się do systemu. Gdy komunikat o błędzie na ekranie Wpisanie się (Sign On) brzmi Błędne hasło, haker może założyć, że identyfikator użytkownika jest prawidłowy. Można wprowadzić hakera w błąd zmieniając tekst dwóch komunikatów za pomocą komendy Zmiana opisu komunikatu (Change Message Description - CHGMSGD). Tabela 5 pokazuje zalecany tekst.

Tabela 5. Komunikaty o błędzie przy wpisywaniu się

ID komunikatu	Oryginalny tekst	Zalecany tekst
CPF1107	CPF1107 – Hasło nie jest poprawne dla profilu użytkownika.	Błędne informacje przy wpisaniu się **Uwaga:** Nie należy w tekście komunikatu umieszczać identyfikatora komunikatu.
CPF1120	CPF1120 – Użytkownik XXXXX nie istnieje.	Błędne informacje przy wpisaniu się **Uwaga:** Nie należy w tekście komunikatu umieszczać identyfikatora komunikatu.

Możliwości harmonogramu profili użytkowników

Istnieje możliwość wpisywania się z określonymi profilami użytkowników w określonych porach dnia lub dniach tygodnia. Na przykład skonfigurowany profil dla programu kontroli ochrony można uaktywnić tylko w godzinach pracy tego programu. Można także zablokować profile użytkowników z uprawnieniem specjalnym *ALLOBJ (w tym profil użytkownika QSECOFR) poza godzinami pracy.

Komenda Zmiana pozycji harmonogramu aktywacji (Change Activation Schedule Entry - CHGACTSCDE) umożliwia skonfigurowanie automatycznego włączania i wyłączania profili użytkowników. W harmonogramie tworzy się wpis dla każdego profilu użytkownika, definiujący jego parametry.

Na przykład, jeśli profil QSECOFR ma być dostępny tylko od godziny 7.00 do 22.00, należy na ekranie CHGACTSCDE wpisać:

```
                    Zmiana pozycji harmonogramu aktywacji
                  (Change Activation Scd Entry - CHGACTSCDE)

Wypełnij pola i naciśnij Enter

Profil użytkownika . . . . . > QSECOFR       Nazwa
Godzina uaktywnienia . . . . . > '7:00'      Godzina, *NONE
Godzina zablokowania . . . . . > '22:00'     Godzina, *NONE
Dni. . . . . . . . . . . . . . > *MON        *ALL, *MON, *TUE, *WED...
                               > *TUE
                               > *WED
                               > *THU
              + więcej wartości > *FRI
```

Rysunek 2. Ekran Zmiana pozycji harmonogramu aktywacji – przykład

Profil QSECOFR może być dostępny tylko przez ograniczoną liczbę godzin dziennie. Można utworzyć inny profil użytkownika o klasie *SECOFR, który będzie realizować większość funkcji systemowych. Pozwoli to uniknąć narażania ogólnie znanego profilu użytkownika na próby włamania.

Można użyć komendy Wyświetlenie pozycji kroniki kontroli (Display Audit Journal Entries - DSPAUDJRNE) w celu okresowego drukowania pozycji kroniki kontroli CP (Change Profile - Zmiana profilu). Pozycje te umożliwiają stwierdzenie, czy system uaktywnia i blokuje profile użytkowników zgodnie z harmonogramem.

Inną metodą weryfikacji jest użycie komendy Drukowanie profilu użytkownika (Print User Profile - PRTUSRPRF). Raport typu *PWDINFO zawiera statusy wszystkich wybranych profili użytkowników. Jeśli na przykład wszystkie profile użytkowników z uprawnieniem specjalnym *ALLOBJ są regularnie blokowane, można zaplanować natychmiast po zablokowaniu profili uruchomienie następującej komendy:

```
PRTUSRPRF TYPE(*PWDINFO) SELECT(*SPCAUT) SPCAUT(*ALLOBJ)
```

Usuwanie nieaktywnych profili użytkowników

W systemie powinny być tylko niezbędne profile użytkowników. Jeśli dany profil nie jest potrzebny, ponieważ użytkownik już nie pracuje lub zmienił stanowisko, należy go usunąć. Jeśli ktoś odszedł z firmy na dłuższy czas, należy wyłączyć (zablokować) profil tego użytkownika. Niepotrzebny profil użytkownika może stać się przyczyną nieuprawnionego wpisania się do systemu.

Automatyczna blokada profili użytkowników

Za pomocą komendy Analiza aktywności profilu (Analyze Profile Activity - ANZPRFACT) można regularnie blokować profile użytkowników, które były nieaktywne przez określoną liczbę dni. Używając komendy ANZPRFACT można określić liczbę dni nieaktywności. System sprawdza datę ostatniego użycia, datę odtworzenia i datę utworzenia profilu użytkownika.

Po podaniu wartości w komendzie ANZPRFACT, system uruchamia zadanie raz w tygodniu o godzinie 1.00 w nocy (począwszy od dnia podania tej wartości po raz pierwszy). Zadanie sprawdza wszystkie profile i blokuje nieaktywne. Nie ma potrzeby ponownego uruchamiania komendy ANZPRFACT, jeśli nie będzie zmieniana liczba dni nieaktywności.

Komendy Zmiana listy aktywnych profili (Change Active Profile List - CHGACTPRFL) można użyć do wyłączenia niektórych profili z przetwarzania komendy ANZPRFACT.

Komenda CHGACTPRFL tworzy listę profili użytkowników, których komenda ANZPRFACT nie zablokuje niezależnie od tego, jak długo były nieaktywne.

Gdy system uruchamia komendę ANZPRFACT, zapisuje pozycję CP w kronice kontroli dla każdego profilu użytkownika, który jest blokowany. Aby wyświetlić ostatnio zablokowane profile użytkowników, można użyć komendy DSPAUDJRNE.

Uwaga: System zapisuje pozycje kontroli tylko wtedy, gdy wartość systemowa QAUDCTL jest równa *AUDLVL, a wartość systemowa QAUDLVL jest równa *SECURITY.

Inną metodą weryfikacji jest użycie komendy Drukowanie profilu użytkownika (Print User Profile - PRTUSRPRF). Raport typu *PWDINFO zawiera statusy wszystkich wybranych profili użytkowników.

Automatyczne usuwanie profili użytkowników

Komendy Zmiana pozycji harmonogramu utraty ważności (Change Expiration Schedule Entry - CHGEXPSCDE) można użyć do zarządzania usuwaniem i blokowaniem profili użytkowników. Wiedząc, że użytkownika nie będzie przez dłuższy okres, można zaplanować usunięcie lub zablokowanie jego profilu.

Przy pierwszym użyciu komenda CHGEXPSCDE tworzy pozycję harmonogramu zadań, która jest uruchamiana codziennie 1 minutę po północy. Zadanie sprawdza zbiór QASECEXP, aby określić, czy w danym dniu mają być usunięte jakieś profile użytkowników.

Za pomocą komendy CHGEXPSCDE można zablokować lub usunąć profil użytkownika. Jeśli zostanie wybrane usunięcie profilu użytkownika, należy określić, co system ma zrobić z obiektami należącymi do tego użytkownika. Przed zaplanowaniem usunięcia profilu użytkownika należy sprawdzić te obiekty. Na przykład jeśli do użytkownika należą programy, które adoptują uprawnienia, to czy mają one zaadoptować uprawnienia nowego użytkownika. Czy nowy użytkownik ma większe uprawnienia, niż to potrzebne (na przykład uprawnienia specjalne)? Być może należy utworzyć nowy profil użytkownika z określonymi uprawnieniami, do którego będą należały programy wymagające uprawnień adoptowanych.

Należy także sprawdzić, czy po usunięciu profilu użytkownika nie wystąpią problemy z jakąś aplikacją. Na przykład czy istnieją opisy zadań, dla których ten profil użytkownika jest domyślny?

Komenda Wyświetlenie harmonogramu ważności (Display Expiration Schedule - DSPEXPSCD) umożliwia wyświetlenie listy profili, które mają być zablokowane lub usunięte.

Komendy Wyświetlenie uprawnionych użytkowników (Display Authorized Users - DSPAUTUSR) można użyć do wyświetlenia wszystkich profili użytkowników w systemie. Aby usunąć niepotrzebne profile użytkowników, należy użyć komendy Usunięcie profilu użytkownika (Delete User Profile - DLTUSRPRF).

Uwaga dotycząca ochrony: Aby zablokować profil użytkownika, należy ustawić jego status na *DISABLED. Zablokowanie profilu użytkownika powoduje, że jest on niedostępny do wykorzystania interaktywnego. Nie można wpisać się ani zmienić zadania przy użyciu zablokowanego profilu użytkownika, natomiast zadania wsadowe mogą go używać.

Unikanie domyślnych haseł

Przy tworzeniu nowego profilu użytkownika domyślnie nadawane jest mu takie samo hasło jak jego nazwa. Jeśli ktoś zna obowiązujące w firmie reguły tworzenia nazw profili i wie, że została zatrudniona nowa osoba, może dostać się do systemu.

Tworząc nowy profil użytkownika, należy rozważyć przypisanie mu unikalnego, nietrywialnego hasła, zamiast domyślnego i poinformować nowego użytkownika o haśle w sposób poufny, na przykład wysyłając list "Witamy w systemie", opisujący strategię ochrony. Należy również wymusić zmianę hasła przy pierwszym wpisaniu się, ustawiając dla profilu użytkownika PWDEXP(*YES).

Komendy Analiza domyślnych haseł (Analyze Default Passwords - ANZDFTPWD) można użyć do sprawdzenia wszystkich profili użytkowników w systemie pod kątem domyślnych haseł. Podczas drukowania raportu jest możliwość określenia, że system powinien podjąć działanie (na przykład zablokować profil użytkownika), jeśli hasło jest takie samo, jak nazwa profilu użytkownika. Komenda ANZDFTPWD drukuje listę znalezionych profili i działanie, jakie zostało podjęte.

Uwaga: Hasła są przechowywane w systemie w postaci zaszyfrowanej w sposób nieodwracalny. Nie mogą zostać zdeszyfrowane. System szyfruje podane hasło i porównuje je z przechowywanym w taki sam sposób, jak to ma miejsce podczas wpisywania się. Podczas kontroli błędów uprawnień (*AUTFAIL) system zapisze pozycję kroniki kontroli PW dla każdego profilu użytkownika, który *nie* ma domyślnego hasła (w systemach w wersji V4R1 lub wcześniejszej). Począwszy od wersji V4R2 system nie zapisuje pozycji kroniki kontroli PW, jeśli została uruchomiona komenda ANZDFTPWD.

Monitorowanie wpisywania się i zmiany haseł

Jeśli istnieje podejrzenie nieuprawnionych prób wejścia do systemu, można użyć komendy PRTUSRPRF w celu monitorowania wpisywania się i zmiany haseł.

Poniżej znajdują się sugestie, jak wykorzystać ten raport:

- Można określić, czy okres ważności hasła dla niektórych profili użytkowników jest dłuższy niż wartość systemowa i czy sytuacja ta jest dopuszczalna. W przykładowym raporcie okres ważności hasła użytkownika USERY wynosi 120 dni.
- Można regularnie generować ten raport, aby monitorować nieudane próby wpisania się. Ktoś, kto próbuje włamać się do systemu, może wiedzieć, że system podejmuje określone działanie po określonej liczbie nieudanych prób. Taki intruz mógłby każdej nocy podejmować mniejszą liczbę prób, niż określa to wartość QMAXSIGN, aby system nie ostrzegał o nich administratora. Generując ten raport codziennie rano można dowiedzieć się, czy miały miejsce częste nieudane próby wpisania się z pewnymi profilami użytkowników, co sugeruje wystąpienie problemu.
- Można określić profile użytkowników, które przez dłuższy czas nie były używane, lub takie, których hasła długo nie były zmieniane.

Przechowywanie haseł

W celu obsługi niektórych funkcji sieciowych i wymagań komunikacyjnych serwer iSeries udostępnia bezpieczną metodę przechowywania haseł, które mogą zostać zdeszyfrowane. System używa tych haseł między innymi do nawiązywania połączenia SLIP z innym systemem. (Sekcja "Ochrona i sesje połączeń wychodzących" na stronie 122 opisuje taki sposób wykorzystania przechowywanych haseł).

Te specjalne hasła są przechowywane na serwerze iSeries w bezpiecznym miejscu, które nie jest dostępne dla żadnych programów ani interfejsów użytkownika. Tylko te funkcje systemowe, którym jawnie nadano uprawnienia, mogą ustawiać i wczytywać te hasła.

Na przykład, stosując hasło dla wychodzących połączeń SLIP, ustawia się je za pomocą komendy systemowej, która tworzy profil konfiguracyjny (WRKTCPPTP). Aby użyć tej komendy, trzeba mieć uprawnienia *IOSYSCFG. Specjalnie zakodowany skrypt połączeniowy pobiera hasło i deszyfruje je podczas nawiązywania połączenia. Zdeszyfrowane hasło nie jest widoczne ani dla użytkowników, ani w żadnym protokole zadania.

Jako administrator ochrony musisz zdecydować, czy zezwolić na przechowywanie w systemie haseł, które można zdeszyfrować. Określa się to za pomocą wartości systemowej Zachowanie danych ochrony serwera (QRETSVRSEC). Domyślną wartością jest 0 (Nie). Oznacza to, że system nie będzie przechowywał haseł, które można zdeszyfrować, dopóki ta wartość systemowa nie zostanie jawnie ustawiona.

Jeśli komunikacja wymaga użycia takich haseł, należy określić odpowiednią strategię ochrony i poznać strategię obowiązującą w systemach, z którymi nawiązywane jest połączenie. Na przykład, jeśli w celu łączenia się z innym serwerem iSeries jest używany protokół SLIP, w obu systemach powinny być skonfigurowane specjalne profile użytkowników służące tylko do nawiązywania sesji. Profile te powinny mieć ograniczone uprawnienia w systemie. Ograniczy to szkody, jeśli w drugim systemie hasło zostanie złamane.

Rozdział 4. Konfigurowanie iSeries do użycia narzędzi ochrony

Ten rozdział opisuje sposób konfigurowania systemu do użycia narzędzi ochrony, które są częścią systemu OS/400. Po zainstalowaniu systemu OS/400 narzędzia ochrony są gotowe do użycia. Poniższe sekcje zawierają sugestie dotyczące procedur związanych z narzędziami ochrony.

Obsługa narzędzi ochrony

Po zainstalowaniu systemu OS/400 obiekty powiązane z narzędziami ochrony są bezpieczne. Aby bezpiecznie pracować z narzędziami ochrony, należy unikać zmian w uprawnieniach do jakiegokolwiek obiektu narzędzi ochrony.

Poniżej są opisane ustawienia ochrony i wymagania wobec obiektów narzędzi ochrony:

- Programy i komendy narzędzi ochrony znajdują się w bibliotece produktu QSYS. Są one dostarczane z uprawnieniem publicznym *EXCLUDE. Wiele komend narzędzia ochrony tworzy zbiory w bibliotece QUSRSYS. Gdy system tworzy te zbiory, nadaje im publiczne uprawnienie *EXCLUDE.

  Zbiory zawierające informacje służące do generowania raportów zmian mają nazwy zaczynające się od QSEC. Zbiory zawierające informacje służące do zarządzania profilami użytkowników mają nazwy zaczynające się od QASEC. Zbiory te zawierają informacje poufne, dlatego nie należy zmieniać uprawnień publicznych dla tych zbiorów.
- Narzędzia ochrony korzystają z normalnej konfiguracji systemu do kierowania wydruków. Raporty te zawierają informacje poufne. Aby skierować dane wyjściowe do bezpiecznej kolejki wyjściowej, należy dokonać odpowiednich zmian w profilu użytkownika lub opisie zadania dla użytkowników, którzy będą uruchamiali narzędzia ochrony.
- Ze względu na funkcje ochrony i to, że mają dostęp do wielu obiektów w systemie, komendy narzędzi ochrony wymagają uprawnienia specjalnego *ALLOBJ. Niektóre z komend wymagają także uprawnień specjalnych *SECADM, *AUDIT lub *IOSYSCFG. Aby zapewnić poprawne działanie tych komend, należy przed użyciem narzędzi ochrony wpisać się jako szef ochrony. Z tego też powodu nie należy przyznawać uprawnień prywatnych do żadnej komendy narzędzi ochrony.

Zapobieganie konfliktom zbiorów

Wiele komend tworzących raporty narzędzi ochrony tworzy zbiór bazy danych, który można wykorzystać do drukowania zmienionej wersji raportu. Sekcja “Komendy i menu dla komend ochrony” na stronie 30 zawiera nazwy zbiorów dla każdej komendy. Komendy ochrony można uruchamiać jednocześnie tylko z jednego zadania. Obecnie większość komend ma zaimplementowane funkcje wymuszające to. Próba uruchomienia komendy, gdy inne zadanie nie zakończyło jej działania, spowoduje wysłanie komunikatu o błędzie.

Wiele zadań pracuje przez długi czas. Wprowadzając raporty do zadań wsadowych lub dodając je do programu do planowania zadań, należy uważać, aby uniknąć konfliktów zbiorów. Na przykład, może zaistnieć potrzeba wydrukowania dwóch wersji raportu PRTUSRPRF z różnymi kryteriami wyboru. Aby zapewnić generowanie raportów jeden po drugim, należy wprowadzając raporty do zadań wsadowych używać kolejki zadań, z której w danym momencie jest uruchomione tylko jedno zadanie.

Używając programu do planowania zadań należy zaplanować dwa zadania w takim odstępie czasowym, aby pierwsza wersja zakończyła działanie przed uruchomieniem drugiego zadania.

Składowanie narzędzi ochrony

Programy narzędzi ochrony należy składować przy każdym uruchomieniu komendy Składowanie systemu (Save System - SAVSYS) lub jakiejkolwiek opcji z menu Składowanie (Save), która uruchamia komendę SAVSYS.

Zbiory narzędzi ochrony znajdują się w bibliotece QUSRSYS. Biblioteka ta powinna być już składowana w ramach zwykłych procedur. Biblioteka QUSRSYS zawiera dane dla wielu programów licencjonowanych w systemie. Centrum informacyjne zawiera więcej informacji o tym, które komendy i opcje umożliwiają składowanie biblioteki QUSRSYS.

Komendy i menu dla komend ochrony

Ta sekcja opisuje komendy i menu narzędzi ochrony. Przykłady użycia komend znajdują się w wielu miejscach w tym rozdziale.

Narzędza ochrony są dostępne z dwóch menu:

- Menu SECTOOLS (Security tools - Narzędzia ochrony), służącego do interaktywnego uruchamiania komend.
- Menu SECBATCH (Submit or Schedule Security Reports to Batch - Wprowadzenie raportów ochrony do zadania wsadowego lub zaplanowanie ich), służącego do uruchamiania komend raportów w trybie wsadowym. Menu SECBATCH składa się z dwóch części. W pierwszej części menu jest wykorzystywana komenda Wprowadzenie zadania (Submit Job - SBMJOB) w celu skierowania raportów do natychmiastowego przetworzenia wsadowego.

  Druga część menu korzysta z komendy Dodanie pozycji harmonogramu zadań (Add Job Schedule Entry - ADDJOBSCDE). Służy ona do zaplanowania generowania raportów ochrony regularnie w określonym dniu i godzinie.

Opcje menu Narzędzia ochrony

Tabela 6 opisuje wymienione opcje menu i powiązane z nimi komendy:

Tabela 6. Komendy do obsługi profilu użytkownika

Opcja menu[1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
1	ANZDFTPWD	Komenda Analiza domyślnych haseł (Analyze Default Passwords) służy do generowania raportów o profilach użytkowników, które mają hasło takie, jak nazwa profilu, i do podejmowania działań wobec tych profili.	QASECPWD[2]
2	DSPACTPRFL	Komenda Wyświetlenie listy aktywnych profili (Display Active Profile List) służy do wyświetlania lub drukowania listy profili użytkowników, które nie podlegają przetwarzaniu przez komendę ANZPRFACT.	QASECIDL[2]
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]

Tabela 6. Komendy do obsługi profilu użytkownika (kontynuacja)

Opcja menu[1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
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 co noc. Aby niektóre profile nie zostały zablokowane, należy użyć komendy CHGACTPRFL.	QASECIDL[2]
5	DSPACTSCD	Komenda Wyświetlenie harmonogramu aktywacji profili (Display Profile Activation Schedule) służy do wyświetlania lub drukowania informacji o harmonogramie uaktywniania i blokowania określonych profili użytkowników. Harmonogram tworzy się za pomocą komendy CHGACTSCDE.	QASECACT[2]
6	CHGACTSCDE	Komenda Zmiana pozycji harmonogramu aktywacji (Change Activation Schedule Entry) służy do uaktywniania profilu użytkownika tylko w określonych porach dnia lub dniach tygodnia. Dla każdego profilu użytkownika, który ma pozycję w harmonogramie, system tworzy pozycje harmonogramu zadań, odpowiadające godzinom uaktywnienia i zablokowania.	QASECACT[2]
7	DSPEXPSCD	Komenda Wyświetlenie harmonogramu ważności (Display Expiration Schedule) służy do wyświetlania lub drukowania listy profili użytkowników, które w przyszłości mają zostać zablokowane lub usunięte z systemu. Aby określić, czy profil użytkownika utracił ważność, należy użyć komendy CHGEXPSCDE.	QASECEXP[2]
8	CHGEXPSCDE	Komenda Zmiana pozycji harmonogramu utraty ważności (Change Expiration Schedule Entry) służy do zaplanowania usunięcia profilu użytkownika. Profil można usunąć tymczasowo (blokując go) lub usunąć go z systemu. Komenda ta używa pozycji harmonogramu zadań, która jest uruchamiana codziennie o godzinie 00:01 (1 minuta po północy). Zadanie sprawdza zbiór QASECEXP, aby określić, czy w danym dniu mają stracić ważność jakieś profile użytkowników. Za pomocą komendy DSPEXPSCD można wyświetlić te profile użytkowników.	QASECEXP[2]
9	PRTPRFINT	Komenda Szczegóły profilu wydruku (Print Profile Internals) służy do drukowania raportu zawierającego informacje dotyczące liczby pozycji znajdujących się w profilu użytkownika. Liczba pozycji określa wielkość profilu użytkownika.	

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 7 opisuje opcje menu i powiązane z nimi komendy służące do kontroli ochrony:

Tabela 7. Komendy narzędzi do kontroli ochrony

Opcja menu[1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
10	CHGSECAUD	Komenda Zmiana kontroli ochrony (Change Security Auditing) służy do konfigurowania kontroli ochrony i zmiany wartości systemowych, które sterują kontrolą ochrony. Po uruchomieniu komendy CHGSECAUD system tworzy kronikę kontroli ochrony (QAUDJRN), jeśli jeszcze nie istnieje. Komenda CHGSECAUD dostarcza opcji, które ułatwiają skonfigurowanie wartości systemowej QAUDLVL (poziom kontroli). Aby uaktywnić wszystkie możliwe ustawienia poziomu kontroli, można podać *ALL. Alternatywnie, aby uaktywnić najczęstsze ustawienia (*AUTFAIL, *CREATE, *DELETE, *SECURITY i *SAVRST), można podać *DFTSET. **Uwaga:** Używając narzędzi ochrony do konfigurowania kontroli, należy zaplanować zarządzanie dziennikami kontroli. W przeciwnym przypadku mogą wkrótce pojawić się problemy z wykorzystaniem dysku.	
11	DSPSECAUD	Komenda Wyświetlenie kontroli ochrony (Display Security Auditing) służy do wyświetlania informacji o kronice kontroli ochrony i wartości systemowych, które sterują kontrolą ochrony.	

Uwagi:

1. Są to opcje z menu SECTOOLS.

Użycie menu Zadania wsadowe ochrony

Poniżej znajduje się pierwsza część menu SECBATCH:

```
SECBATCH
   Wprowadzenie raportów ochrony do zadania wsadowego lub zaplanowanie ich
            (Submit or Schedule Security Reports To Batch)
                                                                    System:
Wybierz jedną z następujących opcji:

  Wprowadzenie raportów do zadania wsadowego
     1. Adoptowanie obiektów
     2. Pozycje kroniki kontroli
     3. Uprawnienia do listy autoryzacji
     4. Uprawnienia do komendy
     5. Uprawnienia prywatne do komendy
     6. Ochrona komunikacji
     7. Uprawnienia do katalogów
     8. Uprawnienia prywatne do katalogów
     9. Uprawnienia do dokumentów
    10. Uprawnienia prywatne do dokumentów
    11. Uprawnienia do zbiorów
    12. Uprawnienia prywatne do zbiorów
    13. Uprawnienia do folderów
```

Po wybraniu opcji z tego menu jest wyświetlany ekran Wprowadzenie zadania (Submit Job - SBMJOB). 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. 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).

Aby wybrać inne ustawienia dla raportu, można ustawić kursor w wierszu *Komenda do wykonania* i nacisnąć klawisz F4 (Podpowiedź). Należy wybrać taką nazwę zadania, aby je rozpoznać podczas wyświetlania pozycji harmonogramu zadań.

Opcje menu Zadania wsadowe ochrony

Tabela 8 opisuje opcje menu i powiązane z nimi komendy dotyczące raportów ochrony.

Generując raporty ochrony, system drukuje tylko informacje spełniające kryteria zarówno podane przez użytkownika, jak i obowiązujące dla narzędzia. Na przykład opisy zadań, które zawierają nazwę profilu użytkownika, są związane z ochroną. W związku z tym raport opisów zadań (PRTJOBDAUT) zawiera opisy zadań w podanej bibliotece tylko wtedy, gdy uprawnienie publiczne dla opisu zadania nie ma wartości *EXCLUDE *oraz* jeśli w opisie zadania, w parametrze USER jest określona nazwa profilu użytkownika.

Podobnie, podczas wyświetlania informacji o podsystemie (komenda PRTSBSDAUT) system uwzględnia informacje o podsystemie tylko wtedy, gdy jego opis zawiera pozycję dotyczącą komunikacji, w której jest podany profil użytkownika.

Jeśli w określonym raporcie jest mniej informacji, niż można się spodziewać, należy skorzystać z pomocy online, aby zapoznać się z kryteriami wyboru raportu.

Tabela 8. Komendy raportów ochrony

Opcja menu[1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
1, 40	PRTADPOBJ	Komenda Drukowanie obiektów adoptujących (Print Adopting Objects) służy do drukowania listy obiektów, które adoptują uprawnienia określonego profilu użytkownika. Można podać pojedynczy profil, nazwę profilu ogólnego (na przykład wszystkie profile zaczynające się od Q) lub wszystkie profile użytkowników w systemie. Ten raport ma dwie wersje. Pełny raport zawiera wszystkie obiekty adoptujące, które spełniają kryteria wyboru. Raport zmian zawiera różnice pomiędzy obiektami adoptującymi, które są obecnie w systemie, a tymi, które były w systemie w momencie poprzedniego generowania raportu.	QSECADPOLD[2]
2, 41	DSPAUDJRNE	Komenda Wyświetlenie pozycji kroniki kontroli (Display Audit Journal Entries) służy do wyświetlania lub drukowania informacji o pozycjach w kronice kontroli ochrony. Można wybrać określone typy pozycji, użytkowników i przedział czasu.	QASYxxJ4[3]

Tabela 8. Komendy raportów ochrony (kontynuacja)

Opcja menu[1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
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, którzy mają uprawnienia do każdej listy, a także uprawnienia, jakie użytkownicy mają do danej listy. Informacje te są pomocne przy analizowaniu źródeł uprawnień do obiektów w systemie. Ten raport ma trzy wersje. Pełny raport zawiera wszystkie listy autoryzacji w systemie. Raport zmian zawiera dodatki i zmiany do autoryzacji od ostatniego generowania raportu. Raport usunięć zawiera użytkowników, których uprawnienia do listy autoryzacji zostały zmienione od ostatniego generowania raportu. Przy drukowaniu pełnego raportu jest możliwość wydrukowania listy obiektów, które każda lista autoryzacji chroni. 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]
15, 54	PRTJOBDAUT	Komenda Drukowanie uprawnień dla JOBD (Print Job Description Authority) służy do drukowania listy opisów zadań, które zawierają profile użytkowników i których uprawnienie publiczne ma wartość inną niż *EXCLUDE. Raport zawiera uprawnienia specjalne dla profilu użytkownika, który jest określony 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]

Tabela 8. Komendy raportów ochrony (kontynuacja)

Opcja menu[1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
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 podaje się typ obiektu i bibliotekę lub biblioteki dla raportu. Komendy PRTPUBAUT należy używać do uzyskiwania informacji o obiektach, do których każdy użytkownik w systemie ma dostęp. Ten raport ma dwie wersje. Pełny raport zawiera wszystkie obiekty, które spełniają kryteria wyboru. Raport zmian zawiera różnice pomiędzy obiektami, które są obecnie w systemie, a obiektami (tego samego typu i w tej samej bibliotece), które były w systemie w momencie poprzedniego generowania raportu.	QPBxxxxxx[5]
Patrz uwaga 5	PRTPVTAUT	Komenda Drukowanie uprawnień prywatnych (Print Private Authorities) służy do drukowania listy uprawnień prywatnych do obiektów określonego typu w określonej bibliotece. Można go użyć do określenia źródła uprawnienia do obiektu. Ten raport ma trzy wersje. Pełny raport zawiera wszystkie obiekty, które spełniają kryteria wyboru. Raport zmian zawiera różnice pomiędzy obiektami, które są obecnie w systemie, a obiektami (tego samego typu i w tej samej bibliotece), które były w systemie w momencie poprzedniego generowania raportu. Raport usunięć zawiera użytkowników, których uprawnienia do obiektu zostały zmienione od ostatniego drukowania raportu.	QPVxxxxxx[5]
24, 63	PRTQAUT	Komenda Drukowanie uprawnień dla kolejki (Print Queue Report) służy do drukowania ustawień ochrony dla kolejek wyjściowych i kolejek zadań w systemie. Ustawienia te określają, kto może przeglądać i zmieniać pozycje w kolejce wyjściowej lub kolejce zadań. Ten raport ma dwie wersje. Pełny raport zawiera wszystkie obiekty kolejki wyjściowej i kolejki zadań, które spełniają kryteria wyboru. Raport zmian zawiera różnice pomiędzy obiektami kolejki wyjściowej i kolejki zadań, które są obecnie w systemie, a tymi, które były w systemie w momencie poprzedniego generowania raportu.	QSECQOLD[2]

Tabela 8. Komendy raportów ochrony (kontynuacja)

Opcja menu[1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
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 pomiędzy 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 wyzwalanych (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]
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, hasłach i poziomach haseł.	
30, 69	PRTPRFINT	Komenda Szczegóły profilu wydruku (Print Profile Internals) służy do drukowania raportu zawierającego szczegółowe informacje dotyczące wielu pozycji.	

Tabela 8. Komendy raportów ochrony (kontynuacja)

Opcja menu[1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
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. Książka *iSeries Ochrona* zawiera więcej informacji o komendzie CHKOBJITG.	

Uwagi:

1. Są to opcje z menu SECBATCH.
2. Zbiór ten znajduje się w bibliotece QUSRSYS.
3. xx jest dwuznakowym typem pozycji kroniki. Na przykład modelowy plik wyjściowy pozycji kroniki AE to QSYS/QASYAEJ4. Modelowe pliki wyjściowe są opisane w Dodatku F książki *iSeries Ochrona*.
4. Menu SECBATCH 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.
5. Menu SECBATCH zawiera opcje dla typów obiektu, które zwykle leżą w obszarze zainteresowań administratorów ochrony. Na przykład opcje 12 i 51 uruchamiają komendę PRTPVTAUT dla obiektów *FILE. Opcje ogólne (19 i 58) służą do podania typu obiektu.
6. Znaki xxxxxx w nazwie zbioru określają typ obiektu. Na przykład zbiór dla obiektów programów nazywa się QPBPGM dla uprawnień publicznych i QPVPGM dla uprawnień prywatnych. Zbiory te znajdują się w bibliotece QUSRSYS.

   Zbiór zawiera podzbiór dla każdej biblioteki, w której wydrukowano raport. Nazwa podzbioru jest taka sama, jak nazwa biblioteki.

Komendy dostosowywania ochrony

Tabela 9 opisuje komendy, których można użyć, aby dostosować ochronę w systemie. Opcje znajdują się w menu SECTOOLS.

Tabela 9. Komendy dostosowywania systemu

Opcja menu[1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
60	CFGSYSSEC	Komenda Konfigurowanie ochrony systemu (Configure System Security) służy do ustawiania zalecanych wartości systemowych dotyczących ochrony. Komenda ta konfiguruje również kontrolę ochrony w systemie. Sekcja “Wartości ustawiane przez komendę Konfigurowanie ochrony systemu” na stronie 38 opisuje działanie komendy. **Uwaga:** Aby zapoznać się z zaleceniami dotyczącymi ochrony w odniesieniu do konkretnej sytuacji, należy zamiast tej komendy uruchomić Kreator ochrony iSeries lub iSeries Security Advisor. Rozdział 2, “Kreator ochrony iSeries i eServer Security Planner”, na stronie 11 zawiera informacje na temat tych narzędzi.	
61	RVKPUBAUT	Komenda Odwołanie uprawnień publicznych (Revoke Public Authority) służy do ustawienia uprawnienia publicznego *EXCLUDE dla zestawu istotnych dla ochrony komend. Sekcja “Funkcje komendy Odwołanie uprawnień publicznych” na stronie 40 zawiera listę czynności wykonywanych przez komendę RVKPUBAUT.	

Tabela 9. Komendy dostosowywania systemu (kontynuacja)

Opcja menu[1]	Nazwa komendy	Opis	Użyty zbiór bazy danych
Uwagi: 1. Są to opcje z menu SECTOOLS.			

Wartości ustawiane przez komendę Konfigurowanie ochrony systemu

Tabela 10 zawiera wartości systemowe, które są ustawiane po uruchomieniu komendy CFGSYSSEC. Komenda CFGSYSSEC uruchamia program o nazwie QSYS/QSECCFGS.

Tabela 10. Wartości ustawiane przez komendę CFGSYSSEC

Nazwa wartości systemowej	Ustawienie	Opis wartości systemowej
QALWOBJRST	*NONE	Określa, czy programy systemowe i programy adoptujące uprawnienia mogą być odtwarzane.
QAUTOCFG	0 (Nie)	Automatyczne konfigurowanie nowych urządzeń.
QAUTOVRT	0	Liczba opisów urządzeń wirtualnych, które system automatycznie utworzy, jeśli nie ma dostępnego urządzenia.
QDEVRCYACN	*DSCMSG (odłączenie z komunikatem)	Działanie podejmowane po ponownym nawiązaniu komunikacji.
QDSCJOBITV	120	Czas, po którym system podejmie działanie wobec odłączonego zadania.
QDSPSGNINF	1 (tak)	Określa, czy jest wyświetlany ekran z informacjami o wpisaniu się.
QINACTITV	60	Czas, po którym system podejmie działanie wobec nieaktywnego zadania interaktywnego.
QINACTMSGQ	*ENDJOB	Działanie podejmowane przez system wobec nieaktywnego zadania.
QLMTDEVSSN	1 (tak)	Określa, czy użytkownicy mogą wpisywać się tylko z jednego urządzenia jednocześnie.
QLMTSECOFR	1 (tak)	Określa, czy użytkownicy *ALLOBJ i *SERVICE mają uprawnienia ograniczone do określonych urządzeń.
QMAXSIGN	3	Liczba dopuszczalnych nieudanych prób wpisania się.
QMAXSGNACN	3 (oba)	Określa, czy system blokuje stację roboczą, czy profil użytkownika, gdy zostanie osiągnięty limit określony w wartości QMAXSIGN.
QRMTSIGN	*FRCSIGNON	Sposób obsługi zdalnych (tranzyt lub TELNET) prób wpisania się.
QRMTSVRATR	0 (wyłączone)	Umożliwia zdalne analizowanie systemu.
QSECURITY 1 na stronie 39	50	Wymuszony poziom ochrony.
QVFYOBJRST	3 (Sprawdzenie podpisu podczas odtwarzania)	Sprawdzenie obiektu podczas odtwarzania.
QPWDEXPITV	60	Częstotliwość wymaganych zmian haseł użytkowników.
QPWDMINLEN	6	Minimalna długość haseł.
QPWDMAXLEN	8	Maksymalna długość haseł.
QPWDPOSDIF	1 (tak)	Określa, czy znak w każdej pozycji w nowym haśle musi być różny od znaku w tej samej pozycji w poprzednim haśle.
QPWDLMTCHR	Patrz uwaga	Znaki niedozwolone w hasłach.
QPWDLMTAJC	1 (tak)	Określa, czy w hasłach są zabronione przylegające cyfry.

Tabela 10. Wartości ustawiane przez komendę CFGSYSSEC (kontynuacja)

Nazwa wartości systemowej	Ustawienie	Opis wartości systemowej
QPWDLMTREP	2 (nie mogą powtarzać się w kolejności)	Określa, czy znaki mogą powtarzać się w haśle.
QPWDRQDDGT	1 (tak)	Określa, czy w haśle musi być co najmniej jedna cyfra.
QPWDRQDDIF	1 (32 unikalne hasła)	Określa, ile różnych haseł należy ustawić przed ustawieniem takiego samego hasła.
QPWDVLDPGM	*NONE	Program obsługi wyjścia wywoływany przez system w celu sprawdzenia poprawności haseł.

Uwagi:

1. Jeśli bieżąca wartość QSECURITY wynosi 40 lub mniej, należy przed przejściem na wyższy poziom ochrony przeczytać informacje w Rozdziale 2 książki *iSeries Ochrona*.
2. Zabronione znaki są przechowywane w komunikacie o ID CPXB302 w zbiorze komunikatów QSYS/QCPFMSG. Domyślna wartość to AEIOU@$#. Znaki te można zmieniać za pomocą komendy Zmiana opisu komunikatu (Change Message Description - CHGMSGD). Wartość systemowa QPWDLMTCHR nie jest wymuszana na poziomie haseł 2 i 3.

Komenda CFGSYSSEC ustawia hasło na *NONE także dla poniższych profili użytkowników:

QSYSOPR

QPGMR

QUSER

QSRV

QSRVBAS

Wreszcie, komenda CFGSYSSEC ustawia kontrolę ochrony za pomocą komendy Zmiana kontroli ochrony (Change Security Auditing - CHGSECAUD). Komenda CFGSYSSEC włącza kontrolę czynności i obiektów, a także określa domyślny zestaw działań kontroli dla komendy CHGSECAUD.

Dostosowanie programu

Jeśli niektóre z tych ustawień nie są odpowiednie dla określonej instalacji, można utworzyć własną wersję programu obsługującego komendę, wykonując poniższe czynności:

__ Krok 1. Za pomocą komendy Odtworzenie źródła CL (Retrieve CL Source - RTVCLSRC) skopiuj źródła programu uruchamianego przez komendę CFGSYSSEC. Należy wczytać program QSYS/QSECCFGS. Następnie zmień jego *nazwę*.

__ Krok 2. Wprowadź do programu odpowiednie zmiany. Następnie skompiluj go. Upewnij się, że *nie* zastępujesz dostarczonego przez IBM programu QSYS/QSECCFGS. Nowy program powinien mieć inną nazwę.

__ Krok 3. Za pomocą komendy Zmiana komendy (Change Command - CHGCMD) zmień parametr Program do przetwarzania komend (PGM) komendy CFGSYSSEC. Wartością parametru PGM powinna być nazwa nowego programu. Na przykład, jeśli tworzysz program o nazwie MYSECCFG w bibliotece QGPL, wpisz:

```
CHGCMD CMD(QSYS/CFGSYSSEC) PGM(QGPL/MYSECCFG)
```

Uwaga: Jeśli zmieniasz program QSYS/QSECCFGS, IBM nie gwarantuje niezawodności, funkcjonalności ani prawidłowego działania tego programu. Domniemane gwarancje przydatności do określonego celu nie są udzielane.

Funkcje komendy Odwołanie uprawnień publicznych

Za pomocą komendy Odwołanie uprawnień publicznych (Revoke Public Authority - RVKPUBAUT) można ustawiać uprawnienie publiczne *EXCLUDE dla zestawu komend i programów. Komenda RVKPUBAUT uruchamia program o nazwie QSYS/QSECRVKP. Domyślnym działaniem programu QSECRVKP jest odwoływanie uprawnień publicznych (poprzez ustawienie ich na wartość *EXCLUDE) dla komend, które zawiera Tabela 11, i aplikacyjnych interfejsów programowych (API), które zawiera Tabela 12. System jest dostarczany z uprawnieniami publicznymi dla tych funkcji API i komend na *USE.

Komendy, które zawiera Tabela 11, i funkcje API, które zawiera Tabela 12, wykonują czynności, które nieodpowiednio użyte mogą spowodować szkody w systemie. Administrator ochrony powinien udzielać osobnych uprawnień do uruchamiania tych komend i nie udostępniać ich wszystkim użytkownikom.

Podczas uruchamiania komendy RVKPUBAUT podaje się bibliotekę, która zawiera komendy. Domyślną biblioteką jest QSYS. Jeśli w systemie jest więcej języków narodowych, należy uruchomić tę komendę dla każdej biblioteki QSYSxxx.

Tabela 11. Komendy, do których uprawnienia publiczne są ustawiane przez komendę RVKPUBAUT

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

Wszystkie funkcje API, które zawiera Tabela 12, znajdują się w bibliotece QSYS:

Tabela 12. Programy, do których uprawnienia publiczne są ustawiane przez komendę RVKPUBAUT

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

Gdy gdy jest uruchamiana komenda RVKPUBAUT, system ustawia uprawnienia publiczne do katalogu głównego na *USE (chyba że już ma on uprawnienie *USE lub mniejsze).

Dostosowanie programu

Jeśli niektóre z tych ustawień nie są odpowiednie dla określonej instalacji, można utworzyć własną wersję programu obsługującego komendę, wykonując poniższe czynności:

__ Krok 1. Za pomocą komendy Odtworzenie źródła CL (Retrieve CL Source - RTVCLSRC) skopiuj źródła programu uruchamianego przez komendę RVKPUBAUT. Należy wczytać program QSYS/QSECRVKP. Następnie zmień jego *nazwę*.

__ Krok 2. Wprowadź do programu odpowiednie zmiany. Następnie skompiluj go. Upewnij się, że *nie* zastępujesz dostarczonego przez IBM programu QSYS/QSECRVKP. Nowy program powinien mieć inną nazwę.

__ Krok 3. Za pomocą komendy Zmiana komendy (Change Command - CHGCMD) zmień parametr Program do przetwarzania komend (PGM) komendy RVKPUBAUT. Wartością parametru PGM powinna być nazwa nowego programu. Na przykład jeśli tworzysz program o nazwie MYRVKPGM w bibliotece QGPL, wpisz:

```
CHGCMD CMD(QSYS/RVKPUBAUT) PGM(QGPL/MYRVKPGM)
```

Uwaga: Jeśli zmieniasz program QSYS/QSECRVKP, IBM nie gwarantuje niezawodności, funkcjonalności ani prawidłowego działania tego programu. Domniemane gwarancje przydatności do określonego celu nie są udzielane.

Część 2. Zaawansowana ochrona serwera iSeries

Rozdział 5. Zabezpieczenie ważnych informacji poprzez uprawnienia do obiektu

Zadaniem administratora ochrony jest zabezpieczenie informacji dostępnych w danej organizacji w taki sposób, aby nie przeszkadzać użytkownikom systemu. Należy nadać użytkownikom uprawnienia wystarczające, aby mogli wykonywać swoje zadania, a jednocześnie, aby nie mieli zbyt szerokich uprawnień w systemie i nie wykonywali niedozwolonych zmian.

Wskazówka dotycząca ochrony

Zbyt restrykcyjne uprawnienia mogą mieć odwrotny skutek. Czasami użytkownicy w odpowiedzi na ograniczenia uprawnień wymieniają się między sobą hasłami.

System operacyjny OS/400 udostępnia zintegrowaną ochronę obiektów. Użytkownicy, aby uzyskać dostęp do obiektów, muszą używać interfejsów udostępnionych w systemie. Na przykład jeśli trzeba uzyskać dostęp do zbioru bazy danych, należy użyć komend lub programów przeznaczonych do tego celu. Nie można używać komendy przeznaczonej do uzyskiwania dostępu do kolejki komunikatów lub protokołu zadania.

Za każdym razem, gdy użytkownik używa interfejsu systemowego do uzyskiwania dostępu do obiektu, system sprawdza, czy ma on uprawnienia, które są wymagane przez ten interfejs. Uprawnienie do obiektu jest skutecznym i elastycznym narzędziem do ochrony informacji w systemie. Zadaniem administratora ochrony jest skonfigurowanie efektywnego schematu ochrony, łatwego w obsłudze i w zarządzaniu.

Wymuszanie uprawnień do obiektu

Za każdym razem, gdy uzyskuje się dostęp do obiektu, system operacyjny sprawdza uprawnienie do tego obiektu. Jednak jeśli poziom ochrony w systemie (wartość systemowa QSECURITY) jest ustawiony na 10 lub 20, każdy użytkownik automatycznie ma uprawnienie do dostępu do każdego obiektu, ponieważ każdy profil użytkownika ma uprawnienie specjalne *ALLOBJ.

Wskazówka dotycząca uprawnienia do obiektu: Aby sprawdzić, czy w systemie używane są uprawnienia do obiektów, należy sprawdzić wartość systemową QSECURITY (poziom ochrony). Jeśli QSECURITY wynosi 10 lub 20, uprawnienia do obiektów nie są używane.

Do zmiany poziomu ochrony na 30 lub wyższy należy się odpowiednio przygotować. Jeśli się tego nie zrobi, użytkownicy mogą nie mieć dostępu do informacji, których potrzebują.

Temat **Planowanie ochrony i ochrona systemu - podstawy** w Centrum informacyjnym opisuje metodę analizy używanych aplikacji i wybierania sposobu skonfigurowania ochrony obiektów. Jeśli ochrona obiektów nie jest jeszcze używana lub jeśli schemat ochrony obiektów jest przestarzały i niejasny, należy przeczytać ten temat. Lektura ta z pewnością pomoże w rozpoczęciu pracy.

Ochrona menu

Serwer iSeries zaprojektowano jako następcę produktów S/36 i S/38. Wiele instalacji iSeries było kiedyś instalacjami S/36 lub S/38. Do kontroli możliwości użytkowników administratorzy ochrony tych wcześniejszych systemów często używali techniki określanej jako **ochrona menu** lub **kontrola dostępu do menu**.

Kontrola dostępu do menu oznacza, że po wpisaniu się danego użytkownika wyświetlane jest określone menu. Użytkownik może wykonać tylko te funkcje, które są dostępne w menu. Nie może natomiast dostać się do wiersza komend w systemie, aby wykonać funkcje niedostępne w menu. Teoretycznie administrator ochrony nie musi się martwić o uprawnienia do obiektów, ponieważ menu i programy sterują zakresem działań użytkowników.

Serwer iSeries udostępnia opcje profilu użytkownika pomagające w kontroli dostępu przez menu. Podane są one poniżej:

- Parametr **Menu początkowe** (INLMNU) służy do określania, które menu użytkownik widzi po wpisaniu się.
- Parametr **Program początkowy** (INLPGM) służy do uruchamiania programu konfiguracyjnego, zanim użytkownik zobaczy menu. Parametru INLPGM można również użyć, aby ograniczyć możliwości użytkownika do pojedynczego programu.
- Parametr **Ograniczenie możliwości** (LMTCPB) służy do ograniczenia zestawu komend, których może używać użytkownik. Ponadto uniemożliwia on użytkownikowi podanie innego programu początkowego lub menu na ekranie Wpisanie się (Sign On). (Parametru LMTCPB można używać tylko do ograniczania dostępu do komend wpisywanych w wierszu komend).

Ograniczenia kontroli dostępu do menu

Komputery i ich użytkownicy znacznie się zmienili w ciągu kilku ostatnich lat. Dostępnych jest wiele narzędzi, takich jak programy do tworzenia zapytań, arkusze kalkulacyjne, tak więc użytkownicy sami niekiedy programują, aby odciążyć programistów. Niektóre narzędzia, takie jak SQL czy ODBC, umożliwiają przeglądanie informacji oraz ich zmianę. Udostępnienie tych narzędzi poprzez strukturę menu jest bardzo trudnym zadaniem.

Stacje robocze pełniące stałą funkcję (“zielone ekrany”) są gwałtownie zastępowane przez komputery osobiste i sieci połączonych ze sobą komputerów. Jeśli system jest podłączony do sieci, użytkownicy mogą mieć dostęp do tego systemu bez konieczności użycia ekranu wpisania się lub menu.

Administrator ochrony próbujący stosować kontrolę dostępu do menu staje przed dwoma podstawowymi problemami:

- Jeśli uda się ograniczyć możliwości użytkowników do używania menu, będą oni prawdopodobnie niezadowoleni, ponieważ ogranicza się ich dostęp do współczesnych narzędzi.
- Jeśli nie uda się to, narazi się newralgiczne informacje, które kontrola dostępu do menu ma chronić. Jeśli system jest włączony do sieci, maleje możliwość stosowania kontroli dostępu do menu. Na przykład parametr LMTCPB stosuje się tylko do komend wpisywanych w wierszu komend podczas sesji interaktywnej. Parametr ten nie jest skuteczny w przypadku żądań z sesji komunikacji, takich jak przesyłanie plików PC, FTP i zdalne komendy.

Rozwinięcie kontroli dostępu do menu o ochronę obiektów

Ze względu na pojawienie się wielu nowych opcji służących do łączenia się z systemami, skuteczny schemat ochrony serwera iSeries nie może opierać się jedynie na kontroli dostępu do menu. Niniejszy temat zawiera sugestie dotyczące przejścia do środowiska ochrony obiektów w celu uzupełnienia kontroli dostępu do menu.

Temat *Planowanie ochrony i ochrona systemu - podstawy* w Centrum informacyjnym opisuje technikę analizy uprawnień do obiektów potrzebnych użytkownikom do uruchamiania aplikacji. Po wykonaniu analizy należy przypisać użytkowników do grup i nadać grupom odpowiednie uprawnienia. Podejście to jest rozsądne i logiczne. Jednak jeśli system działa od wielu lat i dostępnych jest w nim wiele aplikacji, zadanie ich przeanalizowania, a następnie skonfigurowania uprawnień do obiektów wydaje się przytłaczające.

Wskazówka dotycząca uprawnień do obiektów: obecnie dostępne menu w połączeniu z programami adoptującymi uprawnienia właściciela tego programu mogą tworzyć środowisko przejściowe uzupełniające kontrolę dostępu do menu. Należy zabezpieczyć programy adoptujące uprawnienia i profile użytkowników będących ich właścicielami.

Aby skonfigurować środowisko przejściowe, można użyć obecnie dostępnych menu, stopniowo analizując używane aplikacje i obiekty. W przykładzie poniżej wykorzystano menu Zarządzanie zamówieniami (Order Entry - OEMENU), oraz powiązane z nim zbiory i programy.

Przykład: konfigurowanie środowiska przejściowego

W podanym przykładzie przyjęto, że:

- wszystkie zbiory znajdują się w bibliotece ORDERLIB,
- nie są znane nazwy wszystkich zbiorów; nie są również znane uprawnienia, których wymagają opcje menu dla różnych zbiorów,
- menu i wszystkie programy przez nie wywoływane znajdują się w bibliotece o nazwie ORDERPGM,
- wszyscy, którzy mogą wpisać się do systemu, mają mieć możliwość przeglądania informacji (za pomocą zapytań lub arkuszy kalkulacyjnych) we wszystkich zbiorach zamówień, zbiorach klientów i zbiorach z pozycjami,
- tylko użytkownicy, dla których aktualnym menu wpisania się jest OEMENU, mają mieć możliwość zmiany danych w zbiorach; ponadto muszą w tym celu używać programów dostępnych poprzez menu,
- użytkownicy systemu, oprócz administratorów ochrony nie mają uprawnienia specjalnego *ALLOBJ lub *SECADM.

Aby zmienić opisane środowisko kontroli dostępu do menu tak, aby można było używać zapytań, wykonaj następujące kroki:

__ Krok 1. Przygotuj listę użytkowników, dla których menu początkowym jest OEMENU.

Aby otrzymać środowisko dla każdego profilu użytkownika w systemie, można użyć komendy Drukowanie profilu użytkownika (Print User Profile - PRTUSRPRF *ENVINFO). Wydruk zawiera menu początkowe, program początkowy i bibliotekę bieżącą. Rys. 7 na stronie 62 przedstawia przykładowy raport.

__ Krok 2. Sprawdź, czy właścicielem obiektu OEMENU (może to być obiekt *PGM lub *MENU) jest profil użytkownika, nieużywany do wpisania się. Profil użytkownika powinien być wyłączony lub mieć hasło *NONE. W niniejszym przykładzie przyjęto, że OEOWNER jest właścicielem obiektu programu OEMENU.

__ Krok 3. Sprawdź, czy profil użytkownika będący właścicielem obiektu programu OEMENU nie jest profilem grupowym. Można użyć poniższej komendy:

```
DSPUSRPRF USRPRF(OEOWNER) TYPE(*GRPMBR)
```

__ Krok 4. Zmień program OEMENU tak, aby adoptował uprawnienie profilu użytkownika OEOWNER. (Aby zmienić wartość parametru USRPRF na *OWNER, użyj komendy CHGPGM).

Uwaga: Obiekty *MENU nie mogą adoptować uprawnień. Jeśli OEMENU jest obiektem *MENU, można zaadoptować przykład:

- tworząc program wyświetlający menu, albo
- używając uprawnień adoptowanych dla programów uruchamianych, gdy użytkownik wybiera opcję z menu OEMENU.

__ Krok 5. Ustaw uprawnienia publiczne dla wszystkich zbiorów w ORDERLIB na *USE, wpisując dwie poniższe komendy:

```
RVKOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
     AUT(*ALL)
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
     AUT(*USE)
```

Należy pamiętać, że uprawnienie *USE daje użytkownikom możliwość kopiowania zbiorów za pomocą przesyłania plików PC lub protokołu FTP.

__ Krok 6. Profilowi będącemu właścicielem programu menu nadaj uprawnienie *ALL do zbiorów, wpisując:

```
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(OEOWNER)
     AUT(*ALL)
```

W przypadku większości aplikacji uprawnienie do zbiorów *CHANGE jest wystarczające. Aplikacje mogą jednak wykonywać funkcje, takie jak usuwanie zawartości podzbiorów zbioru fizycznego, wymagające szerszych uprawnień niż *CHANGE. Ewentualnie przeanalizuj aplikacje i nadaj tylko minimalne uprawnienia wymagane przez tę aplikację. Jednak w okresie przejściowym stosując uprawnienia *ALL można uniknąć awarii aplikacji spowodowanych niewystarczającymi uprawnieniami.

__ Krok 7. Ogranicz uprawnienia do programów w bibliotece zamówień, wpisując:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(*PUBLIC)
     AUT(*EXCLUDE)
```

__ Krok 8. Nadaj profilowi OEOWNER uprawnienie do programów w bibliotece, wpisując:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(OEOWNER)
     AUT(*USE)
```

__ Krok 9. Nadaj użytkownikom określonym w kroku 1 uprawnienia do programu menu, wpisując dla każdego użytkownika:

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
          USER(nazwa-profilu-użytkownika) AUT(*USE)
```

Po wykonaniu powyższych kroków wszyscy użytkownicy systemu, którzy nie są jawnie wykluczeni, mają dostęp do zbiorów (bez możliwości ich zmiany) w bibliotece ORDERLIB. Użytkownicy mający uprawnienia do programu OEMENU mogą teraz używać programów dostępnych w menu do aktualizacji zbiorów w bibliotece ORDERLIB. Tylko użytkownicy mający uprawnienia do programu OEMENU nie mogą zmieniać zbiorów w tej bibliotece. Połączenie ochrony obiektów i dostępu do menu chroni zbiory.

Po wykonaniu analogicznych kroków dla wszystkich bibliotek zawierających dane użytkowników powstanie prosty schemat sterowania aktualizacjami baz danych. Opisana metoda uniemożliwia użytkownikom systemu aktualizację zbiorów baz danych, chyba że używają dopuszczalnych menu i programów. Jednocześnie udostępniono zbiory bazy danych do przeglądania, analizowania i kopiowania przez użytkowników za pomocą narzędzi wspomagających podejmowanie decyzji lub połączeń z innych systemów i komputerów PC.

Wskazówka dotycząca uprawnienia do obiektu: Jeśli system znajduje się w sieci, uprawnienie *USE może dawać większe możliwości, niż oczekiwano. Na przykład za pomocą FTP można skopiować zbiór do innego systemu (w tym do komputera PC), jeśli ma się uprawnienie *USE do tego zbioru.

Używanie ochrony biblioteki do całkowitej ochrony menu

Aby mieć dostęp do obiektu w bibliotece, należy mieć uprawnienia zarówno do obiektu, jak i do biblioteki. W przypadku większości operacji wymagane jest uprawnienie *EXECUTE lub *USE do biblioteki.

W zależności od konkretnej sytuacji można użyć uprawnienia do biblioteki jako prostego środka do ochrony obiektów. Na przykład, załóżmy, że w Menu zarządzania obiektami (Order Entry Menu) wszyscy, którzy mają do niego uprawnienie, mogą używać wszystkich programów w bibliotece ORDERPGM. Zamiast chronienia pojedynczych programów można ustawić uprawnienie publiczne do biblioteki ORDERPGM na *EXCLUDE. Następnie można nadać uprawnienie *USE do biblioteki konkretnym profilom użytkowników, które umożliwią używanie programów w bibliotece. (Przyjęto, że uprawnienie publiczne do programów to *USE lub uprawnienie szersze).

Uprawnienie do biblioteki może być prostą i skuteczną metodą administrowania uprawnieniami do obiektów. Należy jednak znać zawartość chronionych bibliotek, aby nie umożliwiać nienadzorowanego dostępu do obiektów.

Konfigurowanie praw własności do obiektu

Prawo własności do obiektów jest ważną częścią schematu uprawnień do obiektów. Domyślnie właściciel obiektu ma uprawnienie *ALL do obiektu. Rozdział 5 w książce *iSeries Ochrona* zawiera przykłady i rekomendacje dotyczące planowania praw własności do obiektów. Tutaj podajemy kilka wskazówek.

- Ogólnie profile grupowe nie powinny być właścicielami obiektów. Jeśli profil grupowy jest właścicielem obiektu, wszyscy członkowie grupy mają uprawnienie *ALL do obiektu, chyba że członek grupy zostanie jawnie wyłączony.
- Jeśli używane są uprawnienia adoptowane, należy rozważyć, czy profile użytkownika będące właścicielami programów mają być także właścicielami obiektów aplikacji, takich jak zbiory. Można rozważyć, czy użytkownicy uruchamiający programy adoptujące uprawnienia mają mieć uprawnienie *ALL do zbiorów.

Jeśli używa się programu iSeries Navigator, zadania opisane powyżej można wykonać używając **strategii** ochrony. Więcej informacji zawiera Centrum informacyjne iSeries (patrz sekcja “Informacje wstępne i pokrewne” na stronie xii).

Uprawnienia do obiektów komend systemu i programów

Poniżej podano kilka sugestii dotyczących ograniczania uprawnień do obiektów dostarczonych przez IBM.

- Jeśli w systemie jest więcej niż jeden język narodowy, system ma więcej niż jedną bibliotekę systemową (QSYS). System ma bibliotekę QSYSxxxx dla każdego zainstalowanego języka narodowego. Jeśli do sterowania dostępem do komend systemu używane są uprawnienia do obiektów, należy zabezpieczyć komendę w bibliotece QSYS i we wszystkich bibliotekach QSYSxxx w systemie.
- Biblioteka systemu System/38 niekiedy udostępnia komendę o działaniu takim samym, jak działanie komendy, której stosowanie się ogranicza. Należy pamiętać o ograniczeniu równoważnej komendy w bibliotece QSYS38.
- W środowisku System/36 należy ograniczyć programy dodatkowe, na przykład program QY2FTML zapewniający przesyłanie plików w tym systemie.

Kontrola funkcji ochrony

Rozdział ten opisuje techniki kontroli efektywności ochrony w systemie. Kontrolowanie ochrony systemu może mieć kilka celów:

- Określenie, czy plan ochrony jest kompletny.
- Upewnienie się, że planowane elementy sterujące ochroną są na swoim miejscu i działają poprawnie. Ten typ kontroli jest zwykle realizowany przez szefa ochrony w ramach codziennych czynności administracyjnych. Może on także być wykonywany, czasami w sposób bardziej szczegółowy, w ramach okresowego badania ochrony przez pracowników przedsiębiorstwa lub firmy zewnętrzne.
- Upewnienie się, że ochrona systemu dotrzymuje kroku zmianom w środowisku systemu. Przykładowe zmiany, które mają wpływ na ochronę:
  - nowe obiekty tworzone przez użytkowników systemu,
  - nowi użytkownicy mający uprawnienia w systemie,
  - zmiana praw własności do obiektu (nieodpowiednie uprawnienia),
  - zmiana kompetencji (grupy, do której należy użytkownik),
  - uprawnienie tymczasowe (nieunieważnione w odpowiednim momencie),
  - zainstalowanie nowych produktów.
- Przygotowanie się na zdarzenie w przyszłości, jak na przykład instalację nowej aplikacji, zmianę poziomu ochrony lub instalację sieci.

Techniki opisane w tym rozdziale dotyczą wszystkich tych sytuacji. Dobór kontrolowanych elementów oraz częstotliwość kontrolowania zależą od wielkości organizacji i potrzeb związanych z ochroną. Celem tego rozdziału jest omówienie następujących kwestii: jakie informacje są dostępne, jak je uzyskać i dlaczego są potrzebne, a nie udzielenie wskazówek dotyczących częstotliwości kontroli.

Ten rozdział składa się z trzech części:

- Lista kontrolna elementów ochrony, które można planować i kontrolować.
- Informacje o konfigurowaniu i używaniu systemowej kroniki kontroli.
- Inne dostępne techniki gromadzenia informacji o ochronie w systemie.

Kontrola ochrony wymaga użycia komend systemu iSeries i korzystania z informacji protokołu i kroniki w systemie. Warto utworzyć specjalny profil dla osoby, która będzie wykonywała kontrolę ochrony systemu. Profil ten, aby mógł zmieniać charakterystykę kontroli w systemie, wymaga uprawnienia specjalnego *AUDIT. Niektóre zadania kontroli zalecane w tym rozdziale wymagają profilu użytkownika z uprawnieniami specjalnymi *ALLOBJ i *SECADM. Po zakończeniu okresu kontroli należy upewnić się, że hasło tego profilu zostało ustawione na *NONE.

Szczegółowe informacje o kontroli ochrony zawiera Rozdział 9 książki *Ochrona*.

Analiza profili użytkowników

Komenda Wyświetlenie uprawnionych użytkowników (Display Authorized Users - DSPAUTUSR) umożliwia wyświetlenie lub wydrukowanie pełnej listy wszystkich użytkowników w systemie. Lista może być posortowana według nazwy profilu lub profilu grupowego. Poniższy przykład przedstawia listę posortowaną według profilu grupowego:

```
                    Wyświetlenie uprawnionych użytkowników
                         (Display Authorized Users)

Hasło       Profil      Ostatnia  Brak
grupy       użytkownika zmiana    hasła     Tekst
DPTSM
            ANDERSOR    08/04/0x            Roger Anders
            VINCENTM    09/15/0x            Mark Vincent
DPTWH
            ANDERSOR    08/04/0x            Roger Anders
            WAGNERR     09/06/0x            Rose Wagner
QSECOFR
            JONESS      09/20/0x            Sharon Jones
            HARRISOK    08/29/0x            Ken Harrison
*NO GROUP
            DPTSM       09/05/0x    X       Sales and Marketing
            DPTWH       08/13/0x    X       Warehouse
            RICHARDS    09/05/0x            Janet Richards
            SMITHJ      09/18/0x            John Smith
```

Drukowanie wybranych profili użytkowników

Utworzony za pomocą komendy Wyświetlenie profilu użytkownika (Display User Profile - DSPUSRPRF) zbiór wyjściowy można przetwarzać za pomocą narzędzia zapytań.

```
DSPUSRPRF USRPRF(*ALL) +
          TYPE(*BASIC) OUTPUT(*OUTFILE)
```

Narzędzie zapytań pozwala utworzyć wiele różnych raportów z analizy zbioru wyjściowego, na przykład:

- listę wszystkich użytkowników mających uprawnienia specjalne *ALLOBJ i *SPLCTL,
- listę wszystkich użytkowników posortowaną według dowolnego pola w profilu użytkownika, na przykład według programów początkowych lub klas użytkowników.

Można tworzyć programy zapytań generujące na podstawie utworzonego zbioru wyjściowego różne raporty. Na przykład:

- wyświetlić wszystkie profile użytkowników z uprawnieniami specjalnymi, wybierając rekordy, w których pole UPSPAU jest różne od *NONE,
- wyświetlić wszystkich użytkowników, którzy mogą uruchamiać komendy, wybierając rekordy, w których pole *Ograniczenie możliwości* (o nazwie UPLTCP w modelowym zbiorze wyjściowym bazy danych) ma wartość *NO lub *PARTIAL,
- wyświetlać wszystkich użytkowników z określonym menu lub programem początkowym,
- wyświetlać użytkowników nieaktywnych na podstawie pola z datą ostatniego wpisania się.

Sprawdzanie dużych profili użytkowników

Przypadkowo rozmieszczone w systemie profile użytkowników o dużej liczbie uprawnień są oznaką źle zaplanowanej ochrony. Poniżej opisano jedną z metod odnajdywania dużych profili użytkowników i ich oceny:

1. Użyj komendy Wyświetlenie opisu obiektu (Display Object Description - DSPOBJD), aby utworzyć zbiór wyjściowy zawierający informacje o wszystkich profilach użytkowników w systemie:

   ```
   DSPOBJD OBJ(*ALL) OBJTYPE(*USRPRF) +
           DETAIL(*BASIC) OUTPUT(*OUTFILE)
   ```

2. Utwórz program z zapytaniem wyświetlający nazwę i wielkość każdego profilu użytkownika w kolejności malejącej.

3. Wydrukuj szczegółowe informacje o największych profilach użytkowników i oceń uprawnienia oraz obiekty należące do tych profili:

```
DSPUSRPRF USRPRF(nazwa-profilu-użytkownika) +
          TYPE(*OBJAUT) OUTPUT(*PRINT)
DSPUSRPRF USRPRF(nazwa-profilu-użytkownika) +
          TYPE(*OBJOWN) OUTPUT(*PRINT)
```

Niektóre profile użytkowników IBM są bardzo duże, ponieważ są właścicielami wielu obiektów. Zwykle nie jest konieczne ich wyświetlanie ani analizowanie. Należy jednak sprawdzić, czy w systemie nie ma programów adoptujących uprawnienia profili użytkowników IBM z uprawnieniem specjalnym *ALLOBJ, takich jak QSECOFR i QSYS.

Szczegółowe informacje o kontroli ochrony zawiera Rozdział 9 książki *Ochrona*.

Analiza uprawnień do obiektów

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)
```

Uwaga: Powyższa komenda nie wyświetli tych bibliotek znajdujących się w puli pamięci dyskowej, które nie mają statusu AVAILABLE.

2. Aby wyświetlić uprawnienia do określonej biblioteki, można użyć komendy Wyświetlenie uprawnień dla obiektu (Display Object Authority - DSPOBJAUT).

```
DSPOBJAUT OBJ(QSYS/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(QSYS/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.

Sprawdzanie zmienionych obiektów

Za pomocą komendy Sprawdzenie integralności obiektu (Check Object Integrity - CHKOBJITG) można wyszukać obiekty, które zostały zmodyfikowane. Zmodyfikowany obiekt jest zazwyczaj sygnałem, że ktoś próbuje wprowadzić zmiany w systemie. Komendę tę warto uruchomić po:

- odtwarzaniu programów w systemie,
- użyciu dedykowanych narzędzi serwisowych (DST).

Po uruchomieniu komendy system tworzy zbiór bazy danych zawierający informacje o potencjalnych problemach związanych z integralnością danych. Można sprawdzić obiekty należące do jednego profilu, kilku różnych profili lub do wszystkich profili. Można wyszukać obiekty, których domena została zmieniona. Można także ponownie obliczyć wartości sprawdzania programu, aby wyszukać obiekty typu *PGM, *SRVPGM, *MODULE i *SQLPKG, które zostały zmienione.

Uruchomienie programu CHKOBJITG wymaga uprawnienia specjalnego *AUDIT. Czas wykonania komendy może być długi ze względu na ilość skanowania i obliczeń, jakie są wykonywane. Dlatego należy ją uruchamiać przy małym obciążeniu systemu.

Uwaga: Profile, do których należy wiele obiektów z wieloma uprawnieniami prywatnymi, mogą być bardzo duże. 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. **Nie należy przypisywać wszystkich (lub prawie wszystkich) obiektów do jednego profilu właściciela.**

Analiza programów adoptujących uprawnienia

Programy, które adoptują uprawnienie specjalne *ALLOBJ, stanowią zagrożenie ochrony. Za pomocą poniższej metody można wyszukać i sprawdzić te programy:

1. Dla każdego użytkownika z uprawnieniem specjalnym *ALLOBJ użyj komendy Wyświetlenie programów, które adoptują uprawnienia (Display Programs That Adopt - DSPPGMADP), aby wyświetlić programy, które adoptują uprawnienia użytkownika:

   ```
   DSPPGMADP USRPRF(nazwa-profilu-użytkownika) +
             OUTPUT(*PRINT)
   ```

   Uwaga: Sekcja “Drukowanie wybranych profili użytkowników” na stronie 51 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-biblioteki/nazwa-programu) +
             OUTPUT(*PRINT)
   ```

3. Sprawdź kod źródłowy i opis programu, aby oszacować, czy:
   - Użytkownik programu uruchamianego z adoptowanym profilem nie ma dostępu do zbyt dużej ilości funkcji, takich jak wiersz komend.
   - Program adoptuje minimalny poziom uprawnień potrzebny do realizacji zamierzonych zadań. Istnieje możliwość napisania aplikacji, które wykorzystują błędy w programie, używające tego samego profilu 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-biblioteki/nazwa-programu) +
           DETAIL(*FULL)
   ```

Zarządzanie kronikami kontroli

Kronika kontroli, QSYS/QAUDJRN, służy wyłącznie do kontroli ochrony. Nie należy kronikować w niej obiektów. Również kontrola transakcji nie powinna korzystać z kroniki kontroli. Nie należy też wysyłać do niej pozycji użytkowników za pomocą komendy Wysłanie pozycji do kroniki (Send Journal Entry - SNDJRNE) ani funkcji API Send Journal Entry (QJOSJRNE).

Aby system mógł zapisywać pozycje kontroli do kroniki kontroli, używana jest specjalna blokada. Kiedy kontrola jest aktywna (wartość systemowa QAUDCTL jest różna od *NONE), zadanie arbitra systemowego (QSYSARB) blokuje kronikę QSYS/QAUDJRN. Gdy kronika kontroli jest aktywna, nie można wykonywać na niej takich czynności, jak:

- komenda DLTJRN,
- komenda ENDJRNxxx,
- komenda APYJRNCHG,
- komenda RMVJRNCHG,

- komenda DMPOBJ lub DMPSYSOBJ,
- przenoszenie kroniki,
- odtwarzanie kroniki,
- operacje na uprawnieniach, na przykład komenda GRTOBJAUT,
- komenda WRKJRN.

Informacje zapisane w kronice w pozycjach dotyczących ochrony są opisane w książce *Ochrona*. Wszystkie pozycje dotyczące ochrony w kronice kontroli mają kod kroniki T. W kronice QAUDJRN, obok pozycji dotyczących ochrony, znajdują się pozycje systemowe. Mają one kod kroniki J i dotyczą ładowania programu początkowego (IPL) i ogólnych działań wykonywanych na dziennikach (na przykład składowania).

Jeśli kronika lub jej bieżący dziennik zostanie uszkodzona i pozycje kontroli nie będą kronikowane, wartość systemowa QAUDENDACN będzie określać, jakie czynności powinien podjąć system. Odzyskiwanie zniszczonej kroniki lub dziennika wykonuje się tak samo, jak w przypadku innych kronik.

Można skonfigurować system tak, aby sam zarządzał zmianami dzienników. Podczas tworzenia kroniki QAUDJRN należy podać parametr MNGRCV(*SYSTEM) lub zmienić go w istniejącej kronice. Po podaniu wartości MNGRCV(*SYSTEM) system automatycznie odłączy dziennik, gdy osiągnie on wielkość progową, a następnie utworzy i przyłączy nowy dziennik. Jest to tak zwane **systemowe zarządzanie zmianą kroniki**. Więcej informacji na ten temat zawiera sekcja iSeries Centrum informacyjne—>Zarządzanie systemami–> Zarządzanie kronikami–>Zarządzanie kronikami lokalnymi–>Kroniki zarządzania. Informacje na temat dostępu do Centrum informacyjnego iSeries (patrz “Informacje wstępne i pokrewne” na stronie xii).

Rozdział 6. Zarządzanie uprawnieniami

Do sprawdzania konfiguracji uprawnień w systemie dostępny jest zestaw raportów o ochronie. Podczas pierwszego uruchamiania raportów można na nich wydrukować pełne informacje (na przykład uprawnienia do wszystkich zbiorów lub do wszystkich programów).

Po utworzeniu bazy informacji można regularnie uruchamiać raporty zmian. Raporty zmian pomagają znaleźć w systemie zmiany dotyczące ochrony i wymagające dokładniejszej analizy. Można na przykład co tydzień uruchomić raport zawierający uprawnienia publiczne dla zbiorów. Można wybrać tylko wersję raportu zawierającą zmiany. Będzie on zawierał zarówno nowe zbiory w systemie dostępne dla wszystkich, jak i istniejące zbiory, do których uprawnienia publiczne zmieniły się od ostatniego uruchomienia raportu.

Do uruchamiania narzędzi ochrony dostępne są dwa menu:

- menu SECTOOLS służy do interaktywnego uruchamiania programów,
- menu SECBATCH służy do wsadowego uruchamiania programów; menu SECBATCH składa się z dwóch części: jedna część służy do natychmiastowego wprowadzania zadań do kolejki zadań, druga do umieszczania zadań w programie do planowania zadań.

Jeśli używany jest program iSeries Navigator, należy postępować według poniższych kroków, aby uruchomić narzędzia ochrony:

1. W programie iSeries Navigator, rozwiń dany serwer—>**Ochrona**.
2. Kliknij prawym przyciskiem myszy **Strategie** i zaznacz **Eksploruj**, aby wyświetlnić listę strategii, które możesz tworzyć i zarządzać.

Monitorowanie uprawnień publicznych do obiektów

Ze względu na prostotę i wydajność większość systemów jest skonfigurowanych tak, że większość obiektów jest dostępnych dla większości użytkowników. Użytkownikom raczej odbiera się dostęp do niektórych poufnych, istotnych dla ochrony obiektów, a nie nadaje się im jawnie uprawnienia do wszystkich używanych przez nich obiektów. W niewielu systemach z wysokimi wymaganiami dotyczącymi ochrony przyjęto metodę nadawania uprawnień do obiektów, do których jest potrzebny dostęp. W tych systemach większość obiektów jest tworzonych z uprawnieniem publicznym ustawionym na *EXCLUDE.

System iSeries jest oparty na obiektach z wieloma różnymi typami obiektów. Większość typów obiektów nie zawiera poufnych informacji i nie spełnia funkcji związanych z ochroną. Administrator ochrony w systemie iSeries z typowym zapotrzebowaniem na ochronę skupia uwagę na obiektach wymagających ochrony, takich jak zbiory baz danych i programy. W przypadku obiektów innego typu można ustawić uprawnienie publiczne wystarczające dla używanych aplikacji, które dla większości typów obiektów wynosi *USE.

Do wydrukowania informacji o obiektach, do których mają dostęp użytkownicy publiczni, można użyć komendy Drukowanie obiektów z uprawnieniami publicznymi (Print Public Authority - PRTPUBAUT). (**Użytkownikiem publicznym** jest osoba z uprawnieniem do wpisania się, która nie ma jawnego uprawnienia do obiektu). Używając komendy PRTPUBAUT można podać typy obiektów, biblioteki i katalogi, o których mają zostać wyświetlone informacje. W menu SECBATCH i SECTOOLS dostępne są opcje do drukowania raportu o obiektach z uprawnieniami publicznymi dla typów obiektów, które najczęściej są powiązane z ochroną. Aby zobaczyć obiekty, na które należy zwrócić uwagę, można regularnie drukować raport zmian.

Zarządzanie uprawnieniami do nowych obiektów

OS/400 udostępnia funkcje pomagające w zarządzaniu uprawnieniami i prawami własności nowych obiektów w systemie. Gdy użytkownik tworzy nowy obiekt, system określa:
- kto jest właścicielem obiektu,
- jakie jest uprawnienie publiczne dla tego obiektu,
- czy obiekt ma uprawnienia prywatne,
- gdzie umieścić obiekt (biblioteka lub katalog),
- czy będzie kontrolowany dostęp do obiektu.

Aby ustalić odpowiedzi na te pytania, system używa wartości systemowych, parametrów bibliotek i parametrów profili użytkowników. Sekcja “Assigning Authority and Ownership to New Objects” w rozdziale 5 książki *iSeries Ochrona* zawiera przykłady dostępnych opcji.

Aby wydrukować parametry profilu użytkownika dotyczące praw własności i uprawnień nowych obiektów, można użyć komendy PRTUSRPRF. Rys. 5 na stronie 60 przedstawia przykładowy raport.

Monitorowanie list autoryzacji

Za pomocą listy autoryzacji można grupować obiekty o podobnych wymaganiach dotyczących ochrony. Lista autoryzacji zawiera listę użytkowników i uprawnień, które mają użytkownicy do obiektów chronionych przez listę. Listy autoryzacji są skutecznym sposobem zarządzania uprawnieniami do podobnych obiektów w systemie. Z drugiej strony w niektórych przypadkach utrudniają one śledzenie uprawnień do obiektów.

Aby wydrukować informacje o uprawnieniach listy autoryzacji, można użyć komendy Drukowanie uprawnień prywatnych (Print Private Authority - PRTPVTAUT). Rys. 3 przedstawia przykładowy raport.

```
                          Uprawnienia prywatne - raport pełny
                           (Private Authorities - Full Report)
SYSTEM4
Lista                   Grupa                              Lista  ----------Obiekt----------  ------------Data------------
autoryzacji  Właściciel podstawowa  Użytkownik Uprawnienia Mgt   Opr  Mgt  Exist  Alter  Ref  Read  Add  Upd  Dlt  Execute
LIST1         QSECOFR   *NONE       *PUBLIC    *EXCLUDE
LIST2         BUDNIKR   *NONE       BUDNIKR    *ALL        X     X    X     X      X     X    X     X    X      X
                                     *PUBLIC    *CHANGE           X                         X    X     X    X      X
LIST3         QSECOFR   *NONE       *PUBLIC    *EXCLUDE
LIST4         CJWLDR    *NONE       CJWLDR     *ALL        X     X    X     X      X     X    X     X    X      X
                                     GROUP1     *ALL              X    X     X      X     X    X     X    X      X
                                     *PUBLIC    *EXCLUDE
```

Rysunek 3. Raport uprawnień prywatnych dla list autoryzacji

Przedstawiony raport zawiera te same informacje, które można zobaczyć na ekranie Edycja listy autoryzacji (Edit Authorization List - EDTAUTL). Zaletą raportu jest to, że przedstawia on w jednym miejscu informacje o wszystkich listach autoryzacji. Jeśli na przykład konfiguruje się ochronę dla nowej grupy obiektów, można szybko przejrzeć raport, aby sprawdzić, czy jakaś istniejąca lista autoryzacji spełnia nasze potrzeby dotyczące tych obiektów.

Aby zobaczyć nowe listy autoryzacji i listy autoryzacji z uprawnieniami zmienionymi od ostatniego drukowania raportu, można wydrukować raport zmian. Istnieje również możliwość wydrukowania listy obiektów, które są chronione przez każdą listę autoryzacji. Rys. 4 na stronie 57 przedstawia przykładowy raport dla jednej listy autoryzacji.

```
                      Wyświetlenie obiektów listy autoryzacji
                       (Display Authorization List Objects)
Lista autoryzacji. . . . . . . . . :   CUSTAUTL
Biblioteka . . . . . . . . . . . . :     QSYS
Właściciel . . . . . . . . . . . . :   AROWNER
Grupa podstawowa . . . . . . . . . :   *NONE

                                                          Grupa
Obiekt         Biblioteka     Typ          Właściciel     podstawowa     Tekst
CUSTMAS        CUSTLIB        *FILE        AROWNER        *NONE
CUSTORD        CUSTORD        *FILE        OEOWNER        *NONE
```

Rysunek 4. Raport Wyświetlenie obiektów listy autoryzacji

Ten raport może posłużyć za przykład efektu dodania nowego użytkownika do listy autoryzacji (można zaobserwować uprawnienia, które otrzyma ten użytkownik).

Używanie list autoryzacji

iSeries Navigator udostępnia opcje ochrony zaprojektowane tak, aby asystowały podczas opracowywania planu ochrony i strategii oraz konfigurowały system zgodnie z postawionymi wymaganiami. Jedną z dostępnych opcji jest lista autoryzacji.

Lista autoryzacji:
- grupuje obiekty o podobnych wymaganiach ochrony,
- zawiera listę użytkowników i uprawnień, które mają użytkownicy do obiektów chronionych przez listę,
- każdy użytkownik i grupa mogą mieć inne uprawnienia do zestawu obiektów chronionych przez listę,
- uprawnienia mogą być nadawane poprzez listę zamiast indywidualnym użytkownikom i grupom.

Przy użyciu funkcji obsługi list autoryzacji można:
- utworzyć listę autoryzacji,
- zmienić listę autoryzacji,
- dodać użytkowników i grupy,
- zmienić uprawnienia użytkownika,
- wyświetlić obiekty chronione.

Aby użyć omawianej funkcji:
1. W programie iSeries Navigator, rozwiń dany serwer—>Ochrona. Pojawią się **Listy autoryzacji** oraz **Strategie**.
2. Kliknij prawym przyciskiem myszy **Listy autoryzacji** i zaznacz **Nowa lista autoryzacji**. **Nowa lista autoryzacji** umożliwia ustawianie następujących uprawnień:
   - **Użyj:** Umożliwia dostęp do atrybutów obiektu oraz użycie obiektu. Użytkownicy mogą oglądać obiekty, ale nie mogą ich zmieniać.
   - **Zmień:** Umożliwia zmianę zawartości obiektu (z pewnymi wyjątkami).
   - **Wszystkie:** Umożliwia wykonywanie na obiekcie wszystkich operacji, z wyjątkiem operacji, które może wykonywać tylko właściciel. Użytkownik lub grupa może sterować istnieniem obiektu, określać ochronę obiektu, zmieniać obiekt oraz wykonywać podstawowe funkcje na obiekcie. Użytkownik lub grupa może również zmienić prawa własności do obiektu.
   - **Exclude:** Wszystkie operacje na obiekcie są zabronione. Użytkownicy i grupy z tym uprawnieniem nie mają dostępu do obiektu. Nie mogą również używać obiektu.

Podczas pracy z listą autoryzacji można nadawać uprawnienia zarówno do obiektów, jak i danych. Możliwe uprawnienia do obiektów:

- **Działające:** Uprawnienie do przeglądania opisu obiektu oraz użycia obiektu zgodnie z uprawnieniami posiadanymi przez użytkownika lub grupę.
- **Zarządzanie:** Uprawnienie do określania ochrony obiektu, przenoszenia lub zmiany nazwy obiektu oraz dodawania podzbiorów do zbioru bazy danych.
- **Istnienie:** Uprawnienie do sterowania istnieniem obiektu oraz prawami własności. Użytkownik lub grupa mogą usunąć obiekt, zwolnić pamięć obiektu, wykonać operacje składowania i odtwarzania na obiekcie oraz przenieść prawa własności do obiektu. Jeśli użytkownik lub grupa mają specjalne uprawnienia do składowania, to nie potrzebują uprawnień istnienia.
- **Modyfikacja** (używane tylko dla zbiorów baz danych oraz pakietów SQL): Uprawnienie do modyfikacji atrybutów obiektu. Użytkownik lub grupa mogą dodawać i usuwać wyzwalacze, dodawać i usuwać ograniczenia referencyjne i ograniczenia przez unikalność oraz zmieniać atrybuty zbioru bazy danych. Jeśli użytkownik lub grupa mają to uprawnienie do pakietów SQL, mogą zmieniać atrybuty pakietów. Uprawnienie to jest obecnie używane tylko dla zbiorów baz danych i pakietów SQL.
- **Odniesienie** (używane tylko dla zbiorów baz danych i pakietów SQL): Uprawnienie do tworzenia odniesień pomiędzy obiektami, tak że operacje na obiekcie mogą być ograniczone przez inny obiekt. Jeśli użytkownik lub grupa mają to uprawnienie dla zbioru fizycznego, to mogą dodawać ograniczenia referencyjne, w których jeden ze zbiorów jest nadrzędny. Uprawnienie to jest obecnie używane tylko do zbiorów baz danych.

Możliwe uprawnienia do danych:
- **Odczyt:** Uprawnienie do wyświetlania zawartości obiektu, na przykład rekordów w zbiorze.
- **Dodawanie:** Uprawnienie do dodawania pozycji w obiekcie, na przykład dodawanie komunikatów do kolejki komunikatów lub dodawanie rekordów do zbioru.
- **Aktualizacja:** Uprawnienie do zmiany pozycji w obiekcie, na przykład zmiana rekordów w zbiorze.
- **Usuwanie:** Uprawnienie do usuwania pozycji z obiektu, na przykład usuwanie komunikatów z kolejki komunikatów lub usuwanie rekordów ze zbioru.
- **Wykonywanie:** Uprawnienie do uruchamiania programów, programów serwisowych oraz pakietów SQL. Mając to uprawnienie użytkownik będzie mógł również znaleźć obiekt w bibliotece lub katalogu.

Więcej informacji na temat tworzenia i edycji list autoryzacji można znaleźć w pomocy elektronicznej iSeries Navigator.

Dostęp do strategii w programie iSeries Navigator

Za pomocą programu iSeries Navigator można przeglądać i zarządzać strategiami serwera iSeries. iSeries Navigator posiada pięć obszarów strategii:

- **Strategia kontroli**
  Umożliwia konfigurowanie monitorowania określonych działań i dostęp do określonych zasobów w systemie.
- **Strategia ochrony**
  Umożliwia ustawienie poziomu ochrony i dodatkowych opcji powiązanych z ochroną systemu.
- **Strategia hasła**
  Umożliwia ustawienie poziomu haseł w systemie.
- **Strategia odtwarzania**
  Umożliwia określenie sposobu odtwarzania poszczególnych obiektów w systemie.
- **Strategia wpisywania się**
  Umożliwia określenie sposobu wpisywania się użytkownika do systemu.

Aby przejrzeć lub zmienić strategie za pomocą programu iSeries Navigator:

1. W programie iSeries Navigator, rozwiń dany serwer —>**Ochrona**.
2. Kliknij prawym przyciskiem myszy **Strategie** i zaznacz **Rozwiń**, aby wyświetlić listę strategii, które możesz tworzyć i zarządzać. Więcej informacji na temat tych strategii znajduje się w pomocy programu iSeries Navigator.

Monitorowanie uprawnień prywatnych do obiektów

Opcje menu SECBATCH:
12 *wprowadzanie natychmiastowe* **41** *użycie programu do planowania zadań*

Komenda Drukowanie uprawnień prywatnych (Print Private Authority - PRTPVTAUT) umożliwia wydrukowanie listy wszystkich uprawnień prywatnych dla obiektów określonego typu w podanej bibliotece.

Utworzony raport można wykorzystać jako pomoc podczas wyszukiwania nowych uprawnień do obiektów. Może on również pomóc w zachowaniu przejrzystości schematu uprawnień prywatnych i zarządzaniu nim.

Monitorowanie dostępu do kolejek wyjściowych i kolejek zadań

Zdarza się, że administrator ochrony poświęca wiele pracy, aby zabezpieczyć zbiory przed dostępem nieuprawnionych użytkowników, a następnie zapomina o ochronie, gdy zawartość zbioru zostanie wydrukowana. Serwer iSeries udostępnia funkcje do ochrony istotnych kolejek wyjściowych i kolejek zadań. Kolejki wyjściowe chroni się tak, aby nieuprawnieni użytkownicy nie mogli na przykład przeglądać i kopiować poufnych zbiorów buforowych oczekujących na wydruk. Kolejki zadań chroni się tak, aby nieuprawnieni użytkownicy nie mogli przekierować poufnego zadania do niepoufnej kolejki wyjściowej albo całkowicie anulować zadania.

Opcje menu SECBATCH:
24 *wprowadzenie natychmiastowe* **63** *użycie programu do planowania*

Pozycja *Planowanie ochrony i ochrona systemu - podstawy* w Centrum informacyjnym i książka *iSeries Ochrona* opisują sposób ochrony kolejek wyjściowych i kolejek zadań.

Aby wydrukować ustawienia ochrony dla kolejek zadań i kolejek wyjściowych w systemie, można użyć komendy Drukowanie uprawnień dla kolejki (Print Queue Authority - PRTQAUT). Następnie można ocenić zadania wydruku drukujące poufne informacje i sprawdzić, czy są one kierowane do chronionych kolejek wyjściowych i kolejek zadań.

Dla kolejek wyjściowych i kolejek zadań, które są istotne dla ochrony można porównać ustawienia ochrony z informacją w dodatku D książki *iSeries Ochrona*. Tabele znajdujące się w tym dodatku omawiają wymagane ustawienia do wykonania różnych funkcji kolejki wyjściowej i kolejki zadań.

Monitorowanie uprawnień specjalnych

Gdy użytkownicy w systemie mają zbędne uprawnienia specjalne, wysiłki czynione, aby utworzyć dobry, zorientowany na obiekty schemat ochrony, mogą być daremne. Uprawnienie do obiektu nie ma żadnego znaczenia, gdy profil użytkownika ma uprawnienie specjalne *ALLOBJ. Użytkownik dysponujący uprawnieniem specjalnym *SPLCTL może obserwować wszystkie zbiory buforowe w systemie, bez względu na wysiłki włożone w ochronę kolejek wyjściowych. Użytkownik z uprawnieniem specjalnym *JOBCTL może wpływać na działanie systemu i przekierowywać zadania. Użytkownik z uprawnieniem specjalnym *SERVICE może użyć narzędzi serwisowych, aby uzyskać dostęp do danych nie korzystając z systemu operacyjnego.

Opcje menu SECBATCH:
29 *wprowadzenie natychmiastowe* **68** *użycie programu do planowania*

Aby wydrukować informacje o uprawnieniach specjalnych i klasach użytkowników dla profili użytkowników w systemie, można użyć komendy Drukowanie profilu użytkownika (Print User Profile - PRTUSRPRF). Uruchamiając raport można wybrać kilka opcji:

- wszystkie profile użytkowników,
- profile użytkowników z konkretnymi uprawnieniami specjalnymi,
- profile użytkowników z konkretnymi klasami użytkowników,
- profile użytkowników, w których wystąpiła niezgodność między klasą użytkownika a uprawnieniami specjalnymi.

Rys. 5 przedstawia przykładowy raport zawierający uprawnienia specjalne dla wszystkich profili użytkowników.

```
                                        Informacje o profilach użytkowników
                                             (User Profile Information)
  Typ raportu  . . . . . . . . . . :   *AUTINFO
  Wybór według . . . . . . . . . . :   *SPCAUT
  Uprawnienia specjalne. . . . . :   *ALL
                    ------------Uprawnienia specjalne-----------
                                *IO                                                                  Grupa
Profil    Profile   *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Klasa      Właści-  Uprawnienia Typ         Ograniczone
użytkow.  grupowe    OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  użytkow.   ciel     grupowe     uprawnienia możliwości
USERA     *NONE      X     X     X    X     X     X     X     X    *SECOFR    *USRPRF  *NONE       *PRIVATE    *NO
USERB     *NONE                      X     X                       *PGMR      *USRPRF  *NONE       *PRIVATE    *NO
USERC     *NONE      X     X     X    X     X     X     X     X    *SECOFR    *USRPRF  *NONE       *PRIVATE    *NO
USERD     *NONE                                                    *USER      *USRPRF  *NONE       *PRIVATE    *NO
```

Rysunek 5. Raport informacji o użytkownikach: Przykład 1

Oprócz uprawnień specjalnych raport zawiera również następujące informacje:

- czy profil użytkownika ma ograniczone możliwości,
- czy użytkownik lub grupa użytkownika jest właścicielem nowych obiektów tworzonych przez użytkownika,
- jakie uprawnienia do nowych obiektów tworzonych przez użytkownika automatycznie otrzymuje grupa użytkownika.

Rys. 6 na stronie 61 przedstawia przykładowy raport dla niezgodnych uprawnień specjalnych i klas użytkownika.

```
                                        Informacje o profilach użytkowników
                                             (User Profile Information)
Typ raportu  . . . . . . . . . . :   *AUTINFO
Wybór według . . . . . . . . . . :   *MISMATCH
-------------------------------Uprawnienia specjalne-----------
                                *IO                                                                 Grupa
Profil     Profile   *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Klasa      Właści-   Uprawnienia Typ          Ograniczone
użytkow.   grupowe    OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  użytkow.   ciel      grupowe     uprawnienia możliwości
USERX      *NONE       X                X     X                 X    *SYSOPR    *USRPRF   *NONE       *PRIVATE    *NO
USERY      *NONE                                      X               *USER      *USRPRF   *NONE       *PRIVATE    *NO
USERZ                                                 X               *USER      *USRPRF   *NONE       *PRIVATE    *NO
           QPGMR                          X     X
```

Rysunek 6. Raport informacji o użytkownikach: Przykład 2

Na rysunku Rys. 6 zwróćmy uwagę, że:

- USERX ma klasę użytkownika operator systemu (*SYSOPR), ale ma uprawnienia specjalne *ALLOBJ i *SPLCTL,
- USERY ma klasę użytkownika użytkownik (*USER), ale ma uprawnienie specjalne *SECADM,
- USERZ ma również klasę użytkownika użytkownik (*USER) i uprawnienie specjalne *SECADM; zauważmy również, że USERZ należy do grupy QPGMR, która ma uprawnienia specjalne *JOBCTL i *SAVSYS.

Regularne uruchamianie powyższych raportów pomoże w monitorowaniu i administrowaniu profilami użytkowników.

Monitorowanie środowiska użytkownika

Jedną z roli profilu użytkownika jest zdefiniowanie środowiska dla użytkownika, w tym kolejki wyjściowej, menu początkowego i opisu zadania. Środowisko użytkownika wpływa na sposób, w który użytkownik widzi system i w pewnym stopniu na to, co może on zrobić. Użytkownik musi mieć uprawnienie do obiektów podanych w profilu użytkownika. Jednak jeśli schemat uprawnień jest nadal w fazie rozwojowej lub jeśli nie jest zbytnio ograniczający, środowisko użytkownika zdefiniowane w profilu użytkownika może prowadzić do niezamierzonych rezultatów. Oto kilka przykładów:

Opcje menu SECBATCH:

29 *wprowadzenie natychmiastowe***68** *użycie programu do planowania*

- Opis zadania użytkownika może określać profil użytkownika, który ma więcej uprawnień niż użytkownik.
- Użytkownik może mieć do dyspozycji menu początkowe nie zawierające wiersza komend. Jednak program obsługi klawisza ATTN użytkownika może udostępniać wiersz komend.
- Użytkownik może być uprawniony do uruchamiania poufnych raportów. Jednak dane wyjściowe mogą zostać skierowane do kolejki wyjściowej dostępnej dla użytkowników, którzy nie powinni mieć możliwości oglądania tych raportów.

Jako pomoc w monitorowaniu środowisk zdefiniowanych dla użytkowników systemu można użyć opcji *ENVINFO komendy Drukowanie profilu użytkownika (Print User Profile - PRTUSRPRF). Rys. 7 na stronie 62 przedstawia przykładowy raport.

```
                                        Informacje o profilach użytkowników
                                            (User Profile Information)
  Typ raportu  . . . . . :   *ENVINFO
  Wybór według . . . . . :   *USRCLS
                          Początkowe     Początkowy       Opis           Kolejka        Kolejka        Program
Profil          Bieżąca   menu/          program/         zadania/       komunikatów/   wyjściowa/     Attention/
użytkownika     biblioteka biblioteka    biblioteka       biblioteka     biblioteka     biblioteka     biblioteka
AUDSECOFR       AUDITOR    MAIN          *NONE            QDFTJOBD       QSYSOPR        *WRKSTN        *SYSVAL
                           *LIBL                          QGPL            QSYS
USERA           *CRTDFT    OEMENU        *NONE            QDFTJOBD       USERA          *WRKSTN        *SYSVAL
                           *LIBL                          QGPL            QUSRSYS
USERB           *CRTDFT    INVMENU       *NONE            QDFTJOBD       USERB          *WRKSTN        *SYSVAL
                           *LIBL                          QGPL            QUSRSYS
USERC           *CRTDFT    PAYROLL       *NONE            QDFTJOBD       USERC          PAYROLL        *SYSVAL
                           *LIBL                          QGPL            QUSRSYS         PRPGMLIB
```

Rysunek 7. Drukowanie środowiska profilu użytkownika, przykład

Zarządzanie narzędziami serwisowymi

Narzędzia serwisowe są używane do konfigurowania, zarządzania i obsługi serwera. Dostęp do narzędzi serwisowych można uzyskać poprzez menu DST (Dedicated Service Tools) lub menu SST (System Service Tools). Aby uzyskać dostęp do narzędzi DST, SST, a także aby korzystać z funkcji iSeries Navigator do zarządzania partycjami logicznymi (LPAR) i jednostkami dyskowymi, trzeba mieć specjalne identyfikatory użytkownika narzędzi serwisowych.

Narzędzia DST są dostępne po uruchomieniu Licencjonowanego Kodu Wewnętrznego, nawet jeśli system OS/400 nie został załadowany. Narzędzia SST są dostępne z systemu OS/400. Poniższa tabela przedstawia różnice pomiędzy DST a SST.

Charakterystyka	DST	SST
Sposób dostępu	Dostęp fizyczny poprzez konsolę podczas ręcznego IPL lub po wybraniu opcji 21 z panelu sterującego.	Dostęp poprzez zadanie interaktywne z możliwością wpisania się przy użyciu QSRV lub przedstawionego poniżej sposobu uwierzytelnienia: • uprawnienie do komendy CL STRSST (Start SST), • serwisowe uprawnienia specjalne (*SERVICE) lub uprawnienie specjalne do wszystkich obiektów, (*ALLOBJ), • funkcjonalne uprawnienie do używania SST.
Jeśli są dostępne	Dostępne nawet wtedy, gdy serwer ma ograniczone możliwości. System OS/400 nie jest wymagany do uzyskania dostępu do DST.	Dostępne, gdy system OS/400 został uruchomiony. System OS/400 jest wymagany, aby uzyskać dostęp do narzędzi SST.
Sposób uwierzytelnienia	Wymagają identyfikatora użytkownika i hasła narzędzi serwisowych.	Wymagają identyfikatora użytkownika i hasła narzędzi serwisowych.

Więcej informacji na temat używania narzędzi serwisowych w celu wykonania poniższych zadań znajdują się w Centrum informacyjnym iSeries —>Ochrona—>Narzędzia serwisowe:

- dostęp do narzędzi serwisowych za pomocą DST,
- dostęp do narzędzi serwisowych za pomocą SST,
- dostęp do narzędzi serwisowych za pomocą iSeries Navigator,
- tworzenie identyfikatora użytkownika narzędzi serwisowych,
- zmiana uprawnień funkcjonalnych identyfikatora użytkownika narzędzi serwisowych,
- zmiana opisu identyfikatora użytkownika narzędzi serwisowych,
- wyświetlenie identyfikatora użytkownika narzędzi serwisowych,
- włączenie lub wyłączenie identyfikatora użytkownika narzędzi serwisowych,
- usuwanie identyfikatora użytkownika narzędzi serwisowych,
- zmiana identyfikatora użytkownika i hasła narzędzi serwisowych przy użyciu SST lub DST,
- zmiana identyfikatora użytkownika narzędzi serwisowych przy użyciu STRSST,
- zmiana identyfikatora użytkownika i hasła narzędzi serwisowych przy użyciu
- funkcja API Change Service Tools User ID (QSYCHGDS),
- resetowanie hasła profilu użytkownika do QSECOFR OS/400,
- resetowanie identyfikatora użytkownika i hasła narzędzi serwisowych do QSECOFR,
- składowanie danych ochrony narzędzi serwisowych; odtwarzanie danych ochrony narzędzi serwisowych,
- tworzenie własnej wersji identyfikatora użytkownika narzędzi serwisowych QSECOFR,
- konfigurowanie narzędzi serwisowych serwera dla DST,
- konfigurowanie narzędzi serwisowych serwera dlaOS/400,
- monitorowanie użycia funkcji serwisowych poprzez DST,
- monitorowanie użycia narzędzi serwisowych poprzez protokół kontroli ochrony systemu OS/400.

Informacje na temat dostępu do Centrum informacyjnego iSeries zawiera sekcja “Informacje wstępne i pokrewne” na stronie xii.

Rozdział 7. Używanie ochrony partycji logicznych (LPAR)

Posiadanie wielu partycji logicznych w pojedynczym serwerze iSeries może być korzystne przy realizacji następujących scenariuszy.

- **Zarządzanie niezależnymi systemami**: Dedykując część zasobów (jednostkę pamięci dyskowej, procesory, pamięć oraz urządzenia we/wy) dla partycji można uzyskać logiczne oddzielenie oprogramowania. Poprawnie skonfigurowane partycje logiczne są bardziej odporne na awarie sprzętu. Procesy interaktywne oraz zadania wsadowe, które mogą nie pracować dobrze na jednej maszynie, mogą zostać oddzielone i uruchomione z powodzeniem na różnych partycjach.
- **Scalanie**: Systemy podzielone na partycje logiczne umożliwiają zmniejszenie liczby serwerów iSeries wymaganych w przedsiębiorstwie. Dzięki nim można scalić kilka systemów w pojedynczy system podzielony na partycje logiczne. Eliminuje to dodatkowe wydatki na niezbędny sprzęt. Dodatkowo można w miarę potrzeb przenosić zasoby z jednej partycji logicznej na inną.
- **Tworzenie kombinacji środowiska testowego oraz produkcyjnego:** Można utworzyć kombinację środowiska testowego i produkcyjnego. Na partycji podstawowej można utworzyć pojedynczą partycję produkcyjną. W przypadku wielu partycji produkcyjnych patrz poniższa sekcja *Tworzenie środowiska wielu produkcyjnych partycji logicznych*.

  Partycja logiczna może być zarówno partycją testową jak i logiczną. Na partycji produkcyjnej uruchamiane są główne aplikacje biznesowe. Jakiekolwiek niepowodzenie na partycji produkcyjnej może znacznie utrudnić operacje biznesowe oraz zwiększyć nakłady finansowe i potrzebny czas. Na partycji testowej oprogramowanie jest testowane. Niepowodzenie na partycji testowej nie zakłóca normalnych operacji biznesowych.
- **Tworzenie środowiska produkcyjnego składającego się z wielu partycji logicznych:** Dodatkowe produkcyjne partycje logiczne powinny być tworzone jedynie na partycjach dodatkowych. W takim przypadku partycja podstawowa jest dedykowana do zarządzania partycjami.
- **Replikacja na bieżąco:** W przypadku replikacji partycji dodatkowej do innej partycji logicznej w obrębie tego samego systemu, po wystąpieniu awarii należy jedynie przełączyć system na partycję zapasową. Ta konfiguracja pozwala również znacznie ograniczyć wielkość okien składowania. Można wyłączyć partycje zapasowe i zeskładować je nie przerywając pracy partycji produkcyjnych. Aby wykorzystać strategię replikacji na bieżąco wymagane jest specjalne oprogramowanie.
- **Zintegrowane klastry:** Użycie OptiConnect/400 oraz oprogramowania aplikacji wysokiej dostępności umożliwia uruchomienie systemu podzielonego na partycje jako zintegrowanego klastra. Zintegrowany klaster można wykorzystać do ochrony systemu przed większością nie planowanych awarii w obrębie partycji dodatkowej.

Uwaga: Podczas konfigurowania partycji dodatkowej należy rozważyć konieczność rozmieszczenia kart. Jeśli jako konsola zostanie wybrany procesor IOP posiadający kartę LAN nie przeznaczoną do pracy z Operations Console, karta ta zostanie uruchomiona przez konsolę, jednak nie będzie można jej wykorzystać do zamierzonych celów. Więcej informacji na temat pracy z Operations Console zawiera Rozdział 8, “Konsola iSeries Operations Console”, na stronie 67.

Więcej szczegółowych informacji na ten temat można znaleźć w sekcji ″Partycje Logiczne″ w Centrum informacyjnym.

Zarządzanie ochroną partycji logicznych

Zadania związane z ochroną wykonywane w systemie podzielonym na partycje są takie same, jak w systemie bez partycji logicznych. Jednakże, po utworzeniu partycji logicznych praca jest wykonywana w kilku niezależnych systemach. W związku z tym te same zadania należy wykonać na każdej partycji logicznej a nie tylko raz, jak w systemie bez partycji logicznych.

Poniżej przedstawione są podstawowe zasady ochrony partycji logicznych:

- W danej chwili można dodawać użytkowników tylko do jednej partycji logicznej w systemie. Użytkowników należy dodać do każdej partycji, do której mają mieć dostęp.
- Należy ograniczyć liczbę osób mających uprawnienia do narzędzi Dedicated Service Tools (DST) oraz systemowych narzędzi serwisowych (SST) na partycji podstawowej. Więcej informacji o narzędziach DST i SST można znaleźć w sekcji ″Zarządzanie partycjami logicznymi za pomocą iSeries Navigator, DST i SST″ w Centrum informacyjnym iSeries. Informacje na temat użycia profili użytkownika narzędzi serwisowych do kontroli dostępu do partycji można znaleźć w sekcji “Zarządzanie narzędziami serwisowymi” na stronie 62.

  Uwaga: Przed użyciem iSeries Navigator z funkcjami LPAR należy zainicjować serwer narzędzi serwisowych (STS - Service Tools Server). Więcej informacji na ten temat zawiera artykuł iSeries Centrum Informacyjne —>Ochrona—>Narzędzia usług. Informacje na temat dostępu do Centrum informacyjnego iSeries zawiera sekcja “Informacje wstępne i pokrewne” na stronie xii.
- Partycje dodatkowe nie widzą i nie mogą korzystać z pamięci głównej oraz z jednostek dyskowych innych partycji logicznych.
- Partycje dodatkowe widzą jedynie własne zasoby sprzętowe.
- Na partycji podstawowej można zobaczyć wszystkie zasoby sprzętowe systemu na ekranach Praca z partycjami systemowymi (Work with System Partitions) narzędzi DST oraz SST.
- System operacyjny na partycji podstawowej widzi tylko własne zasoby.
- Partycją podstawową można sterować z panelu sterowania systemu. Po ustawieniu trybu panelu na Chroniony, na ekranie Praca ze statusem partycji (Work with Partition Statu) nie mogą być wykonywane żadne operacje z poziomu narzędzi SST. Aby uruchomić DST na panelu sterowania, należy zmienić tryb na Ręczny.
- Po ustawieniu trybu pracy partycji dodatkowej na Chroniony można ograniczyć użycie ekranu Praca ze statusem partycji (Work with Partition Status) w następujący sposób:
  - Do zmiany statusu partycji można używać tylko narzędzi DST z partycji dodatkowej; do zmiany statusu partycji nie można użyć narzędzi SST.
  - Można uruchomić DST na partycji dodatkowej z ekranu Praca ze statusem partycji (Work with Partition Status) na partycji podstawowej przy użyciu narzędzi DST lub SST.
  - Do zmiany trybu partycji dodatkowej z chronionego na inny można użyć wyłącznie narzędzi DST na partycji podstawowej.

W przypadku, gdy partycja dodatkowa nie jest chroniona, do zmiany statusu partycji można używać narzędzi DST i SST z partycji dodatkowej.

Więcej informacji o ochronie serwera iSeries, można znaleźć w książce Ochrona oraz w dokumencie Ochrona systemu i planowanie - podstawy w Centrum informacyjnego iSeries.

Rozdział 8. Konsola iSeries Operations Console

Konsola Operations Console umożliwia wykorzystanie komputera PC do dostępu i sterowania serwerem iSeries. Obsługuje również pracę zdalnych komputerów PC połączonych połączeniem dial-up z serwerami bez urządzenia konsoli, umożliwiając wykorzystanie zdalnego komputera PC jako konsoli. Podczas używania Operations Console, należy zwrócić uwagę na następujące kwestie:

- Z poziomu Operations Console można wykonywać wszystkie zadania, które można było wykonywać na tradycyjnej konsoli. Na przykład profile użytkownika o uprawnieniach specjalnych *SERVICE lub *ALLOBJ umożliwiają wpisanie się do sesji Operations Console nawet w przypadku, gdy zostały wyłączone.
- Operations Console używa profili użytkownika narzędzi serwisowych oraz haseł w celu udostępnienia połączenia z serwerem iSeries. Dlatego bardzo ważna jest zmiana profili użytkownika narzędzi systemowych oraz haseł. Hakerzy znają wartości domyślne profili użytkownika narzędzi serwisowych oraz hasła i mogą je wykorzystać przy próbie ustanowienia sesji zdalnej konsoli w serwerze iSeries. Wskazówki na ten temat można znaleźć w sekcjach “Zmiana znanych haseł” na stronie 20 oraz “Unikanie domyślnych haseł” na stronie 26.
- Aby chronić informacje podczas używania konsoli zdalnej, należy użyć opcji wywołania zwrotnego Windows Dial-Up Networking.
- Podczas konfigurowania partycji dodatkowej należy rozważyć konieczność rozmieszczenia kart. Jeśli jako konsola zostanie wybrany procesor IOP posiadający kartę LAN nie przeznaczoną do pracy z Operations Console, karta ta zostanie uruchomiona przez konsolę, jednak nie będzie można jej wykorzystać do zamierzonych celów.

W wersji V5R1 Operations Console została rozszerzona o możliwość wykonywania zadań w sieci lokalnej (LAN). Zaawansowane uwierzytelnianie i szyfrowanie danych umożliwiło ochronę procedur konsoli. W przypadku używania Operations Console z połączeniem LAN zaleca się zainstalowanie następujących produktów:

- w serwerze iSeries, Cryptographic Access Provider, 5722–AC2 lub 5722–AC3
- na komputerze PC z Operations Console, PC Client Encryption, 5722–CE2 lub 5722–CE3.

Aby dane konsoli były szyfrowane, należy zainstalować w serwerze iSeries jeden z produktów Cryptographic Access Provider **oraz** na komputerze PC produkty Client Encryption.

Uwaga: Jeśli produkty do szyfrowania danych nie zostaną zainstalowane, dane nie będą szyfrowane.

Poniższa tabela podsumowuje rezultaty szyfrowania dostępnych produktów:

Tabela 13. Rezultat szyfrowania

Cryptographic Access Provider w serwerze iSeries	Client Encryption na komputerze PC z Operations Console	Rezultat szyfrowania danych
brak	brak	brak
5722–AC2	5722–CE2	56 bitowe
5722–AC2	5722–CE3	56 bitowe
5722–AC3	5722–CE2	56 bitowe
5722–AC3	5722–CE3	128 bitowe

Więcej informacji o konfigurowaniu i administrowaniu serwerem iSeries Operations Console, można znaleźć w Centrum informacyjnym iSeries.

Ochrona Operations Console

Na ochronę Operations Console składa się:

- uwierzytelnianie urządzenia konsoli,
- uwierzytelnianie użytkownika,
- ochrona danych,
- integralność danych.

Połączenia bezpośrednie punkt z punktem Operations Console implikują uwierzytelnianie urządzenia, ochronę danych oraz integralność danych. Aby wpisać się do konsoli, wymagana jest ochrona uwierzytelniania użytkownika.

Uwierzytelnianie urządzenia konsoli

Uwierzytelnianie urządzenia konsoli jest wykonywane w celu sprawdzenia, czy urządzenie fizyczne jest konsolą. Operations Console z połączeniem bezpośrednim wykorzystuje połączenie bezpośrednie podobnie jak konsola twinaksowa. Połączenie bezpośrednie Operations Console może być chronione podobnie jak połączenia twinaksowe poprzez kontrolę praw dostępu do fizycznego urządzenia konsoli.

Operations Console z połączeniem LAN używa warstwy SSL obsługującej urządzenia oraz uwierzytelnianie użytkowników, ale nie używa certyfikatów. Ta forma połączenia oraz uwierzytelniania urządzenia jest oparta na profilu urządzenia narzędzi serwisowych. Informacje szczegółowe zawiera sekcja “Używanie konsoli Operations Console z połączeniem LAN” na stronie 69.

Uwierzytelnianie użytkownika

Uwierzytelnianie użytkownika jest wykonywane w celu sprawdzenia osoby używającej urządzenia konsoli. Wszystkie czynności związane z uwierzytelnianiem użytkownika są takie same dla wszystkich typów konsol.

Ochrona danych

Ochrona danych umożliwia odbieranie danych konsoli tylko uprawnionemu użytkownikowi. Do ochrony danych konsoli Operations Console z połączeniem bezpośrednim wykorzystuje połączenie fizyczne, podobnie jak konsola twinaksowa lub chronione połączenie sieciowe LAN. Operations Console z połączeniem bezpośrednim używa tej samej ochrony danych co połączenie twinaksowe. Jeśli połączenie fizyczne jest chronione, to dane konsoli pozostają zabezpieczone.

Operations Console z połączeniem LAN wykorzystuje chronione połączenie sieciowe, jeśli został zainstalowany odpowiedni produkt szyfrujący (ACx oraz CEx). Sesja konsoli używa najsilniejszego możliwego szyfrowania zależnego od zainstalowanego w serwerze iSeries oraz na komputerze PC z Operations Console produktu szyfrującego.

Uwaga: Jeśli produkty do szyfrowania danych nie zostaną zainstalowane, dane nie będą szyfrowane.

Integralność danych

Integralność danych umożliwia sprawdzenie, czy dane konsoli nie zostały zmienione przed dotarciem do odbiorcy. Do ochrony danych konsoli Operations Console z połączeniem bezpośrednim wykorzystuje połączenie fizyczne, podobnie jak konsola twinaksowa lub chronione połączenie sieciowe LAN. Operations Console z połączeniem bezpośrednim używa tej samej integralności danych, co połączenie twinaksowe. Jeśli połączenie fizyczne jest chronione, to dane konsoli pozostają zabezpieczone.

Operations Console z połączeniem LAN wykorzystuje chronione połączenie sieciowe, jeśli został zainstalowany odpowiedni produkt szyfrujący (ACx oraz CEx). Sesja konsoli używa najsilniejszego możliwego szyfrowania zależnego od zainstalowanego w serwerze iSeries oraz na komputerze PC z Operations Console produktu szyfrującego.

Uwaga: Jeśli produkty do szyfrowania danych nie zostaną zainstalowane, dane nie będą szyfrowane.

Używanie konsoli Operations Console z połączeniem LAN

Uwaga: Dowolne urządzenie Operations Console może być konsolą, jednak tylko konfiguracje oparte na sieci LAN mogą używać profilu użytkownika narzędzi serwisowych.

Serwer iSeries dostarczany jest z domyślnym profilem urządzenia narzędzi serwisowych QCONSOLE z hasłem o wartości domyślnej QCONSOLE. Operations Console z połączeniem LAN będzie zmieniać hasło podczas każdego połączenia, które się powiedzie. Więcej informacji można znaleźć w sekcji “Używanie kreatora konfiguracji Operations Console”.

Więcej informacji na temat iSeries Operations Console z połączeniem LAN, znajduje się w Centrum informacyjnym, w artykule Operations Console z połączeniem LAN.

Zabezpieczenie konsoli Operations Console z połączeniem LAN

Podczas używania konsoli Operations Console z połączeniem LAN zaleca się:

- Utworzenie profilu urządzenia narzędzi serwisowych z atrybutami konsoli i umieszczenie informacji o profilu w bezpiecznym miejscu.
- Zainstalowanie w serwerze iSeries programu Cryptographic Access Provider, 5722–AC2 lub 5722–AC3 oraz na komputerze z Operations Console PC programu Client Encryption, 5722–CE2 lub 5722–CE3.
- Wybranie nietrywialnego hasła urządzenia serwisowego.
- Zabezpieczenie komputera PC z Operations Console, podobnie jak konsolę twinaksową lub Operations Console z połączeniem bezpośrednim.

Używanie kreatora konfiguracji Operations Console

Wszystkie wymagane informacje na komputerze PC używającym Operations Console z połączeniem LAN zostaną dodane przez kreator instalacji. Kreator instalacji poprosi o wprowadzenie profilu urządzenia narzędzi serwisowych, hasła profilu urządzenia narzędzi serwisowych oraz hasła do zabezpieczenia informacji o profilu urządzenia narzędzi serwisowych.

Uwaga: Hasło do informacji o profilu urządzenia narzędzi serwisowych jest wykorzystywane do blokowania i odblokowywania informacji o profilu (profilu urządzenia narzędzi serwisowych i hasła) na komputerze PC.

Po ustanowieniu połączenia sieciowego kreator instalacji Operations Console, zanim udostępni zaszyfrowany profil urządzenia narzędzi serwisowych i hasła, zapyta o hasło do informacji o urządzeniu serwisowym. Konieczne też będzie podanie poprawnego identyfikatora użytkownika narzędzi serwisowych oraz hasła.

Rozdział 9. Wykrywanie podejrzanych programów

Gwałtowny rozwój sieci komputerowych spowodował zwiększenie prawdopodobieństwa, że system używa programów z niezaufanych źródeł i programów wykonujących nieznane operacje. Oto przykłady:

- użytkownik komputera osobistego czasami dostaje programy od innych użytkowników komputerów PC; jeśli komputer PC jest podłączony do systemu iSeries, programy te mogą wpływać na serwer iSeries,
- użytkownicy połączeni w sieci również mogą otrzymywać programy,
- hakerzy są bardziej aktywni i sławni; często publikują stosowane metody i otrzymane rezultaty; prowadzi to do naśladownictwa przez zwykle przestrzegających prawa programistów.

Opisane trendy doprowadziły do problemu związanego z ochroną komputerów, czyli do **wirusów komputerowych**. Wirus jest programem, który może zmodyfikować inne programy tak, aby zawierały jego kopię. Mówi się wówczas, że inne programy są zainfekowane. Wirus może wykonywać dodatkowo inne operacje, które zajmą część zasobów systemowych, lub niszczą dane.

Architektura serwera iSeries zapewnia pewną ochronę przed infekcjami charakterystycznymi dla wirusów komputerowych. Zagadnienie to opisuje poniższa sekcja “Ochrona przed wirusami komputerowymi”. Administrator ochrony serwera iSeries musi zwracać baczną uwagę na programy wykonujące nieuprawnione funkcje. Pozostałe sekcje w tym rozdziale opisują niektóre sposoby działania hakerów. Zawierają również wskazówki dotyczące ochrony przed wykonaniem nieuprawnionych funkcji przez programy.

Wskazówka dotycząca ochrony

Uprawnienie do obiektu jest zawsze pierwszą linią obrony. System, w którym nie ma dobrego planu zabezpieczenia obiektów, jest bezbronny. Ten rozdział opisuje sposoby, których może próbować użyć użytkownik autoryzowany, aby wykorzystać luki w schemacie uprawnień do obiektów.

Ochrona przed wirusami komputerowymi

W komputerze, który jest zarażony wirusem, znajduje się program, który może zmieniać inne programy. Architektura obiektowa systemu iSeries utrudnia tym programom generowanie i rozprzestrzenianie wirusów w dużo większym stopniu niż w przypadku innych architektur komputerów. W serwerze iSeries do pracy z każdym typem obiektów używa się określonych komend i instrukcji. Nie można użyć instrukcji przeznaczonej dla zbiorów do zmiany działającego obiektu programowego (co czyni większość twórców wirusów). Nie można też łatwo utworzyć programu zmieniającego inny obiekt programowy. Wykonanie tego zadania wymaga znacznej ilości czasu, wysiłku i doświadczenia, a ponadto dostępu do narzędzi i dokumentacji, które nie są ogólnie dostępne.

Jednak wraz z pojawianiem się nowych funkcji serwera iSeries umożliwiających zaistnienie w środowisku systemów otwartych, niektóre funkcje zabezpieczenia serwera iSeries oparte na obiektach nie są już stosowane. Na przykład użytkownicy zintegrowanego systemu plików mają bezpośredni dostęp do niektórych obiektów w katalogach, takich jak pliki strumieniowe.

Ponadto, architektura serwera iSeries utrudnia wprawdzie wirusowi rozprzestrzenianie się pomiędzy programami iSeries, ale nie chroni serwera iSeries przed przenoszeniem wirusów do innych systemów. Jako serwer plików, iSeries może przechowywać programy współużytkowane przez wielu użytkowników komputerów PC. Każdy z tych programów może zawierać wirus nie wykrywany przez serwer iSeries. Aby uniemożliwić temu typowi wirusa zarażenie komputerów PC podłączonych do serwera iSeries, należy używać oprogramowania PC wyszukującego wirusy.

W serwerze iSeries dostępne są funkcje uniemożliwiające użytkownikom używanie języka niskiego poziomu z obsługą wskaźników do zmiany działającego obiektu programowego:

- Jeśli system działa z poziomem ochrony 40 lub wyższym, zabezpieczenie integralności obejmuje zabezpieczenie przed zmianą obiektów programowych. Na przykład nie można pomyślnie uruchomić programu zawierającego zablokowane (zabezpieczone) instrukcje maszynowe.
- Dostępna jest również wartość potwierdzania programu użytkownika podczas odtwarzania programu zeskładowanego (i potencjalnie zmienionego) w innym systemie. Rozdział 2 w książce *iSeries Ochrona* opisuje funkcje zabezpieczenia integralności dla poziomu ochrony 40 i wyższego, w tym wartości potwierdzania programu.

  Uwaga: Wartość potwierdzania programu może zostać uszkodzona, dlatego nic nie zastępuje czujności, którą należy wykazać w ocenianiu programów odtwarzanych w systemie.

Dostępne są również narzędzia pomagające wykryć pojawienie się zmienionego programu w systemie:

- Można użyć komendy Sprawdzenie integralności obiektu (Check Object Integrity - CHKOBJITG), aby skanować obiekty (działające obiekty) odpowiadające wartościom wyszukiwania, aby sprawdzić, czy te obiekty nie zostały zmienione. Funkcja ta jest podobna do funkcji wyszukiwania wirusów.
- Można użyć funkcji kontroli ochrony do monitorowania programów zmienianych i odtwarzanych. Wartości *PGMFAIL, *SAVRST i *SECURITY dla wartości systemowej Poziom uprawnień udostępniają rekordy kontroli pomocne w wykrywaniu prób wprowadzenia do systemu wirusów. Rozdział 9 i dodatek F w książce *iSeries Ochrona* zawierają więcej informacji na temat wartości kontroli i pozycji kroniki kontroli.
- Można użyć parametru Wymuszenie tworzenia (FRCCRT) komendy Zmiana programu (Change Program - CHGPGM) do ponownego utworzenia wszystkich programów, które zostały odzyskane w systemie. Do ponownego utworzenia programu system używa szablonu. Jeśli obiekt programu został zmieniony po kompilacji, system ponownie tworzy zmieniony obiekt i zastępuje go. Jeśli szablon programu zawiera zablokowane (zabezpieczone) instrukcje, system nie utworzy ponownie programu.
- Można użyć wartości systemowej QFRCCVNRST (wymuszenie konwersji przed odtwarzaniem), aby ponownie utworzyć dowolny program zeskładowany w systemie. Do ponownego utworzenia programu system używa szablonu. Ta wartość systemowa udostępnia kilka metod ponownego utworzenia programu.
- Można użyć wartości systemowej QVFYOBJRST (sprawdzanie obiektów przed odtworzeniem), aby zapobiec odtworzeniu programów nie posiadających podpisu cyfrowego lub z niepoprawnym podpisem cyfrowym. Jeśli podpis cyfrowy jest niepoprawny, oznacza to, że program został zmieniony od czasu jego ustanowienia przez twórcę. Istnieją funkcje API umożliwiające podpisywanie własnych programów, zbiorów składowania oraz plików strumieniowych.

Więcej informacji o podpisywaniu i wykorzystywaniu podpisów do zabezpieczenia systemu przed atakami można znaleźć w sekcji “Podpisywanie obiektów” na stronie 82.

Monitorowanie użycia uprawnień adoptowanych

W serwerze iSeries można utworzyć program adoptujący uprawnienie właściciela programu. Oznacza to, że każdy użytkownik uruchamiający program ma takie same uprawnienia (uprawnienie prywatne i uprawnienia specjalne), jak profil użytkownika będący właścicielem programu.

Uprawnienie adoptowane jest cennym narzędziem ochrony, jeśli jest poprawnie używane. Sekcja “Rozwinięcie kontroli dostępu do menu o ochronę obiektów” na stronie 46 opisuje na przykład, jak łączyć uprawnienie adoptowane i menu, aby rozszerzyć ochronę o elementy inne niż kontrola dostępu przez menu. Uprawnień adoptowanych można używać do zabezpieczenia ważnych zbiorów przed zmianami poza upoważnionymi programami, umożliwiając jednocześnie kierowanie zapytań do tych zbiorów.

Administrator ochrony musi być pewien, że uprawnienia adoptowane są poprawnie używane:

- Programy powinny adoptować uprawnienia profilu użytkownika posiadającego tylko uprawnienia wystarczające do wykonania niezbędnych funkcji, a nie profilu o szerokich uprawnieniach. Należy zachować szczególną ostrożność w przypadku programów adoptujących uprawnienie profilu użytkownika dysponującego uprawnieniem specjalnym *ALLOBJ lub będącego właścicielem ważnych obiektów.
- Programy adoptujące uprawnienia powinny mieć konkretne, ograniczone funkcje i nie powinny umożliwiać wprowadzania komend.
- Programy adoptujące uprawnienia powinny być odpowiednio zabezpieczone.
- Nadmierne użycie uprawnienia adoptowanego może mieć negatywny wpływ na wydajność systemu. Aby uniknąć problemów związanych z wydajnością, należy przejrzeć sieci działań sprawdzania uprawnień i sugestie dotyczące używania uprawnień adoptowanych w rozdziale 5 książki *iSeries Ochrona*.

Opcje menu SECBATCH:
1 *wprowadzenie natychmiastowe* **40** *użycie programu do planowania*

Do monitorowania użycia uprawnień adoptowanych w systemie pomocne może być użycie komendy Drukowanie obiektów adoptujących (Print Adopting Objects - PRTADPOBJ) (opcja 21 w menu SECTOOLS).

Wydruk prezentuje uprawnienia specjalne określonych profili użytkowników, programy, które akceptują zarówno uprawnienia profili użytkowników, jak i urządzenia ASP wykorzystujące te uprawnienia. Po ustanowieniu bazy informacji można regularnie drukować zmienioną wersję raportu o adoptowanych obiektach. Raport ten zawiera nowe programy adoptujące uprawnienia i programy, które zostały zmienione w taki sposób, że adoptują uprawnienia. Raport obejmuje zmiany od ostatniego uruchomienia tego raportu.

Jeśli zachodzi podejrzenie, że uprawnienie adoptowane jest nadużywane w systemie, można ustawić wartość systemową QAUDLVL na *PGMADP. Gdy ta wartość jest aktywna, system tworzy pozycję kroniki kontroli, gdy rozpoczyna się lub kończy pracę programu adoptującego uprawnienie. Pozycja zawiera nazwę użytkownika, który uruchomił program, i nazwę programu.

Ograniczenie użycia uprawnień adoptowanych

Gdy program iSeries działa, może on używać uprawnienia adoptowanego w celu uzyskania dostępu do obiektów na dwa różne sposoby:

- Program sam może adoptować uprawnienie właściciela. Podaje się to w parametrze profil użytkownika (USRPRF) programu lub programu serwisowego.
- Program może dziedziczyć uprawnienie adoptowane od poprzedniego programu, który nadal znajduje się na stosie wywołań zadania. Program może dziedziczyć uprawnienie adoptowane od poprzednich programów, nawet jeśli sam nie adoptuje uprawnienia. Parametr Użycie uprawnień adoptowanych (USEADPAUT) programu lub programu serwisowego kontroluje, czy program dziedziczy uprawnienie adoptowane od poprzednich programów na stosie programu.

Poniżej znajduje się przykład sposobu działania użycia uprawnienia adoptowanego od poprzednich programów.

Przyjmijmy, że profil użytkownika ICOWNER ma uprawnienie *CHANGE do zbioru ITEM i uprawnienie publiczne do tego zbioru to *USE. Żadne inne profile użytkowników nie mają jawnie zdefiniowanych uprawnień do zbioru ITEM. Tabela 14 przedstawia atrybuty dla trzech programów używających zbioru ITEM:

Tabela 14. Użycie uprawnień adoptowanych (USEADPAUT) - przykład

Nazwa programu	Właściciel programu	Wartość USRPRF	Wartość USEADPAUT
PGMA	ICOWNER	*OWNER	*YES
PGMB	ICOWNER	*USER	*YES
PGMC	ICOWNER	*USER	*NO

Przykład 1 – adoptowanie uprawnienia:
1. USERA uruchamia program PGMA.
2. Program PGMA próbuje otworzyć zbiór ITEM z możliwością aktualizacji.

Rezultat: próba powiodła się. USERA ma dostęp *CHANGE do zbioru ITEM ponieważ program PGMA adoptuje uprawnienie ICOWNER.

Przykład 2 – użycie uprawnień adoptowanych:
1. USERA uruchamia program PGMA.
2. Program PGMA wywołuje program PGMB.
3. Program PGMB próbuje otworzyć zbiór ITEM z możliwością aktualizacji.

Rezultat: próba powiodła się. Mimo że program PGMB nie adoptuje uprawnienia (*USRPRF ma wartość *USER), umożliwia on użycie poprzednio adoptowanego uprawnienia (*USEADPAUT ma wartość *YES). Program PGMA nadal znajduje się na stosie programu. Tak więc USERA otrzymuje dostęp *CHANGE do zbioru ITEM ponieważ program PGMA adoptuje uprawnienie ICOWNER.

Przykład 3 – brak użycia uprawnień adoptowanych:
1. USERA uruchamia program PGMA.
2. Program PGMA wywołuje program PGMC.
3. Program PGMC próbuje otworzyć zbiór ITEM z możliwością aktualizacji.

Rezultat: błąd uprawnień. Program PGMC nie adoptuje uprawnienia. Program PGMC również nie zezwala na użycie uprawnienia adoptowanego z poprzednich programów. Mimo że program PGMA nadal znajduje się na stosie wywołań, jego uprawnienie adoptowane jest używane.

Zabezpieczenie przed użyciem uprawnień adoptowanych przez nowe programy

Przekazywanie uprawnień adoptowanych do następnych programów na stosie umożliwia doświadczonemu programiście utworzenie programu typu koń trojański. Program typu koń trojański może od poprzednich programów na stosie pobrać uprawnienie potrzebne do popełnienia oszustwa. Aby temu zapobiec, można ograniczyć liczbę użytkowników, którzy mogą tworzyć programy używające uprawnień adoptowanych od poprzednich programów.

Podczas tworzenia nowego programu system automatycznie ustawia parametr USEADPAUT na wartość *YES. Aby program nie dziedziczył uprawnienia adoptowanego, należy użyć komendy Zmiana programu (Change Program - CHGPGM) lub Zmiana programu serwisowego (Change Service Program - CHGSRVPGM) do ustawienia parametru USEADPAUT na *NO.

Do określania, kto może tworzyć programy dziedziczące uprawnienie adoptowane, można użyć listy autoryzacji i wartości systemowej uprawnienie adoptowane (QUSEADPAUT). Po podaniu nazwy listy autoryzacji w wartości systemowej QUSEADPAUT, system używa tej listy autoryzacji do określania, jak tworzyć nowe programy.

Gdy użytkownik tworzy program lub program serwisowy, system sprawdza uprawnienia użytkownika do listy autoryzacji. Jeśli użytkownik ma uprawnienie *USE, parametr USEADPAUT dla nowego programu jest ustawiany na *YES. Jeśli użytkownik nie ma uprawnienia *USE, parametr USEADPAUT jest ustawiany na wartość *NO. Uprawnienie użytkownika do listy autoryzacji nie może pochodzić od uprawnienia adoptowanego.

Lista autoryzacji podana w wartości systemowej QUSEADPAUT określa również, czy użytkownik może używać komendy CHGxxx do ustawienia wartości USEADPAUT dla programu i programu serwisowego.

Uwagi:

1. Nie trzeba nadawać liście autoryzacji nazwy QUSEADPAUT. Można utworzyć listę autoryzacji o innej nazwie. Następnie należy podać tę listę w wartości systemowej QUSEADPAUT. W komendach w podanym przykładzie należy podstawić nazwę własnej listy autoryzacji.
2. Wartość systemowa QUSEADPAUT nie wpływa na programy istniejące w systemie. Aby ustawić parametr USEADPAUT dla istniejących programów, należy użyć komendy CHGPGM lub CHGSRVPGM.

Bardziej zamknięte środowisko: jeśli większość użytkowników ma tworzyć nowe programy z parametrem USEADPAUT ustawionym na *NO:

1. Aby ustawić uprawnienie publiczne dla listy autoryzacji na *EXCLUDE, należy wpisać:
   ```
   CHGAUTLE AUTL(QUSEADPAUT) USER(*PUBLIC)
      AUT(*EXCLUDE)
   ```
2. Aby skonfigurować konkretnych użytkowników tak, aby tworzyli programy używające uprawnień adoptowanych poprzednich programów, należy wpisać:
   ```
   ADDAUTLE AUTL(QUSEADPAUT) USER(nazwa-użytkownika)
      AUT(*USE)
   ```

Mniej wymagające środowisko: jeśli większość użytkowników ma tworzyć nowe programy z parametrem USEADPAUT ustawionym na *YES, należy:

1. Pozostawić niezmienione uprawnienie publiczne dla listy autoryzacji ustawione na *USE.
2. Aby uniemożliwić konkretnym użytkownikom tworzenie programów używających uprawnień adoptowanych od poprzednich programów, należy wpisać:

```
ADDAUTLE AUTL(QUSEADPAUT)
   USER(nazwa-użytkownika)
        AUT(*EXCLUDE)
```

Monitorowanie użycia programów wyzwalanych

DB2 UDB umożliwia powiązanie programów wyzwalanych ze zbiorami bazy danych. Obsługa programów wyzwalanych jest powszechna w przypadku menedżerów baz danych stosowanych w przemyśle.

Podczas wiązania programu wyzwalanego ze zbiorem bazy danych, użytkownik określa, kiedy ma on być uruchamiany. Na przykład można skonfigurować zbiór zamówień klienta tak, aby uruchamiał program wyzwalany za każdym razem, gdy do zbioru jest dodawany nowy rekord. Gdy bilans zaległości klienta przekroczy określony limit, program wyzwalany może wydrukować list ostrzegawczy do klienta i wysłać komunikat do menedżera kredytów.

Programy wyzwalane są produktywnym narzędziem zarówno do udostępniania funkcji aplikacji, jak i do zarządzania informacją. Programy wyzwalane są również dla osób z nieuczciwymi intencjami środkiem do tworzenia "koni trojańskich" w systemie. Destrukcyjny program może oczekiwać na odpowiedni moment do uruchomienia, gdy nastąpi określone zdarzenie w zbiorze bazy danych w systemie.

Uwaga: Historycznie koń trojański był ogromnym, drewnianym koniem, w środku którego znajdowali się greccy żołnierze. Gdy koń znalazł się wewnątrz murów Troi, żołnierze wyszli z niego, otwarli bramy i wpuścili do Troi żołnierzy greckich. W świecie komputerów program, który ukrywa niszczące funkcje, jest często nazywany koniem trojańskim.

Opcje menu SECBATCH:
27 *wprowadzenie natychmiastowe* **66** *użycie programu do planowania*

W dostarczanym systemie możliwość dodawania programów wyzwalanych do zbioru bazy danych jest ograniczona. Jeśli ostrożnie zarządza się uprawnieniami do obiektów, zwykły użytkownik nie będzie miał wystarczających uprawnień do dodawania programów wyzwalanych do zbioru bazy danych. (Dodatek D w książce *iSeries Ochrona* podaje wymagane uprawnienia i wszystkie komendy, w tym Dodanie wyzwalacza zbioru fizycznego (Add Physical File Trigger - ADDPFTRG).

Aby wydrukować listę wszystkich programów wyzwalanych w konkretnej bibliotece lub we wszystkich bibliotekach, można użyć komendy Drukowanie programów wyzwalanych (Print Trigger Programs - PRTTRGPGM).

Raportu początkowego można użyć jako bazy do oceny programów wyzwalanych już istniejących w systemie. Następnie można regularnie drukować raport zmian, aby zobaczyć jakie nowe programy wyzwalane zostały dodane do systemu.

Podczas oceny programów wyzwalanych należy wziąć pod uwagę:

- Kto utworzył dany program wyzwalany? Aby to sprawdzić, można użyć komendy Wyświetlenie opisu obiektu (Display Object Description - DSPOBJD).
- Co robi dany program? Aby to ustalić, należy obejrzeć program źródłowy lub porozmawiać z autorem danego programu. Na przykład czy program wyzwalany sprawdza, kim jest użytkownik? Być może program wyzwalany czeka na konkretnego użytkownika (QSECOFR), aby uzyskać dostęp do zasobów systemu.

Po przygotowaniu bazy informacji można regularnie drukować raport zmian, aby monitorować nowe programy wyzwalane, które dodano do systemu.

Szukanie ukrytych programów

Zastosowanie programów wyzwalanych nie jest jedynym sposobem wprowadzenia do systemu konia Trojańskiego. Programy wyzwalane są przykładem **programów obsługi wyjścia**. Gdy wystąpi pewne zdarzenie, takie jak aktualizacja zbioru w przypadku programu wyzwalanego, system uruchamia program obsługi wyjścia powiązany z tym zdarzeniem.

Tabela 15 przedstawia inne przykłady programów obsługi wyjścia, które mogą znajdować się w systemie. Do określenia sposobu użycia i zawartości tych programów należy użyć tych samych metod, których używa się dla programów wyzwalanych.

Uwaga: Tabela 15 nie zawiera wszystkich możliwych programów obsługi wyjścia.

.

Tabela 15. Programy obsługi wyjścia dostarczone przez system

Nazwa programu	Uruchomienie programu
Nazwa podana przez użytkownika w atrybucie sieciowym DDMACC.	Gdy użytkownik próbuje otworzyć plik DDM w systemie lub nawiązuje połączenie DRDA.
Nazwa podana przez użytkownika w atrybucie sieciowym PCSACC.	Gdy użytkownik próbuje użyć funkcji programu Client Access używając Oryginalnych klientów do uzyskania dostępu do obiektów w systemie.
Nazwa podana przez użytkownika w wartości systemowej QPWDVLDPGM.	Gdy użytkownik uruchamia funkcję Zmiana hasła.
Nazwa podana przez użytkownika w wartości systemowej QRMTSIGN.	Gdy użytkownik próbuje wpisać się interaktywnie ze zdalnego systemu.
QSYS/QEZUSRCLNP	Gdy zostają uruchomione funkcje automatycznego czyszczenia.
Nazwa podana przez użytkownika w parametrze EXITPGM komendy CHGBCKUP.	Gdy używa się funkcji składowania Asysty operacyjnej.
Nazwy podane przez użytkownika w komendzie CRTPRDLOD.	Przed i po składowaniu, odzyskaniu i usunięciu produktu utworzonego za pomocą tej komendy.
Nazwa podana przez użytkownika w parametrze DFTPGM komendy CHGMSGD.	Jeśli dla komunikatu podano program domyślny, system uruchamia ten program po wydaniu komunikatu. Z powodu dużej liczby opisów komunikatów w typowym systemie, trudno monitorować użycie programów domyślnych. Aby uniemożliwić użytkownikom publicznym dodawanie programów domyślnych dla komunikatów, można ustawić uprawnienie publiczne dla zbiorów komunikatów (obiekty *MSGF) na *USE.
Nazwa podana przez użytkownika w parametrze FKEYPGM komendy STREML3270.	Gdy użytkownik naciśnie klawisz funkcyjny podczas sesji emulacji urządzenia 3270. System zwraca sterowanie do sesji emulacji urządzenia 3270 po zakończeniu programu obsługi wyjścia.
Nazwa podana przez użytkownika w parametrze EXITPGM komend monitora wydajności.	Do przetworzenia danych zgromadzonych przez komendy: STRPFRMON, ENDPFRMON, ADDPFRCOL i CHGPFRCOL. Program jest uruchamiany, gdy zakończy się zbieranie danych.
Nazwa podana przez użytkownika w parametrze EXITPGM komendy RCVJRNE.	Dla każdej pozycji lub grupy pozycji kroniki czytanej z podanej kroniki lub dziennika.
Nazwa podana przez użytkownika w funkcji API QTNADDCR.	Podczas operacji COMMIT i ROLLBACK.
Nazwy podane przez użytkownika w funkcji API QHFRGFS.	Do wykonania funkcji systemu plików.

Tabela 15. Programy obsługi wyjścia dostarczone przez system (kontynuacja)

Nazwa programu	Uruchomienie programu
Nazwa podana przez użytkownika w parametrze SEPPGM opisu drukarki.	Do określenia, co należy drukować na stronie separującej przed i po zbiorze buforowym i zadaniu drukowania.
QGPL/QUSCLSXT	Gdy zamykany jest zbiór bazy danych, w celu umożliwienia przechwycenia informacji o użyciu zbioru.
Nazwa podana przez użytkownika w parametrze FMTSLR zbioru logicznego.	Gdy do zbioru bazy danych zapisywany jest rekord i nazwa formatu rekordu nie jest dołączana do programu w języku wysokiego poziomu. Program selektor otrzymuje rekord jako dane wejściowe, określa używany format rekordu i zwraca go do bazy danych.
Nazwa podana przez użytkownika podana w wartości systemowej QATNPGM, parametrze ATNPGM w profilu użytkownika lub parametrze PGM komendy SETATNPGM.	Gdy użytkownik naciśnie klawisz Attention.
Nazwa podana przez użytkownika w parametrze EXITPGM komendy TRCJOB.	Przed uruchomieniem procedury Śledzenie zadania.

W przypadku komend umożliwiających podanie programu obsługi wyjścia należy sprawdzić, czy nie zmieniono domyślnych ustawień komendy na podawanie programu obsługi wyjścia. Należy również upewnić się, że uprawnienia publiczne dla tych komend nie umożliwiają zmiany wartości domyślnych komend. Komenda CHGCMDDFT wymaga uprawnienia *OBJMGT do komendy. Uprawnienie *OBJMGT nie jest potrzebne do uruchomienia komendy.

Ocena zarejestrowanego programu obsługi wyjścia

Do rejestrowania programów obsługi wyjścia, które powinny być uruchamiane, gdy nastąpi określone zdarzenie, można użyć systemowej funkcji rejestrowania. Aby wyświetlić informacje rejestracyjne w systemie, należy wpisać WRKREGINF OUTPUT(*PRINT). Rys. 8 przedstawia przykładowy raport.

```
                  Praca z informacją rejestracyjną
                (Work with Registration Information)
Punkt wyjścia. . . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
Format punktu wyjścia. . . . . . . . . :   NJE00100
Zarejestrowany punkt wyjścia . . . . . :   *YES
Zezwolenie na usuwanie z rejestru. . . :   *YES
Maksymalna liczba prog. obsł. wyjścia. :   *NOMAX
Bieżąca liczba programów obsł. wyjścia :   0
Wstępne przetwarzanie dla dodawania. . :   *NONE
  Biblioteka . . . . . . . . . . . . . :
  Format . . . . . . . . . . . . . . . :
Wstępne przetwarzanie dla usuwania . . :   *NONE
  Biblioteka . . . . . . . . . . . . . :
  Format . . . . . . . . . . . . . . . :
Wstępne przetwarzanie dla pobierania . :   *NONE
  Biblioteka . . . . . . . . . . . . . :
```

Rysunek 8. Praca z informacją rejestracyjną - przykład

Dla każdego punktu wyjścia w systemie raport podaje, czy są zarejestrowane jakieś programy obsługi wyjścia. Gdy punkt wyjścia ma aktualnie zarejestrowane programy, aby wyświetlić informacje o tych programach można wybrać opcję 8 (Wyświetlenie programów) z ekranu komendy WRKREGINF:

```
                    Praca z informacją rejestracyjną
                  (Work with Registration Information)

Wpisz opcje i naciśnij klawisz Enter.
5=Wyświetlenie punktu wyjścia  8=Praca z programami obsługi wyjścia

                          Format
     Punkt                punktu
Opc  wyjścia              wyjścia   Zarejestr.  Tekst
     QIBM_QGW_NJEOUTBOUND  NJEO0100     *YES     Network Job Entry outbound ex
8    QIBM_QHQ_DTAQ         DTAQ0100     *YES     Original Data Queue Server
     QIBM_QLZP_LICENSE     LICM0100     *YES     Original License Mgmt Server
     QIBM_QMF_MESSAGE      MESS0100     *YES     Original Message Server
     QIBM_QNPS_ENTRY       ENTR0100     *YES     Network Print Server - entry
     QIBM_QNPS_SPLF        SPLF0100     *YES     Network Print Server - spool
     QIBM_QNS_CRADDACT     ADDA0100     *YES     Add CRQ description activity
     QIBM_QNS_CRCHGACT     CHGA0100     *YES     Change CRQ description activi
```

Do oceny tych programów obsługi wyjścia należy użyć tych samych metod, których używa się do innych programów obsługi wyjścia i programów wyzwalanych.

Sprawdzenie zaplanowanych programów

Serwer iSeries udostępnia wiele metod planowania zadań przeznaczonych do uruchomienia w późniejszym czasie, w tym program do planowania zadań. W normalnych warunkach omawiane metody nie naruszają ochrony, ponieważ użytkownik planujący zadanie musi mieć to samo uprawnienie, które jest wymagane do wprowadzenia zadania wsadowego.

Jednak od czasu do czasu należy sprawdzać zaplanowane zadania. Nienależący już do organizacji niezadowolony użytkownik może użyć tej metody do zaplanowania katastrofy w systemie.

Ograniczanie możliwości składowania i odtwarzania

Większość użytkowników nie wykonuje składowania i odtwarzania obiektów w systemie. Komendy służące do składowania umożliwiają skopiowanie na nośniki lub do innego systemu ważnych zasobów organizacji. Większość komend składowania obsługuje zbiory składowania, które mogą być wysłane do innego systemu (przy użyciu komendy SNDNETF) bez dostępu do nośnika lub urządzenia składowania/odtwarzania.

Komendy odtwarzania umożliwiają odtwarzanie w systemie nieautoryzowanych obiektów, takich jak programy, komendy i zbiory. Można również odtwarzać informacje bez dostępu do nośnika lub urządzenia składowania/odtwarzania używając zbiorów składowania. Zbiory składowania mogą być wysyłane z innego systemu za pomocą komendy SNDNETF lub poprzez FTP.

Poniżej znajdują się sugestie dotyczące ograniczania operacji składowania i odtwarzania w systemie:

- Należy kontrolować, którzy użytkownicy mają uprawnienie specjalne *SAVSYS. Uprawnienie to umożliwia użytkownikowi składowanie i odtwarzanie obiektów, nawet jeśli użytkownik nie ma niezbędnych uprawnień do tych obiektów.
- Należy sprawować kontrolę nad dostępem do urządzeń składowania i odtwarzania.
- Należy ograniczać dostęp do komend składowania i odtwarzania. Podczas instalowania programów licencjonowanych OS/400 uprawnienia publiczne dla komend RSTxxx mają wartość *EXCLUDE. Uprawnienia publiczne dla komend SAVxxx mają wartość *USE. Należy rozważyć zmianę uprawnienia publicznego dla komend SAVxxx na *EXCLUDE. Należy ograniczyć liczbę użytkowników uprawnionych do używania komend RSTxxx.

- Należy użyć wartości systemowej QALWOBJRST do ograniczenia odtwarzania programów zmieniających stan systemu, programów adoptujących uprawnienia i obiektów, w których wystąpiły błędy sprawdzania.
- Należy użyć wartości systemowej QVFYOBJRST w celu sterowania odtwarzaniem podpisanych obiektów w systemie.
- Do ponownego utworzenia konkretnych obiektów, które są odtwarzane w systemie, należy użyć wartości systemowej QFRCCVNRST.
- Należy używać kontroli ochrony do monitorowania operacji odtwarzania. Należy włączyć *SAVRST do wartości systemowej QAUDLVL i okresowo drukować rekordy kontroli tworzone przez operacje odtwarzania. (Rozdział 9 i dodatek F w książce *iSeries Ochrona* zawierają więcej informacji na temat operacji na pozycjach kontroli.)

Sprawdzenie obiektów użytkownika w zabezpieczonych bibliotekach

Każde zadanie serwera iSeries ma listę bibliotek. Lista bibliotek określa, w jakiej kolejności system będzie przeszukiwał biblioteki, jeśli wraz z nazwą obiektu nie podano nazwy biblioteki. Na przykład jeśli wywołuje się program nie podając gdzie on się znajduje, system przeszukuje listę bibliotek zgodnie z podaną kolejnością i uruchamia pierwszą odnalezioną kopię programu.

Książka *iSeries Ochrona* zawiera więcej informacji o narażaniu ochrony w przypadku list bibliotek i wywoływania programów bez podawania nazwy biblioteki (tak zwane **wywołanie niekwalifikowane**). Zawiera ona również sugestie dotyczące kontrolowania zawartości listy bibliotek i możliwości zmiany list bibliotek systemowych.

Aby system działał poprawnie, niektóre biblioteki systemowe, takie jak QSYS i QGPL muszą znajdować się na liście bibliotek dla każdego zadania. Do kontrolowania, kto może dodawać programy do tych bibliotek należy użyć uprawnień do obiektów. Chroni to przed umieszczeniem w jednej z tych bibliotek programu oszusta z taką samą nazwą co program, który znajduje się w bibliotece występującej dalej na liście bibliotek.

Należy również określić, kto ma uprawnienia do komendy CHGSYSLIBL i monitorować rekordy SV w kronice kontroli ochrony. Użytkownik o nieuczciwych planach może umieścić na liście bibliotek przed QSYS jakąś bibliotekę i w ten sposób umożliwić innym użytkownikom uruchamianie nieautoryzowanych komend o takich samych nazwach, co komendy dostarczone przez IBM.

Opcje menu SECBATCH:
28 *wprowadzenie natychmiastowe* **67** *użycie programu do planowania*

Aby wydrukować listę obiektów użytkownika (obiektów nie utworzonych przez IBM) znajdujących się w danej bibliotece, można użyć komendy Drukowanie obiektów użytkownika (Print User Objects - PRTUSROBJ). Następnie można przejrzeć programy znajdujące się na liście i określić, kto je utworzył i jaką pełnią funkcję.

Obiekty użytkownika inne niż programy również stanowią zagrożenie dla ochrony, gdy znajdują się w bibliotekach systemowych. Na przykład jeśli program zapisuje poufne dane do zbioru o niekwalifikowanej nazwie, może on otworzyć wersję tego zbioru znajdującą się w bibliotece systemowej.

Rozdział 10. Wykrywanie prób włamania i zapobieganie im

Ten rozdział zawiera wiele wskazówek pomocnych przy wykrywaniu potencjalnego narażenia ochrony i osób czyniących szkody.

Ochrona fizyczna

Jednostka systemowa jest rzeczą wartościową i stanowi potencjalne drzwi do systemu. Niektóre komponenty systemu znajdujące się w środku są niewielkie i cenne. Jednostka systemowa powinna znajdować się w nadzorowanym miejscu, aby uniemożliwić wyjęcie z niej cennych komponentów systemu.

Jednostka systemowa ma panel sterowania umożliwiający wykonanie podstawowych funkcji bez stacji roboczej. Na przykład panelu sterowania można użyć do:

- zatrzymania systemu,
- uruchomienia systemu,
- załadowania systemu operacyjnego,
- uruchomienia funkcji serwisowych.

Wszystkie wymienione działania mogą przerwać pracę użytkowników systemu. Są one również zagrożeniem dla ochrony systemu. Do kontrolowania podejmowania wymienionych działań można użyć blokady dostarczonej razem z systemem. Aby uniemożliwić użycie panelu sterowania, należy ustawić kluczyk blokady w pozycji Secure, wyjąć go i umieścić w bezpiecznym miejscu.

Uwagi:

1. W przypadku zdalnego IPL lub diagnostyki systemu, należy ustawić blokadę w innym położeniu. Temat Pierwsze kroki w Centrum informacyjnym iSeries zawiera więcej informacji o ustawieniach blokady (szczegóły znajdują się w sekcji “Informacje wstępne i pokrewne” na stronie xii).
2. Nie wszystkie modele systemów są dostarczane z blokadą jako opcją standardową.

Monitorowanie aktywności profilu użytkownika

Profile użytkowników umożliwiają dostęp do systemu. Parametry podane w profilu użytkownika określają jego środowisko i charakterystyki dotyczące ochrony użytkownika. Administrator ochrony musi kontrolować zmiany zachodzące w profilach użytkowników w systemie.

Można tak skonfigurować kontrolę ochrony, aby system zapisywał zmiany w profilach użytkowników. Do wydrukowania raportu zmian można użyć komendy DSPAUDJRNE.

Do oceny żądanych działań na profilach użytkowników można utworzyć programy obsługi wyjścia. Tabela 16 przedstawia punkty wyjścia dostępne dla komend profilu użytkownika.

Tabela 16. Punkty wyjścia dla profilu użytkownika

Komenda profilu użytkownika	Nazwa punktu wyjścia
Tworzenie profilu użytkownika (Create User Profile - CRTUSRPRF)	QIBM_QSY_CRT_PROFILE
Zmiana profilu użytkownika (Change User Profile - CHGUSRPRF)	QIBM_QSY_CHG_PROFILE

Tabela 16. Punkty wyjścia dla profilu użytkownika (kontynuacja)

Komenda profilu użytkownika	Nazwa punktu wyjścia
Usunięcie profilu użytkownika (Delete User Profile - DLTUSRPRF)	QIBM_QSY_DLT_PROFILE
Odtworzenie profili użytkowników (Restore User Profile - RSTUSRPRF)	QIBM_QSY_RST_PROFILE

Program obsługi wyjścia może na przykład odszukać zmiany, które mogą spowodować, że użytkownik uruchomi nieautoryzowaną wersję programu. Do takich zmian należy przypisanie innego opisu zadania lub nowej biblioteki bieżącej. Program obsługi wyjścia może w takim przypadku powiadomić kolejkę komunikatów lub podjąć określone działanie (takie jak zmiana lub wyłączenie profilu użytkownika) w zależności od otrzymanych informacji.

Książka *iSeries Ochrona* zawiera więcej informacji na temat programów obsługi wyjścia dla działań związanych z profilami użytkowników.

Podpisywanie obiektów

Wszystkie zabezpieczenia nie mają sensu, gdy ktoś pominie je, wprowadzając celowo błędne dane do systemu. Serwer iSeries ma wiele wbudowanych funkcji uniemożliwiających załadowanie niebezpiecznego oprogramowania do systemu i wykrywających takie oprogramowanie, jeśli jest już ono w systemie. Jedną z technik dodanych w wersji V5R1 jest podpisywanie obiektów.

Podpisywanie obiektów jest zastosowaną w serwerze iSeries wersją koncepcji szyfrowania zwanej ″podpisami cyfrowymi″. Pomysł jest stosunkowo prosty: w momencie, gdy producent przygotuje gotową wersję oprogramowania dla klientów, ″podpisuje″ ją. Podpis ten nie gwarantuje, że oprogramowanie będzie wykonywało określone funkcje. Stanowi jednak dowód, że oprogramowanie pochodzi od producenta, który je podpisał, i że nie zostało zmienione od momentu wyprodukowania i podpisania. Jest to szczególnie ważne w sytuacji, gdy oprogramowanie zostało przesłane przez Internet lub przechowywane na nośniku, który mógł zostać zmodyfikowany.

Zastosowanie podpisów cyfrowych zwiększa kontrolę nad tym, jakie oprogramowanie jest ładowane do systemu, i zwiększa prawdopodobieństwo wykrycia zmian od momentu, kiedy zostanie załadowane. Nowa wartość systemowa Weryfikacja odtworzenia obiektu (QVFYOBJRST) umożliwia określenie restrykcyjnej strategii, która wymaga, aby całość oprogramowania ładowanego do systemu była podpisana przez znane źródło. Można także wybrać bardziej otwartą strategię i po prostu weryfikować podpisy wtedy, gdy istnieją.

Całe oprogramowanie systemu OS/400, a także oprogramowanie dla opcji i programy licencjonowane iSeries zostały podpisane przez zaufany system. Podpisy te pomagają w zachowaniu integralności systemu i są sprawdzane w momencie stosowania poprawek dla systemu w celu upewnienia się, że poprawka pochodzi z zaufanego systemu i nie została zmieniona w trakcie przesyłania. Podpisy mogą być także sprawdzane w czasie, gdy oprogramowanie jest już w systemie. Komenda CHKOBJITG (Sprawdzanie integralności obiektu) została rozbudowana i obecnie również sprawdza podpisy. Ponadto Menedżer certyfikatów cyfrowych zawiera ekrany, na których można sprawdzać podpisy obiektów, również tych, które są częścią systemu operacyjnego.

Ponieważ cały system operacyjny jest podpisany, można za pomocą podpisów cyfrowych zabezpieczyć integralność oprogramowania, które jest newralgiczne dla firmy. Można kupować oprogramowanie podpisane przez twórców, a także podpisywać zakupione lub napisane oprogramowanie. Częścią strategii ochrony może być regularne uruchamianie

komendy CHKOBJITG lub Menedżera certyfikatów cyfrowych w celu sprawdzenia, czy sygnatury oprogramowania są nadal poprawne - to jest, czy obiekty nie uległy modyfikacji od momentu, gdy zostały podpisane. Można także nałożyć wymóg, aby całe oprogramowanie odtwarzane na systemie było podpisane przez użytkownika lub znane źródło. Jednakże, ponieważ większość nie produkowanego przez IBM oprogramowania dla serwera iSeries nie jest obecnie podspisana, wymóg ten może być zbyt restrykcyjny dla danego systemu. Nowa obsługa podpisów cyfrowych daje elastyczność w decydowaniu, jak najlepiej zabezpieczyć integralność oprogramowania.

Podpisy cyfrowe zabezpieczające oprogramowanie to tylko jedno z możliwych ich zastosowań. Dodatkowe informacje na ten temat zawiera także Centrum informacyjne w temacie dotyczącym Menedżera certyfikatów cyfrowych (szczegółowe informacje znajdują się w sekcji “Informacje wstępne i pokrewne” na stronie xii).

Monitorowanie opisów podsystemu

Podczas uruchamiania podsystemu, serwer iSeries tworzy środowisko pracy umożliwiające wejście do systemu i działanie w nim. Środowisko to definiuje opis podsystemu. Dlatego opisy podsystemów nie powinny być dostępne dla niepowołanych użytkowników. Osoba, której celem jest czynienie szkód, może użyć opisu podsystemu do automatycznego uruchomienia programu lub do udostępnienia wpisania się bez profilu użytkownika.

Podczas uruchamiania komendy Odwołanie uprawnień publicznych (Revoke Public Authority - RVKPUBAUT), system ustawia uprawnienie publiczne do komend opisów podsystemów na *EXCLUDE. Uniemożliwia to użytkownikom, którzy nie są jawnie uprawnieni (i którzy nie mają uprawnienia specjalnego *ALLOBJ), zmianę i tworzenie opisów podsystemów.

Poniższe sekcje zawierają sugestie dotyczące przeglądania opisów podsystemów aktualnie istniejących w systemie. Aby utworzyć listę wszystkich opisów podsystemów, można użyć komendy Praca z opisami podsystemów (Work with Subsystem Descriptions - WRKSBSD). Po wybraniu z listy opcji 5 (Wyświetlanie) wyświetlane jest menu dla wybranego opisu systemu. Zawiera ono listę części należących do środowiska podsystemu.

Aby zobaczyć szczegóły dotyczące poszczególnych części podsystemu, należy wybierać odpowiednie opcje. Aby zmienić dwie pierwsze pozycje z menu, można użyć komendy Zmiana opisu podsystemu (Change Subsystem Description - CHGSBSD). Aby zmienić pozostałe pozycje, należy użyć odpowiedniej dla typu pozycji komendy dodawania, usuwania lub zmiany. Na przykład aby zmienić pozycję stacji roboczej, należy użyć komendy Zmiana pozycji stacji roboczej (Change Workstation Entry - CHGWSE).

Książka *Zarządzanie pracą w systemie AS/400* zawiera więcej informacji na temat pracy z opisami podsystemów. Podaje ona również standardowe wartości dla opisów podsystemów dostarczonych przez IBM.

Pozycje zadania autostartu

Pozycja zadania autostartu zawiera nazwę opisu zadania. Opis zadania może zawierać żądanie danych (RQSDTA), które powoduje uruchomienie programu lub komendy. Na przykład żądanie RQSDTA może mieć postać CALL LIB1/PROGRAM1. Za każdym razem gdy uruchamiany jest podsystem, system uruchamia program PROGRAM1 w bibliotece LIB1.

Należy przejrzeć pozycje zadania autostartu i powiązane z nimi opisy zadań oraz poznać funkcje wszystkich programów uruchamianych automatycznie podczas uruchamiania podsystemu.

Nazwy i typy stacji roboczych

Podsystem podczas uruchamiania przydziela wszystkie nieprzydzielone stacje robocze, wymienione w opisie w pozycjach określających nazwy i typy stacji roboczych. Gdy użytkownik wpisuje się, to wpisuje się do podsystemu, który przydzielił daną stację roboczą.

Pozycja stacji roboczej informuje, który opis zadania będzie używany, gdy na tej stacji roboczej zostanie uruchomione zadanie. Opis zadania może zawierać żądanie danych, które powoduje uruchomienie programu lub komendy. Na przykład parametr RQSDTA może mieć postać CALL LIB1/PROGRAM1. Za każdym razem gdy użytkownik wpisuje się do stacji roboczej w danym podsystemie, system uruchamia program PROGRAM1 w bibliotece LIB1.

Należy przejrzeć pozycje stacji roboczej i powiązane z nimi opisy zadań. Należy sprawdzić, czy ktoś nie dodał i nie uaktualnił pozycji uruchamiających programy, o których nie wiemy.

Pozycja stacji roboczej może również określać domyślny profil użytkownika. W przypadku niektórych konfiguracji podsystemów umożliwia to wpisanie się po prostu przez naciśnięcie klawisza Enter. Jeśli poziom ochrony (wartość systemowa QSECURITY) w systemie jest mniejszy niż 40, należy przejrzeć pozycje stacji roboczych dla domyślnych użytkowników.

Pozycje kolejki zadań

Podczas uruchamiania podsystem przydziela wszystkie nieprzydzielone kolejki zadań podane w opisie podsystemu. Pozycje kolejki zadań same w sobie nie stanowią bezpośredniego zagrożenia dla ochrony. Jednak umożliwiają one manipulowanie wydajnością systemu poprzez uruchamianie zadań w nieprzeznaczonych do tego środowiskach.

Należy okresowo przeglądać pozycje kolejki zadań w opisach podsystemów, aby sprawdzić, czy zadania wsadowe są uruchamiane tam, gdzie powinny.

Pozycje routingu

Pozycja routingu definiuje, co robi zadanie po pojawieniu się w podsystemie. Podsystem używa pozycji routingu dla wszystkich typów zadań: wsadowych, interaktywnych i komunikacyjnych. Pozycja routingu określa:

- Klasę dla zadania. Podobnie, jak pozycja kolejki zadań, klasa powiązana z zadaniem może wpłynąć na wydajność, ale nie stanowi ona zagrożenia dla ochrony.
- Program uruchamiany podczas uruchamiania zadania. Należy przejrzeć pozycje routingu i sprawdzić, czy ktoś nie dodał i nie uaktualnił pozycji uruchamiających programy, o których nie wiemy.

Pozycje komunikacji i nazwy zdalnego miejsca

Gdy zadanie komunikacyjne pojawia się w systemie, system używa pozycji komunikacji i pozycji określających nazwy zdalnych miejsc w aktywnym podsystemie, aby określić, w jaki sposób będzie uruchomione zadanie komunikacyjne. Poniżej podajemy trzy pozycje:

- Wszystkie podsystemy mogą uruchamiać zadania komunikacyjne. Jeśli podsystem przeznaczony do komunikacji jest nieaktywny, zadanie próbujące wejść do systemu może znaleźć pozycję spełniającą określone wymagania w innym opisie podsystemu. Należy przejrzeć pozycje we wszystkich opisach podsystemów.
- Pozycja komunikacji zawiera opis zadania. Opis zadania może zawierać żądanie danych, które powoduje uruchomienie programu lub komendy. Należy przejrzeć pozycje komunikacji i powiązane z nimi opisy zadań, aby zrozumieć sposób uruchamiania zadań.

- Pozycja komunikacji podaje również domyślny profil użytkownika używany przez system w niektórych sytuacjach. Należy rozumieć, jaką rolę pełnią profile domyślne. Jeśli system zawiera profile domyślne, należy zadbać, aby były to profile z minimalnymi uprawnieniami. Rozdział 12, “Ochrona komunikacji APPC” zawiera więcej informacji na temat domyślnych profili użytkowników.

  Aby odnaleźć pozycje komunikacyjne podające nazwy profili użytkowników, można użyć komendy Drukowanie opisu podsystemu (Print Subsystem Description - PRTSBSDAUT).

Pozycje zadania prestartu

Pozycji zadań prestartu można użyć do przygotowania podsystemu do pewnych rodzajów zadań, tak aby zadania te szybciej się uruchamiały. Zadania prestartu mogą być uruchamiane podczas uruchamiania podsystemu lub wtedy gdy są potrzebne. Pozycja zadania prestartu określa:

- program, który ma być uruchomiony,

  domyślny profil użytkownika,

  opis zadania.

Wszystkie wymienione elementy stanowią potencjalne zagrożenie dla ochrony. Należy sprawdzić, czy pozycje zadań prestartu wykonują tylko autoryzowane i zamierzone funkcje.

Zadania i opisy zadań

Opisy zadań zawierają dane żądania i dane routingu, które powodują uruchomienie konkretnego zadania, gdy używany jest dany opis zadania. Gdy opis zadania podaje program w parametrze dane żądania, system uruchamia ten program. Gdy opis zadania podaje dane routingu, system uruchamia program podany w pozycji routingu odpowiadający danym routingu.

System używa opisów zadań zarówno dla zadań interaktywnych, jak i wsadowych. W przypadku zadań interaktywnych pozycja stacji roboczej podaje opis zadania. Zazwyczaj pozycja stacji roboczej to *USRPRF, tak więc system używa opisu zadania podanego w profilu użytkownika. W przypadku zadań wsadowych opis podaje się podczas wprowadzania zadania.

Aby upewnić się, że nie uruchamiają one niewłaściwych programów, należy okresowo przeglądać opisy zadań. Należy również używać uprawnień do obiektów, aby uniemożliwić dokonywanie zmian w opisach zadań. Uprawnienie *USE jest wystarczające do uruchomienia zadania za pomocą opisu zadania. Zwykły użytkownik nie potrzebuje uprawnienia *CHANGE do opisów zadań.

Opcje menu SECBATCH:
15 *wprowadzenie natychmiastowe* **54** *użycie programu do planowania*

Opisy zadań mogą również określać, pod którym profilem użytkownika powinno być uruchamiane zadanie. Gdy poziom ochrony wynosi 40 lub więcej, należy użyć uprawnienia *USE do opisu zadania i do profilu użytkownika, który jest podany w opisie zadania. Gdy poziomy ochrony są niższe niż 40, uprawnienie *USE jest potrzebne tylko do opisu zadania.

Aby wydrukować listę opisów zadań podających profile użytkowników i mających uprawnienia publiczne *USE, można użyć komendy Drukowanie uprawnień dla JOBD (Print Job Description Authority - PRTJOBDAUT).

Raport zawiera uprawnienia specjalne dla profilu użytkownika, który jest określony w opisie zadania. Raport ten włącza uprawnienia specjalne wszystkich profili grupowych posiadanych przez profil użytkownika. Aby wyświetlić uprawnienia prywatne profilu użytkownika, można użyć następującej komendy:

```
DSPUSRPRF USRPRF(nazwa-profilu) TYPE(*OBJAUT)
```

Opis zadania określa listę bibliotek używanych przez zadanie, gdy jest ono uruchomione. Jeśli ktoś może zmienić listę bibliotek użytkownika, użytkownik może uruchomić niewłaściwą wersję programu w innej bibliotece. Należy okresowo przeglądać listy bibliotek podane w opisach zadań w systemie.

Należy również upewnić się, że wartości domyślne dla komend Wprowadzenie zadania (Submit Job - SBMJOB) i Tworzenie profilu użytkownika (Create User Profile - CRTUSRPRF) nie zostały zmienione tak, że wskazują na niewłaściwe opisy zadań.

Nazwy programu transakcyjnego architektury

Niektóre żądania komunikacyjne wysyłają do systemu specyficzny typ sygnału. Takie żądanie jest określane jako **nazwa programu transakcyjnego (TPN) architektury**, ponieważ nazwa programu transakcyjnego jest dla systemu częścią architektury APPC. Żądanie funkcji tranzytu terminalu jest przykładem nazwy TPN architektury. Nazwy TPN architektury są normalnym sposobem funkcjonowania komunikacji i nie stanowią zagrożenia dla ochrony. Jednak nazwy TPN architektury mogą umożliwić nieoczekiwane wejście do systemu.

Niektóre nazwy TPN nie przekazują profilu w żądaniu. Jeśli żądanie staje się powiązane z pozycją komunikacji, dla której domyślnym użytkownikiem jest *SYS, zadanie może zostać zainicjowane w systemie. Jednak profil *SYS może uruchamiać tylko funkcje systemowe, a nie aplikacje użytkownika.

Jeśli nazwy TPN architektury nie mają być uruchamiane z domyślnym profilem, można zmienić domyślnego użytkownika z *SYS na *NONE w pozycjach komunikacji. “Żądania nazw TPN architektury” na stronie 87 przedstawia nazwy TPN architektury i powiązane z nimi profile użytkowników.

Jeśli konkretna nazwa TPN ma nie być uruchamiana w systemie, należy:

1. Utworzyć program w języku CL akceptujący wiele parametrów. Program nie powinien wykonywać żadnego działania. Powinien on po prostu zawierać instrukcje Declare (DCL) dla parametrów i zakończyć działanie.
2. Dodać pozycję routingu dla danej nazwy TPN do każdego podsystemu mającego pozycje komunikacji i pozycje określające nazwy zdalnych miejsc. Pozycja routingu powinna określać:
   - Wartość *Wartość do porównania* (CMPVAL) taką samą, jak nazwa programu dla nazwy TPN (patrz Żądania nazw TPN architektury) z pozycją początkową 37.
   - Wartość *Program do wywołania* (PGM) taką samą, jak nazwa programu utworzonego w kroku 1. Uniemożliwia to nazwie TPN znalezienie innej pozycji routingu, takiej jak *ANY.

Niektóre nazwy TPN mają już własne pozycje routingu w podsystemie QCMN. Dodano je ze względu na wydajność.

Żądania nazw TPN architektury

Tabela 17. Programy i użytkownicy żądań nazw TPN

Żądanie TPN	Program	Profil użytkownika	Opis
X'30F0F8F1'	AMQCRC6A	*NONE	Kolejka komunikatów
X'06F3F0F1'	QACSOTP	QUSER	Program transakcji wpisania się APPC
X'30F0F2D1'	QANRTP	QADSM	Konfiguracja APPC ADSM/400
X'30F0F1F9'	QCNPCSUP	*NONE	Foldery współużytkowane
X'07F0F0F1'	QCNTEDDM	QUSER	DDM
X'07F6C4C2'	QCNTEDDM	QUSER	Zdalny SQL–DRDA1
X'30F0F7F7'	QCQNRBAS	QSVCCS	SNA CC_Server
X'30F0F1F4'	QDXPRCV	QUSER	Odbiornik DSNX–PC
X'30F0F1F3'	QDXPSEND	QUSER	Nadajnik DSNX–PC
X'30F0F2C4'	QEVYMAIN	QUSER	ENVY**/400 Server
X'30F0F6F0'	QHQTRGT	*NONE	Kolejka danych PC
X'30F0F8F0'	QLZPSERV	*NONE	Menedżer licencji Client Access
X'30F0F1F7'	QMFRCVR	*NONE	Odbiornik komunikatów PC
X'30F0F1F8'	QMFSNDR	*NONE	Nadajnik komunikatów PC
X'30F0F6F6'	QND5MAIN	QUSER	Kontroler stacji roboczej APPN 5394
DB2DRDA	QCNTEDDDM	QUSER	DB2DRDA
APINGD	QNMAPINGD	QUSER	APINGD
X'30F0F5F4'	QNMEVK	QUSER	Narzędzia zarządzania systemem
X'30F0F2C1'	QNPSERVR	*NONE	Sieciowy serwer wydruków PWS-I
X'30F0F7F9'	QOCEVOKE	*NONE	Kalendarz międzysystemowy
X'30F0F6F1'	QOKCSUP	QDOC	Tworzenie cienia katalogu
X'20F0F0F7'	QOQSESRV	QUSER	DIA wersja 2
X'20F0F0F8'	QOQSESRV	QUSER	DIA wersja 2
X'30F0F5F1'	QOQSESRV	QUSER	DIA wersja 2
X'20F0F0F0'	QOSAPPC	QUSER	DIA wersja 1
X'30F0F0F5'	QPAPAST2	QUSER	Tranzyt S/36—S/38
X'30F0F0F9'	QPAPAST2	QUSER	Tranzyt drukarki
X'30F0F4F6'	QPWFSTP0	*NONE	Foldery współużytkowane typ 2
X'30F0F2C8'	QPWFSTP1	*NONE	Serwer plików Client Access
X'30F0F2C9'	QPWFSTP2	*NONE	Serwer plików Windows** Client Access
X'30F0F6F9'	QRQSRVX	*NONE	Zdalny SQL–converged server
X'30F0F6F5'	QRQSRV0	*NONE	Zdalny SQL bez zatwierdzania
X'30F0F6F4'	QRQSRV1	*NONE	Zdalny SQL bez zatwierdzania
X'30F0F2D2'	QSVRCI	QUSER	SOC/CT
X'21F0F0F8'	QS2RCVR	QGATE	Odbiornik SNADS FS2
X'21F0F0F7'	QS2STSND	QGATE	Nadajnik SNADS FS2
X'30F0F1F6'	QTFDWNLD	*NONE	Funkcja przesyłania plików PC
X'30F0F2F4'	QTIHNPCS	QUSER	Funkcja TIE

Tabela 17. Programy i użytkownicy żądań nazw TPN (kontynuacja)

Żądanie TPN	Program	Profil użytkownika	Opis
X'30F0F1F5'	QVPPRINT	*NONE	Wirtualne drukowanie PC
X'30F0F2D3'	QWGMTP	QWGM	Ultimedia Mail/400 Server
X'30F0F8F3'	QZDAINIT	QUSER	Serwer dostępu do danych PWS-I
X'21F0F0F2'	QZDRCVR	QSNADS	Odbiornik SNADS
X'21F0F0F1'	QZDSTSND	QSNADS	Nadajnik SNADS
X'30F0F2C5'	QZHQTRG	*NONE	Serwer kolejek danych PWS-I
X'30F0F2C6'	QZRCSRVR	*NONE	Serwer komend zdalnych PWS-I
X'30F0F2C7'	QZSCSRVR	*NONE	Serwer centralny PWS-I

Metody monitorowania zdarzeń dotyczących ochrony

Konfigurowanie ochrony nie jest zadaniem, które można wykonać jednorazowo. Należy stale obserwować zmiany w systemie i awarie ochrony. Następnie należy poprawić środowisko ochrony z uwzględnieniem zdobytych informacji.

Raporty o ochronie pomagają monitorować zmiany dotyczące ochrony występujące w systemie. Poniżej podano inne funkcje systemowe, których można użyć do wykrycia awarii lub zagrożenia dla ochrony:

- Kontrola ochrony jest silnym narzędziem, którego można użyć do obserwowania wielu różnych zdarzeń dotyczących ochrony, które występują w systemie. Na przykład można skonfigurować system tak, aby powstawał zapis kontroli za każdym razem, gdy użytkownik otwiera do aktualizacji konkretny zbiór bazy danych. Można kontrolować wszystkie zmiany w wartościach systemowych. Można kontrolować czynności wykonywane w czasie, gdy użytkownicy odtwarzają obiekty.

  Rozdział 9 w książce *iSeries Ochrona* zawiera wyczerpujące informacje o funkcji kontroli ochrony. Aby skonfigurować kontrolę ochrony w systemie, można użyć komendy Zmiana kontroli ochrony (Change Security Auditing - CHGSECAUD). Można również użyć komendy Wyświetlenie pozycji kroniki kontroli (Display Audit Journal Entries - DSPAUDJRNE) do wydrukowania wybranych informacji z kroniki kontroli ochrony.
- Utworzenie kolejki komunikatów QSYSMSG umożliwia przechwytywanie newralgicznych komunikatów operatora systemu. Kolejka komunikatów QSYSOPR podczas zwykłego dnia pracy otrzymuje wiele komunikatów o różnych stopniach ważności. Newralgiczne komunikaty dotyczące ochrony mogą zostać niezauważone z powodu wielkiej liczby komunikatów w kolejce QSYSOPR.

  Jeśli w systemie utworzy się kolejkę komunikatów QSYSMSG w bibliotece QSYS, system automatycznie skieruje pewne newralgiczne komunikaty do kolejki komunikatów QSYSMSG zamiast do kolejki QSYSOPR.

  Można albo utworzyć program monitorujący kolejkę komunikatów QSYSMSG, albo przypisać ją sobie w trybie przerwania lub innemu zaufanemu użytkownikowi.

Część 3. Aplikacje i komunikacja sieciowa

Rozdział 11. Używanie Zintegrowanego systemu plików do ochrony plików

Zintegrowany system plików udostępnia wiele sposób przechowywania i przeglądania informacji w serwerze iSeries. Stanowi on część systemu operacyjnego OS/400, która obsługuje strumieniowe operacje wejścia i wyjścia. Wykorzystuje on metody zarządzania pamięcią masową podobne i zgodne ze stosowanymi w systemach operacyjnych komputerów PC i systemach operacyjnych UNIX.

W zintegrowanym systemie plików na wszystkie obiekty w systemie można spojrzeć z perspektywy hierarchicznej struktury katalogów. W większości przypadków jednak, użytkownicy oglądają obiekty w sposób, który jest napopularniejszy dla danego systemu plików. Na przykład ″tradycyjne″ obiekty iSeries znajdują się w systemie plików QSYS.LIB. Zazwyczaj użytkownicy oglądają je z perpektywy bubliotek. Obiekty znajdujące się w systemie plików QDLS oglądają natomiast z perspektywy dokumentów w folderach. Systemy plików root (/), QOpenSys oraz systemy plików zdefiniowane przez użytkowników mają strukturę hierarchicznych (zagnieżdżonych) katalogów.

Administrator ochrony musi:

- wiedzieć, które systemy plików są używane w systemie,
- znać unikalną charakterystykę ochrony każdego systemu plików.

Poniższe sekcje zawierają ogólne rozważania dotyczące ochrony zintegrowanego systemu plików.

Podejście do ochrony w Zintegrowanym systemie plików

Główny system plików (root) funkcjonuje jako podstawa dla wszystkich pozostałych systemów plików serwerów iSeries. Na najwyższym poziomie udostępnia on zintegrowany podgląd wszystkich obiektów znajdujących się w systemie. Pozostałe systemy plików istniejące w serwerze iSeries, w zależności od swojego przeznaczenia, w różny sposób obsługują zarządzanie obiektami i ich integrację. Na przykład system plików QOPT (optyczny) umożliwia aplikacjom i serwerom iSeries (w tym serwerowi plików iSeries Access for Windows) dostęp do napędu CD-ROM w serwerze iSeries. Podobnie, system plików QFileSvr.400 umożliwia aplikacjom dostęp do danych zintegrowanego systemu plików, znajdujących się w zdalnych serwerach iSeries. Serwer plików QLANSrv umożliwia dostęp do plików przechowywanych na serwerach Integrated xSeries Server for iSeries lub innych serwerach w sieci.

Podejście do ochrony w przypadku każdego systemu plików zależy od danych, które system plików udostępnia. Na przykład system plików QOPT nie zapewnia ochrony na poziomie obiektu, ponieważ nie istnieje technologia zapisywania informacji o uprawnieniach na dysku CD-ROM. W przypadku systemu plików QFileSvr.400 kontrola dostępu ma miejsce na zdalnym systemie (czyli tam, gdzie pliki są fizycznie przechowywane i zarządzane). W przypadku systemów plików takich, jak QLANSrv, kontrolę dostępu zapewnia Integrated xSeries Server for iSeries. Pomimo różnych modeli ochrony wiele systemów plików obsługuje spójne zarządzanie kontrolą dostępu za pomocą komend zintegrowanego systemu plików, takich jak Zmiana uprawnień (Change Authority - CHGAUT) i Zmiana właściciela (Change Owner - CHGOWN).

Poniżej podano wskazówki dotyczące ochrony zintegrowanego systemu plików. Zintegrowany system plików został zaprojektowany w taki sposób, aby był najbardziej zbliżony do standardów POSIX. Prowadzi to do interesujących sytuacji, gdy połączone zostają uprawnienia serwera iSeries i POSIX:

1. Nie należy usuwać uprawnienia prywatnego danego użytkownika do katalogu, którego jest on właścicielem. Dotyczy to również sytuacji, gdy jest on uprawniony przez uprawnienia publiczne, grupowe lub listę autoryzacji. W przypadku bibliotek lub folderów w standardowym modelu ochrony serwera iSeries usunięcie uprawnienia prywatnego właściciela spowoduje zmniejszenie objętości danych dotyczących uprawnień, przechowywanych w profilu użytkownika, lecz nie wpływa na żadne operacje. Jednak ze względu na sposób, w jaki standard POSIX definiuje dziedziczenie uprawnień do katalogów, właściciel nowo utworzonego katalogu będzie miał te same uprawnienia do tego katalogu, co właściciel katalogu nadrzędnego w stosunku do katalogu nadrzędnego, nawet jeśli właściciel nowo utworzonego katalogu ma inne uprawnienia prywatne do katalogu nadrzędnego. Ponieważ jest to nieco skomplikowane, podajemy przykład: UŻYTKOWNIK_A jest właścicielem katalogu /KATALOG_A, ale uprawnienia prywatne użytkownika UŻYTKOWNIK_A zostały usunięte. UŻYTKOWNIK_B ma uprawnienie prywatne do katalogu /KATALOG_A. UŻYTKOWNIK_B tworzy katalog /KATALOG_A/KATALOG_B. Ponieważ UŻYTKOWNIK_A nie ma uprawnienia do obiektu w stosunku do katalogu /KATALOG_A, UŻYTKOWNIK_B nie będzie miał uprawnień do obiektu /KATALOG_A/KATALOG_B. UŻYTKOWNIK_B nie będzie mógł zmienić nazwy lub usunąć katalogu /KATALOG_A/KATALOG_B bez uprzedniej zmiany uprawnień do obiektu użytkownika UŻYTKOWNIK_B. Sytuacja taka ma również miejsce podczas tworzenia plików za pomocą funkcji API open() z flagą O_INHERITMODE. Jeśli użytkownik UŻYTKOWNIK_B utworzy plik /KATALOG_A/PLIK_B, UŻYTKOWNIK_B nie będzie mieć uprawnień do obiektu ANI uprawnień do danych w tym pliku. UŻYTKOWNIK_B nie będzie mógł zapisywać do nowego pliku.
2. Uprawnienie adoptowane nie jest honorowane przez większość systemów plików fizycznych. Dotyczy to systemów plików root (/), QOpenSys, QDLS i systemów plików użytkownika.
3. Profil użytkownika, który utworzył obiekty, nie jest właścicielem obiektów, nawet jeśli pole OWNER profilu użytkownika jest ustawione na *GRPPRF.
4. Wiele operacji w systemie plików wymaga uprawnienia do danych *RX do każdego komponentu w ścieżce, włącznie z katalogiem (/). Jeśli występują problemy z uprawnieniami, należy sprawdzić uprawnienie użytkownika do katalogu root.
5. Wyświetlenie i wczytanie bieżącego katalogu roboczego (DSPCURDIR, getcwd() itp.) wymaga uprawnienia do danych *RX do każdego komponentu znajdującego się w ścieżce. Zmiana bieżącego katalogu roboczego (CD, chdir() itp.) wymaga tylko uprawnienia do danych *X w stosunku do każdego komponentu. Użytkownik może zatem zmienić bieżący katalog roboczy na określoną ścieżkę i nie być w stanie wyświetlić tej ścieżki.
6. Komenda COPY służy do powielania obiektu. Ustawienia uprawnień w nowym pliku będą takie same, jak oryginalne - z wyjątkiem właściciela. Komenda CPYTOSTMF służy natomiast do powielania danych. Użytkownik nie może sterować ustawieniami uprawnień w nowym pliku. Twórca/właściciel będą mieli uprawnienie do danych *RWX, ale uprawnienia grupowe i publiczne będą ustawione na *EXCLUDE. Aby przypisać określone uprawnienia, użytkownik musi użyć innych narzędzi (CHGAUT, chmod() itp.).
7. Aby pobrać informacje o uprawnieniach do obiektu, użytkownik musi być właścicielem obiektu lub mieć uprawnienie do obiektu *OBJMGT. Sytuacja ta występuje na przykład podczas używania komendy COPY, która musi pobrać informacje o uprawnieniach w obiekcie źródłowym, aby ustawić takie same uprawnienia w obiekcie docelowym.
8. Podczas zmiany właściciela lub grupy obiektu użytkownik musi nie tylko mieć odpowiednie uprawnienia do obiektu, ale musi również mieć uprawnienie do danych

*ADD do nowego profilu użytkownika właściciela lub grupy i uprawnienie do danych *DELETE do starego profilu właściciela lub grupy. Uprawnienia te nie są powiązane z uprawnieniami do danych systemu plików. Mogą być one wyświetlone za pomocą komendy DSPOBJAUT i zmienione za pomocą komendy EDTOBJAUT. Taka sytuacja występuje na przykład podczas używania komendy COPY, gdy próbuje ona ustawić identyfikator grupy dla nowego obiektu.

9. Użycie komendy MOV często wiąże się z pojawianiem się błędów związanych z uprawnieniami, szczególnie podczas przenoszenia danych pomiędzy różnymi fizycznymi systemami plików i podczas wykonywania konwersji danych. W takich sytuacjach przenoszenie w rzeczywistości jest operacją kopiowania, a następnie usuwania. Zatem wszystkie rozważania dotyczące uprawnień dla komendy COPY (punkty 7 i 8 powyżej) i komendy RMVLNK dotyczą również komendy MOV, oprócz rozważań charakterystycznych dla tej właśnie komendy.

Poniższe sekcje zawierają rozważania dotyczące kilku reprezentatywnych systemów plików. Więcej informacji na temat konkretnego systemu plików iSeries zawiera dokumentacja programu licencjonowanego używającego tego systemu plików.

System plików Root (/), QOpenSys i system plików użytkownika

Ta sekcja zawiera rozważania dotyczące ochrony systemów plików root, QOpenSys i systemów plików użytkownika.

Jak działają uprawnienia

Główny system plików (root), QOpenSys i systemy plików użytkownika udostępniają możliwości serwera iSeries, systemów operacyjnych PC i systemu UNIX**, zarówno pod względem zarządzania obiektami, jak i ich ochrony. Jeśli w sesji serwera iSeries używa się komend zintegrowanego systemu plików (WRKAUT i CHGAUT), można ustawić wszystkie zwykłe uprawnienia do obiektu iSeries. Są to uprawnienia *R, *W oraz *X, zgodne ze specyfikacją Spec 1170 (systemy operacyjne typu UNIX).

Uwaga: Systemy plików root, QOpenSys i systemy plików użytkownika pod względem funkcjonalnym są sobie równe. W systemie plików QOpenSys rozróżniane są wielkości liter. W systemie plików root wielkości liter nie są rozróżniane. System plików użytkownika można definiować z rozróżnianiem wielkości liter. Ponieważ omawiane systemy plików mają takie same charakterystyki ochrony, w poniższym tekście ich nazwy są używane zamiennie.

Gdy administrator uzyskuje dostęp do systemu plików root poprzez sesję PC, może ona ustawiać atrybuty obiektów używanych przez komputer PC do ograniczania dostępu. Są to następujące atrybuty:

- systemowy,
- ukryty,
- archiwalny,
- tylko do odczytu.

Podane atrybuty PC stanowią uzupełnienie wartości uprawnień do obiektów w serwerze iSeries, ale ich nie zastępują.

Gdy użytkownik próbuje uzyskać dostęp do obiektu w systemie plików root, system OS/400 sprawdza wartości uprawnień do obiektów i atrybuty dla tego obiektu, bez względu na to, czy są one ″widoczne″ poprzez interfejs użytkownika. Na przykład przyjmijmy, że jest włączony atrybut tylko do odczytu. Użytkownik PC nie może usunąć obiektu, używając interfejsu iSeries Access. Użytkownik serwera iSeries korzystający ze stacjonarnej stacji roboczej również nie może usunąć tego obiektu, nawet jeśli ma uprawnienia specjalne *ALLOBJ. Aby obiekt mógł zostać usunięty, uprawniony użytkownik musi na komputerze PC wyłączyć

atrybut tylko do odczytu. Użytkownik PC może nie mieć wystarczających uprawnień w systemie OS/400, aby zmienić stosowane na komputerze PC atrybuty ochrony obiektu.

Aplikacje typu UNIX, działające w serwerze iSeries, używają UNIX-owych interfejsów API w celu uzyskania dostępu do systemu plików root. Aplikacje używające UNIX-owych interfejsów API mogą rozpoznać i obsługiwać następujące informacje o ochronie:
- właściciel obiektu,
- właściciel grupy (uprawnienie grupy podstawowej serwera iSeries),
- odczyt (pliki),
- zapis (zmiana zawartości),
- wykonanie (uruchamianie programów i przeszukiwanie katalogów).

System odwzorowuje te uprawnienia do danych na istniejące uprawnienia do obiektów i danych iSeries:
- Read (*R) = *OBJOPR i *READ,
- Write (*W) = *OBJOPR, *ADD, *UPD, *DLT,
- Execute (*X) = *OBJOPR i *EXECUTE.

Koncepcja innych uprawnień do obiektu (*OBJMGT, *OBJEXIST, *OBJALTER i *OBJREF) nie istnieje w środowisku typu UNIX.

Mimo to podane uprawnienia do obiektu istnieją dla wszystkich obiektów w systemie plików root. Podczas tworzenia obiektu przy użyciu UNIX-owego interfejsu API obiekt dziedziczy te uprawnienia od katalogu nadrzędnego. Dlatego:
- właściciel nowego obiektu ma takie same uprawnienie do obiektu jak właściciel katalogu nadrzędnego,
- grupa podstawowa nowego obiektu ma takie same uprawnienie do obiektu jak grupa podstawowa katalogu nadrzędnego,
- uprawnienia publiczne do nowego obiektu są takie same jak uprawnienia publiczne do katalogu nadrzędnego.

Uprawnienie do danych właściciela, grupy podstawowej i uprawnienia publiczne do nowego obiektu są określane w interfejsie API za pomocą parametru trybu (mode). Gdy wszystkie uprawnienia do obiektu są włączone (on), zakres działań powiązanych z uprawnieniami jest taki, jakiego można się spodziewać w środowisku typu UNIX. Najlepiej nie zmieniać tych uprawnień pozostawiając je włączone (on), o ile nie chce się zakresu działań typu POSIX.

Gdy uruchamia się aplikacje używające UNIX-owych interfejsów API, system sprawdza wszystkie uprawnienia obiektu, bez względu na to, czy są one ″widoczne″ dla UNIX-owych aplikacji. Na przykład system sprawdzi uprawnienia list autoryzacji, mimo że koncepcja list autoryzacji nie istnieje w UNIX-owych systemach operacyjnych.

Gdy używa się środowiska z aplikacjami z różnych systemów, nie należy dokonywać zmian w uprawnieniach w jednym środowisku, bo może to spowodować nieprawidłowe działanie tej aplikacji w innym środowisku.

Praca z ochroną w systemach plików root (/), QOpenSys i systemach plików użytkownika

Wraz z wprowadzeniem zintegrowanego systemu plików, serwera iSeries również udostępnił nowy zestaw komend służących do pracy z obiektami w wielu systemach plików. Zestaw ten zawiera komendy dotyczące ochrony:
- Zmiana wartości kontroli (Change Auditing - CHGAUD)
- Zmiana uprawnień (Change Authority - CHGAUT)
- Zmiana właściciela (Change Owner - CHGOWN)
- Zmiana grupy podstawowej (Change Primary Group - CHGPGP)
- Wyświetlenie uprawnień (Display Authority - DSPAUT)

- Praca z uprawnieniami (Work with Authority - WRKAUT)

Te komendy grupują podstawowe uprawnienia do danych i obiektów w UNIX-owe podzbiory uprawnień:
***RWX** Read/write/execute
***RW** Read/write
***R** Read
***WX** Write/execute
***W** Write
***X** Execute

Ponadto do pracy z ochroną można wykorzystać UNIX-owe interfejsy API.

Uprawnienia publiczne do katalogu głównego (root)

W dostarczanym systemie uprawnienia publiczne do katalogu głównego (root) to *ALL (wszystkie uprawnienia do obiektów i wszystkie uprawnienia do danych). Ustawienie to zapewnia elastyczność i jest zgodne z oczekiwaniami aplikacji UNIX-owych i typowych użytkowników serwera iSeries. Użytkownik serwera iSeries, który ma dostęp do wiersza komend, może utworzyć nową bibliotekę w systemie plików QSYS.LIB, używając komendy CRTLIB. Uprawnienie w typowym serwerze iSeries umożliwia wykonanie tego zadania. Podobna sytuacja ma miejsce w przypadku dostarczonego systemu głównego plików (root). Typowy użytkownik może utworzyć nowy katalog w systemie plików root (tak jak użytkownik komputera PC może utworzyć nowy katalog na komputerze PC).

Administrator ochrony musi poinstruować podlegających mu użytkowników o odpowiednim zabezpieczeniu tworzonych przez nich obiektów. Gdy użytkownik tworzy bibliotekę, uprawnienia publiczne do niej nie powinny mieć wartości *CHANGE (wartość domyślna). Użytkownik ten powinien zmienić ustawienie publiczne albo na *USE, albo na *EXCLUDE - w zależności od zawartości biblioteki.

Jeśli użytkownicy tworzą nowe katalogi w systemie plików root (/), QOpenSys lub systemie plików użytkownika, administrator ochrony ma do dyspozycji kilka opcji ochrony.

- Może on nauczyć użytkowników zmieniania uprawnień domyślnych, gdy tworzą nowe katalogi. Domyślnie uprawnienia są dziedziczone od bezpośredniego katalogu nadrzędnego. W przypadku utworzenia nowego katalogu w katalogu root domyślnie uprawnieniem publicznym będzie *ALL.
- Administrator może utworzyć podkatalog ″główny″ w katalogu root, a następnie ustawić uprawnienie publiczne dla tego katalogu, odpowiednie dla danej organizacji. Kolejnym krokiem jest poinstruowanie użytkowników, aby nowe katalogi osobiste tworzyli w podkatalogu głównym. Tworzone przez nich katalogi będą dziedziczyły uprawnienia podkatalogu głównego.
- Można rozważyć zmianę uprawnienia publicznego dla katalogu root, aby uniemożliwić użytkownikom tworzenie obiektów w tym katalogu. (Należy usunąć uprawnienia *W, *OBJEXIST, *OBJALTER, *OBJREF i *OBJMGT). Należy jednak przemyśleć, czy ta zmiana nie spowoduje problemów w przypadku innych aplikacji. Mogą na przykład istnieć UNIX-owe aplikacje, które zakładają, że mają możliwość usuwania obiektów z katalogu root.

Komenda Drukowanie uprawnień prywatnych (PRTPVTAUT)

Komenda Drukowanie uprawnień prywatnych (Print Private Authorities - PRTPVTAUT) umożliwia wydrukowanie raportu o wszystkich uprawnieniach prywatnych dla obiektów określonego typu i w określonej bibliotece, folderze lub katalogu. Raport zawiera wszystkie obiekty podanego typu i użytkowników, którzy mają uprawnienia do tych obiektów. Jest to metoda sprawdzenia różnych źródeł uprawnień do obiektów.

Ta komenda drukuje trzy raporty dla wybranych obiektów. Pierwszy raport (Pełny raport - Full Report) zawiera wszystkie uprawnienia prywatne dla wszystkich wybranych obiektów. Drugi raport (Raport zmian - Changed Report) zawiera dodatki i zmiany wykonane na uprawnieniach prywatnych do wybranych obiektów od poprzedniego uruchomienia komendy PRTPVTAUT dla podanych obiektów w podanej bibliotece, folderze lub katalogu. Raport ten zawiera wszystkie nowe obiekty podanego typu, nowe uprawnienia do istniejących obiektów i zmiany uprawnień do istniejących obiektów. Jeśli komenda PRTPVTAUT nie została uprzednio uruchomiona dla podanych obiektów w podanej bibliotece, folderze lub katalogu, to Raport zmian nie zostanie utworzony. Jeśli komenda została uprzednio uruchomiona, ale nie wykonano żadnych zmian w uprawnieniach do obiektów, to Raport zmian jest drukowany, ale nie zawiera żadnych obiektów.

Trzeci raport (Raport usunięć - Deleted Report) zawiera wszystkich użytkowników z uprawnieniami prywatnymi usuniętymi z podanych obiektów od czasu ostatniego uruchomienia komendy PRTPVTAUT. Raport ten zawiera wszystkie usunięte obiekty oraz usuniętych użytkowników u uprawnieniami prywatnymi. Jeśli komenda PRTPVTAUT nie została uprzednio uruchomiona, Raport usunięć nie zostanie utworzony. Jeśli komenda została uprzednio uruchomiona, ale nie usunięto żadnych obiektów, to Raport usunięć jest drukowany, ale nie zawiera żadnych obiektów.

Ograniczenie: aby używać tej komendy, należy mieć uprawnienie *ALLOBJ.

Przykłady:

Poniższa komenda tworzy następujące raporty: pełny, zmian i usunięć dla wszystkich obiektów zbiorów w bibliotece PAYROLLLIB:

```
PRTPVTAUT OBJTYPE(*FILE) LIB(PAYROLLLIB)
```

Poniższa komenda tworzy następujące raporty: pełny, zmian i usunięć dla wszystkich obiektów plików strumieniowych w katalogu garry:

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*NO)
```

Poniższa komenda tworzy następujące raporty: pełny, zmian i usunięć dla wszystkich obiektów plików strumieniowych w strukturze podkatalogów rozpoczynającej się w katalogu garry:

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*YES)
```

Komenda Drukowanie obiektów z uprawnieniami publicznymi (PRTPUBAUT)

Komenda Drukowanie obiektów z uprawnieniami publicznymi (Print Publicly Authorized Objects - PRTPUBAUT) umożliwia wydrukowanie raportu o określonych obiektach, które nie mają uprawnienia publicznego *EXCLUDE. W przypadku obiektów *PGM w raporcie znajdą się tylko programy, które nie mają uprawnienia publicznego *EXCLUDE, które użytkownik może wywołać (program jest albo domeną użytkownika, albo poziom ochrony systemu ,wartość systemowa QSECURITY, wynosi 30 lub mniej). Jest to metoda sprawdzenia, do których obiektów uprawnienia dostępu mają wszyscy użytkownicy.

Omawiana komenda drukuje dwa raporty. Pierwszy raport (Pełny raport - Full Report) zawiera wszystkie podane obiekty, które nie mają uprawnienia publicznego *EXCLUDE. Drugi raport (Raport zmian - Changed Report) zawiera obiekty, które nie mają uprawnienia publicznego *EXCLUDE, a które miały to uprawnienie publiczne lub które nie istniały, gdy komenda PRTPUBAUT była ostatnio uruchamiana. Jeśli komenda PRTPUBAUT nie została uprzednio uruchomiona dla podanych obiektów w bibliotece, folderze lub katalogu, to Raport

zmian nie zostanie utworzony. Jeśli komenda została uprzednio uruchomiona, ale żadne dodatkowe obiekty nie mają uprawnienia publicznego *EXCLUDE, to Raport zmian jest drukowany, ale nie zawiera żadnych obiektów.

Ograniczenie: aby używać tej komendy, należy mieć uprawnienie specjalne *ALLOBJ.

Przykłady:

Poniższa komenda tworzy raporty pełny i zmian dla wszystkich obiektów zbiorów w bibliotece GARRY, które nie mają uprawnienia publicznego *EXCLUDE:

```
PRTPUBAUT OBJTYPE(*FILE) LIB(GARRY)
```

Poniższa komenda tworzy raporty pełny i zmian dla wszystkich obiektów plików strumieniowych w strukturze podkatalogów rozpoczynającej się w katalogu garry, które nie mają uprawnienia publicznego *EXCLUDE:

```
PRTPUBAUT OBJTYPE(*STMF) DIR(GARRY) SCHSUBDIR(*YES)
```

Ograniczanie dostępu do systemu plików QSYS.LIB

Ponieważ nadrzędnym systemem plików jest root, system plików QSYS.LIB jest widoczny w katalogu root jako podkatalog. Dlatego użytkownik PC z dostępem do serwera iSeries może manipulować obiektami przechowywanymi w bibliotekach iSeries (system plików QSYS.LIB) za pomocą zwykłych komend i operacji wykonywanych na komputerze PC. Użytkownik PC może więc przeciągnąć obiekt QSYS.LIB (na przykład bibliotekę ze zbiorami danych zawierającymi newralgiczne dane) do pojemnika z niepotrzebnymi obiektami.

Zgodnie z tym, co opisuje sekcja “System plików Root (/), QOpenSys i system plików użytkownika” na stronie 93, system wymaga uprawnienia do wszystkich obiektów, bez względu na to, czy są one widoczne. Tak więc użytkownik nie może usunąć obiektu, chyba że ma do niego uprawnienie *OBJEXIST. Jeśli jednak system iSeries jest chroniony poprzez kontrolę dostępu do menu, a nie poprzez ochronę obiektów, użytkownik PC może równie dobrze znaleźć w systemie plików QSYS.LIB obiekty, które można usunąć.

Wraz z rozszerzaniem się wykorzystania systemu i stosowaniem różnych metod dostępu, okazuje się, że ochrona poprzez kontrolę dostępu do menu nie jest wystarczająca. Rozdział 5, “Zabezpieczenie ważnych informacji poprzez uprawnienia do obiektu”, na stronie 45, zawiera omówienie strategii uzupełnienia ochrony poprzez kontrolę dostępu do menu o ochronę obiektów. Z drugiej strony jednak, serwer iSeries udostępnia prosty sposób blokowania dostępu do systemu plików QSYS.LIB przez strukturę katalogową systemu plików root. Do określania, którzy użytkownicy mają dostęp do systemu plików QSYS.LIB poprzez katalog root, można używać listy autoryzacji QPWFSERVER.

Gdy użytkownik ma uprawnienie *EXCLUDE do listy autoryzacji QPWFSERVER, to nie ma on dostępu do katalogu QSYS.LIB ze struktury katalogów root. Jeśli użytkownik ma uprawnienie *USE, ma dostęp do tego katalogu. Gdy użytkownik ma już uprawnienia dostępu do tego katalogu, może wykonywać na obiekcie w systemie plików QSYS.LIB te operacje, do których ma uprawnienia. Innymi słowy, uprawnienie do listy autoryzacji QPWFSERVER działa jak drzwi umożliwiające dostęp do całego systemu plików QSYS.LIB. W przypadku użytkownika z uprawnieniem *EXCLUDE drzwi są zamknięte. W przypadku użytkownika z uprawnieniem *USE (lub szerszym) drzwi są otwarte.

W większości sytuacji użytkownicy nie muszą używać interfejsu katalogów do uzyskania dostępu do systemu plików QSYS.LIB. Można rozważyć ustawienie uprawnienia publicznego do listy autoryzacji QPWFSERVER na *EXCLUDE. Należy pamiętać, że uprawnienie do listy autoryzacji otwiera i zamyka drzwi do wszystkich bibliotek w systemie plików

QSYS.LIB, łącznie z bibliotekami użytkowników. Jeśli niektórzy użytkownicy sprzeciwiają się takiemu ustawieniu uprawnienia, można indywidualnie rozważyć ich wymagania. Jeśli jest to potrzebne, można jawnie nadawać każdemu użytkownikowi uprawnienia do listy autoryzacji. Należy wtedy jednak sprawdzić, czy ma on odpowiednie uprawnienia do obiektów w systemie plików QSYS.LIB. Jeśli się tego nie zrobi, to może on niechcący usunąć obiekty lub nawet całe biblioteki.

Uwagi:

1. W dostarczanym systemie uprawnienia publiczne do listy autoryzacji QPWFSERVER są ustawione na *USE.
2. Jeśli jawnie nadaje się uprawnienia każdemu użytkownikowi, lista autoryzacji określa prawa dostępu tylko przy udostępnianiu plików przez iSeries Access, NetServer i przy udostępnianiu plików między serwerami iSeries. Nie blokuje to dostępu do tych katalogów przez FTP, ODBC i z innych sieci.

Bezpieczne katalogi

Aby uzyskać dostęp do obiektu znajdującego się w systemie plików root, odczytuje się całą ścieżkę do tego obiektu. Aby przeszukać katalog, należy mieć do niego uprawnienie *X (*OBJOPR i *EXECUTE). Przyjmijmy na przykład, że chcemy uzyskać dostęp do następującego obiektu:

```
/firma/klienci/klient.dat
```

W takim przypadku trzeba mieć uprawnienie *X do katalogów firma i klienci.

W systemie plików root można tworzyć dowiązanie symboliczne do obiektu. Pojęciowo dowiązanie symboliczne jest aliasem nazwy ścieżki. Zazwyczaj jest ono krótsze i łatwiejsze do zapamiętania niż pełna nazwa ścieżki. Dowiązanie symboliczne nie tworzy jednak innej ścieżki fizycznej do obiektu. Użytkownik nadal potrzebuje uprawnienia *X do każdego katalogu i podkatalogu w ścieżce fizycznej obiektu.

W przypadku obiektów w systemie plików root można używać ochrony katalogów tak samo, jakby używało się ochrony bibliotek w systemie plików QSYS.LIB. Na przykład można ustawić uprawnienie publiczne do katalogu na *EXCLUDE, aby zabezpieczyć obiekty w strukturze katalogów przed dostępem użytkowników o uprawnieniach publicznych.

Ochrona nowych obiektów

Gdy tworzony jest nowy obiekt w systemie plików root, o jego uprawnieniach decyduje interfejs użyty do jego utworzenia. Na przykład jeśli użyto komendy CRTDIR wraz z wartościami domyślnymi, nowy katalog dziedziczy wszystkie charakterystyki katalogu nadrzędnego, w tym uprawnienia prywatne, uprawnienie grupy podstawowej i powiązanie z listą autoryzacji. Poniższe sekcje opisują sposób określania uprawnień dla każdego typu interfejsu.

Uprawnienie pochodzi z katalogu bezpośrednio nadrzędnego, a nie z katalogów znajdujących się wyżej w strukturze katalogów. Tak więc administrator ochrony musi spojrzeć z dwóch perspektyw na uprawnienia, które nadaje do katalogów w strukturze:

- jak uprawnienie wpływa na dostęp do obiektów w strukturze (na przykład uprawnienie do bibliotek),
- jak uprawnienie wpływa na nowo utworzone obiekty (na przykład wartość CRTAUT dla bibliotek).

Zalecenie: Może być korzystne utworzenie katalogu osobistego dla użytkowników pracujących w zintegrowanym systemie plików (na przykład katalogu

/home/usrxxx), a następnie odpowiednie ustawienie ochrony (na przykład PUBLIC *EXCLUDE). Wszystkie katalogi tworzone przez użytkowników w strukturze katalogów home będą dziedziczyły uprawnienia.

Poniżej opisano dziedziczenie uprawnień dla różnych interfejsów.

Korzystanie z komendy Tworzenie katalogu

Podczas tworzenia nowego podkatalogu przy użyciu komendy CRTDIR można określić uprawnienia na dwa sposoby:

- określając uprawnienie publiczne (uprawnienie do danych, uprawnienie do obiektu lub oba),
- określając uprawnienie *INDIR jako uprawnienie do danych, uprawnienie do obiektu lub oba. Jeśli poda się *INDIR zarówno jako uprawnienie do danych, jak i uprawnienie do obiektu, system wiernie kopiuje wszystkie informacje o uprawnieniach z katalogu nadrzędnego do nowego obiektu, uprawnienia z listy autoryzacji, grupy podstawowej, uprawnienie publiczne i prywatne. (System nie kopiuje uprawnień prywatnych, które profile QSYS i QSECOFR mają do danego obiektu).

Tworzenie katalogu za pomocą funkcji API

Tworząc katalog za pomocą funkcji API mkdir() podaje się uprawnienie do danych dla właściciela, grupy podstawowej oraz publiczne (nadając uprawnienia *R, *W i *X). System używa podanych informacji z katalogu nadrzędnego do ustawienia uprawnienia do obiektu dla właściciela, grupy podstawowej i publiczne.

Ponieważ w systemach typu UNIX nie istnieje koncepcja uprawnień do obiektów, funkcja API mkdir() nie obsługuje podawania takich uprawnień. Jeśli potrzebne są różne uprawnienia do obiektów, można użyć komendy serwera iSeries CHGAUT. Jednak jeśli usunie się niektóre uprawnienia do obiektów, aplikacje typu UNIX mogą pracować niezgodnie z oczekiwaniami.

Tworzenie pliku strumieniowego za pomocą funkcji API open() lub creat()

Podczas tworzenia pliku strumieniowego przy użyciu funkcji API creat() można podać uprawnienie do danych dla właściciela, grupy podstawowej oraz publiczne (używając uprawnień UNIX-owych *R, *W i *X). System używa podanych informacji z katalogu nadrzędnego do ustawienia uprawnienia do obiektu dla właściciela, grupy podstawowej i publiczne.

Uprawnienia te można również podać podczas tworzenia pliku strumieniowego za pomocą funkcji API open(). Alternatywnie używając funkcji API open() można określić dziedziczenie przez obiekt wszystkich uprawnień z katalogu nadrzędnego. Jest to tak zwany tryb dziedziczenia. Jeśli poda się tryb dziedziczenia, system nadaje uprawnienia całkowicie zgodne z uprawnieniami katalogu nadrzędnego, w tym uprawnienia listy autoryzacji, grupy podstawowej, publiczne i prywatne. Ta opcja działa jak podanie *INDIR jako parametru komendy CRTDIR.

Tworzenie obiektu za pomocą interfejsu PC

Jeśli do utworzenia obiektu w systemie plików root używa się aplikacji PC, automatycznie dziedziczy on wszystkie uprawnienia z katalogu nadrzędnego. Dotyczy to listy autoryzacji, grupy podstawowej, uprawnień publicznych i prywatnych. Aplikacje PC nie mają odpowiednika określania uprawnień podczas tworzenia obiektu.

System plików QFileSvr.400

W systemie plików QFileSvr.400 użytkownik (USERX) w jednym systemie iSeries (SYSTEMA) może mieć dostęp do danych w innym połączonym systemie iSeries (SYSTEMB). Użytkownik USERX korzysta z interfejsu podobnego do interfejsu Client Access. Zdalny serwer iSeries (SYSTEMB) jest widoczny jako katalog z systemami plików jako podkatalogami.

Gdy USERX usiłuje uzyskać dostęp do systemu SYSTEMB za pomocą interfejsu, SYSTEMA wysyła nazwę profilu użytkownika i zaszyfrowane hasło użytkownika USERX do systemu SYSTEMB. Ten sam profil użytkownika i hasło muszą istnieć w systemie SYSTEMB. W przeciwnym przypadku SYSTEMB odrzuca zgłoszenie.

Jeśli SYSTEMB akceptuje zgłoszenie, USERX jest widoczny w systemie SYSTEMB jak każdy użytkownik Client Access. Te same reguły sprawdzania uprawnień mają zastosowanie do wszystkich działań podejmowanych przez użytkownika USERX.

Administrator ochrony musi wiedzieć, że system plików QFileSvr.400 umożliwia inne wejście do systemu. Administrator nie może przyjąć, że ogranicza dostęp zdalnych użytkowników poprzez interaktywne wpisanie się za pomocą tranzytu przez terminal. Jeśli w systemie działa podsystem QSERVER i system jest podłączony do innego systemu iSeries, zdalni użytkownicy mogą mieć dostęp do systemu, tak jakby pracowali na lokalnym komputerze PC z oprogramowaniem Client Access. Jest bardzo prawdopodobne, że w systemie będzie istnieć połączenie wymagające uruchomienia podsystemu QSERVER. Jest to jeszcze jeden powód, dla którego bardzo ważny jest dobrze zaplanowany schemat uprawnień do obiektów.

System plików NFS

System plików NFS umożliwia dostęp z i do systemów z zaimplementowanym systemem NFS. NFS jest metodą o standardzie przemysłowym, służącą do współużytkowania informacji między użytkownikami w systemach sieciowych. Większość najważniejszych systemów operacyjnych (w tym systemy operacyjne dla komputerów PC) obsługuje NFS. W systemach UNIX system plików NFS jest podstawową metodą dostępu do danych. Serwer iSeries może działać jako klient NFS i jako serwer NFS.

Administrator ochrony systemu iSeries działającego jako serwer NFS musi rozumieć i zarządzać elementami ochrony związanymi z systemem plików NFS. Poniżej podano kilka sugestii i uwag dotyczących NFS.

- Należy jawnie uruchomić serwer NFS używając komendy STRNFSSVR. Należy sprawdzić, kto ma uprawnienia do używania tej komendy.
- Katalogi i obiekty udostępnia się klientom NFS eksportując je. Tak więc można dokładnie określić, które części systemu udostępnia się klientom NFS w sieci.
- Podczas eksportu można podać, którzy klienci mają mieć dostęp do obiektów. Klienta identyfikuje się przez nazwę systemu lub adres IP. Klientem może być pojedynczy komputer PC, cały serwer iSeries lub system UNIX. W terminologii NFS, klient (adres IP) jest nazywany maszyną.
- Podczas eksportu można określić dostęp tylko do odczytu lub odczyt/zapis dla wszystkich maszyn, które mają dostęp do eksportowanego katalogu lub obiektu. W większości przypadków określa się dostęp tylko do odczytu.
- System plików NFS nie zapewnia ochrony przez hasła. Został on zaprojektowany do współużytkowania danych w obrębie zaufanej grupy systemów. Gdy użytkownik żąda dostępu, serwer odbiera identyfikator użytkownika. Poniżej podano kilka uwag dotyczących identyfikatorów użytkowników:

- Serwer iSeries próbuje znaleźć profil użytkownika z tym samym identyfikatorem użytkownika. Jeśli go znajdzie, używa uwierzytelnienia profilu użytkownika. Uwierzytelnienie jest terminem związanym z systemem plików NFS stosowanym do opisania używania uprawnienia użytkownika. Jest to podobne do wymiany profili w innych aplikacjach serwera iSeries.
- Podczas eksportowania katalogu lub obiektu można określić, czy zezwala się na dostęp przy użyciu profilu z uprawnieniami administratora. Serwer NFS w iSeries traktuje uprawnienie administratora tak samo jak uprawnienie specjalne *ALLOBJ. Jeśli określi się, że nie udostępnia się uprawnień administratora, użytkownik NFS z identyfikatorem użytkownika, który jest odpowiednikiem profilu użytkownika z uprawnieniem specjalnym *ALLOBJ, nie będzie miał dostępu do obiektu z tym profilem. Jeśli zezwolono na dostęp anonimowy, requester zostanie odwzorowany do profilu anonimowego.
- Podczas eksportowania katalogu lub obiektu można określić, czy zezwala się na żądania anonimowe. Żądanie anonimowe jest żądaniem z identyfikatorem użytkownika, który nie jest zgodny z żadnym identyfikatora użytkownika w systemie. Jeśli zezwoli się na żądania anonimowe, system odwzorowuje użytkownika anonimowego na profil użytkownika QNFSANON dostarczony przez IBM. Ten profil nie ma żadnych uprawnień specjalnych ani uprawnień jawnych. (Podczas eksportu można określić inny profil użytkownika dla żądań anonimowych.)

- Jeśli serwer iSeries znajduje się w sieci NFS (lub innej sieci z systemami UNIX zależnymi od identyfikatorów użytkowników), lepiej jest samemu zarządzać identyfikatorami użytkowników, a nie wykorzystywać identyfikatory automatycznie przypisywane przez system. Należy skoordynować identyfikatory użytkowników z innymi systemami w sieci.

  Może się okazać, że trzeba zmienić identyfikatory użytkowników (nawet w przypadku profili użytkowników IBM), aby zachować zgodność z innymi systemami w sieci. Dostępny jest program ułatwiający zmianę identyfikatorów użytkowników dla profili użytkowników. (Gdy zmienia się identyfikator użytkownika dla profilu użytkownika, należy również zmienić identyfikator użytkownika dla wszystkich obiektów, których właścicielem jest ten profil, zarówno w katalogu root, jak i katalogu QOpenSrv.) Program QSYCHGID automatycznie zmienia identyfikatory użytkowników zarówno w profilu użytkownika, jak i we wszystkich obiektach, których jest właścicielem. Informacje na temat sposobu używania tego programu zawiera książka *iSeries System API Reference*.

Rozdział 12. Ochrona komunikacji APPC

Jeśli system jest podłączony do sieci, w której znajdują się również inne systemy, pojawiają się nowe sposoby dostępu do niego. Administrator ochrony musi wiedzieć, jakie są możliwości kontroli dostępu do systemu w środowisku APPC.

Zaawansowana komunikacja program-program (APPC) jest używana przez komputery, w tym przez komputery osobiste, do wzajemnej komunikacji. Komunikacja APPC znajduje zastosowanie w funkcjach tranzytu terminalu, zarządzania danymi rozproszonymi oraz iSeries Access for Windows.

W poniższych sekcjach przedstawiono podstawowe informacje dotyczące sposobu działania komunikacji APPC i sposobu ustawienia odpowiedniej ochrony. W opisie skoncentrowano się przede wszystkim na zagadnieniach konfiguracji APPC związanych z ochroną. Aby dostosować podany opis do własnych potrzeb, należy nawiązać współpracę z ludźmi zarządzającymi siecią komunikacyjną i być może również z dostawcami aplikacji. Podane informacje powinny stanowić podstawę do zrozumienia zagadnień związanych z ochroną i opcji dostępnych dla komunikacji APPC.

Poprawa ochrony systemu zawsze wiąże się z pewnymi kosztami. Niektóre sugestie mające uprościć ochronę sieci mogą skomplikować administrowanie nią. Na przykład w tej książce nie kładzie się nacisku na sieć APPN (zaawansowana sieć typu każdy z każdym), ponieważ ochronę łatwiej zrozumieć i łatwiej nią zarządzać bez APPN. Jednak bez sieci APPN, administrator musi samodzielnie utworzyć dane konfiguracyjne, które w przypadku zastosowania tej sieci tworzą się automatycznie.

Komputery PC również używają komunikacji

Wiele metod połączenia komputerów PC z serwerami iSeries zależy od sposobów komunikacji, takich jak APPC i TCP/IP. Czytając poniższe sekcje należy rozważyć zagadnienia dotyczące ochrony obejmujące zarówno połączenie z innymi systemami, jak i z komputerami PC. Podczas planowania ochrony sieci należy pamiętać również o komputerach PC połączonych z systemem.

Terminologia dotycząca komunikacji APPC

Komunikacja APPC umożliwia użytkownikowi w systemie pracę z innym systemem. System, z którego pochodzi żądanie, jest określany jako:

- **system źródłowy,**
- **system lokalny,**
- **klient.**

System, który odbiera żądanie, jest określany jako:

- **system docelowy,**
- **system zdalny,**
- **serwer.**

Podstawowe elementy komunikacji APPC

Z perspektywy administratora ochrony, zanim użytkownik w systemie (SYSTEMA) będzie mógł pracować z innym systemem (SYSTEMB) muszą zajść następujące zdarzenia:

- system źródłowy (SYSTEMA) musi dostarczyć ścieżkę do systemu docelowego (SYSTEMB); ścieżka ta jest nazywana **sesją APPC**,
- system docelowy musi zidentyfikować użytkownika i powiązać go z profilem użytkownika; musi także obsługiwać algorytm szyfrowania systemu źródłowego (patrz “Poziomy haseł” na stronie 16),
- system docelowy musi uruchomić zadanie dla użytkownika we właściwym środowisku (wartości zarządzania pracą).

Sekcje podane poniżej opisują wymienione elementy i ich powiązanie z ochroną. W systemie docelowym za naruszenie ochrony przez użytkowników APPC jest odpowiedzialny administrator ochrony. Jeśli jednak administratorzy ochrony w obu systemach współpracują ze sobą, zadanie zarządzania ochroną APPC jest dużo łatwiejsze.

Przykład: podstawy sesji APPC

W środowisku APPC, gdy użytkownik lub aplikacja w jednym systemie żąda dostępu do innego systemu, oba systemy ustanawiają sesję. Aby ustanowić sesję, systemy muszą znaleźć dwa zgodne opisy urządzeń APPC. Parametr nazwa zdalnego miejsca (RMTLOCNAME) w opisie urządzenia SYSTEMA musi być zgodny z parametrem nazwa lokalnego miejsca (LCLLOCNAME) w opisie urządzenia SYSTEMB i odwrotnie.

Aby dwa systemy ustanowiły sesję APPC, hasła miejsca w opisach urządzeń APPC w systemach SYSTEMA i SYSTEMB muszą być identyczne. W obu systemach musi być podana wartość *NONE, lub oba muszą zawierać tę samą wartość.

Jeśli hasła są wartościami innymi niż *NONE, to są przechowywane i przesyłane w zaszyfrowanym formacie. Jeśli hasła są zgodne, systemy ustanawiają sesję. Jeśli hasła nie są zgodne, żądanie użytkownika jest odrzucane. Podawanie przez systemy haseł miejsc w celu ustanowienia sesji jest nazywane **konsolidacją ochrony**.

Uwaga: Nie wszystkie systemy komputerowe udostępniają obsługę funkcji konsolidacji ochrony.

Ograniczanie sesji APPC

Administrator ochrony w systemie źródłowym może użyć uprawnień do obiektów, aby ustalić, kto ma dostęp do innych systemów. Należy ustawić uprawnienie publiczne dla opisów urządzeń APPC na *EXCLUDE i określonym użytkownikom nadać uprawnienie *CHANGE. Aby uniemożliwić użytkownikom z uprawnieniem *ALLOBJ używanie komunikacji APPC, należy użyć wartości systemowej QLMTSECOFR.

Administrator ochrony w systemie docelowym może również użyć uprawnienia do używania urządzeń APPC, aby uniemożliwić użytkownikom uruchamianie sesji APPC w systemie. Musi on jednak wiedzieć, który identyfikator użytkownika będzie używany do uzyskania dostępu do opisu urządzenia APPC. Sekcja “Sposoby uzyskania dostępu do systemu docelowego przez użytkownika APPC” na stronie 105 opisuje, jak serwer iSeries w trakcie sesji APPC kojarzy identyfikator użytkownika ze zgłoszeniem.

Uwaga: Aby dowiedzieć się, kto ma w systemie uprawnienia do opisów urządzeń, można użyć komend Drukowanie obiektów z uprawnieniami publicznymi (Print Publicly Authorized Objects - PRTPUBAUT *DEVD) i Drukowanie uprawnień prywatnych (Print Private Authorities (PRTPVTAUT *DEVD).

Jeśli w systemie używana jest sieć APPN, nowe urządzenie APPC jest tworzone automatycznie, gdy brak jest urządzeń dla trasy wybranej przez system. Jedną z możliwości ograniczenia dostępu do urządzeń APPC w systemie używającym sieciAPPN jest lista

autoryzacji. Zawiera ona użytkowników, którzy mogą uzyskać dostęp do urządzeń APPC. Następnie używa się komendy Zmiana wartości domyślnych komendy (Change Command Default - CHGCMDDFT) do zmiany komendy CRTDEVAPPC. Jako wartość domyślną parametru uprawnień (AUT) komendy CRTDEVAPPC należy podać utworzoną listę autoryzacji.

Uwaga: Jeśli w systemie używany jest język inny niż angielski, należy zmienić wartość domyślną komendy w bibliotece QSYSxxxx dla każdego języka narodowego zainstalowanego w systemie.

Aby sprawdzić tożsamość innego systemu żądającego otwarcia sesji w systemie (w imieniu użytkownika lub programu), używa się parametru Hasło miejsca (LOCPWD) w opisie urządzenia APPC. Hasło miejsca pomaga wykryć system popełniający oszustwo.

Gdy używa się haseł miejsca należy współpracować z administratorami ochrony innych systemów w sieci. Należy również kontrolować, kto może tworzyć i zmieniać opisy urządzeń APPC i listy konfiguracji. System wymaga posiadania uprawnienia specjalnego *IOSYSCFG, aby można było używać komend pracujących z urządzeniami i listami konfiguracji APPC.

Uwaga: Jeśli używa się sieci APPN, hasła miejsc są przechowywane na liście konfiguracji QAPPNRMT, a nie w opisach urządzeń.

Sposoby uzyskania dostępu do systemu docelowego przez użytkownika APPC

Gdy systemy ustanawiają sesję APPC. tworzona jest ścieżka dla użytkownika zgłaszającego żądanie. Ścieżka ta umożliwia mu uzyskanie dostępu do systemu docelowego. Kilka innych elementów określa, co musi zrobić użytkownik, aby uzyskać dostęp do innego systemu.

Poniższe sekcje opisują elementy określające, w jaki sposób użytkownik APPC uzyskuje dostęp do systemu docelowego.

Metody używane przez system do wysyłania informacji o użytkowniku

Architektura APPC udostępnia trzy metody wysyłania informacji o ochronie o użytkowniku z systemu źródłowego do systemu docelowego. Metody te bywają nazywane **wartościami ochrony architektury**. Tabela 18 zawiera te metody.

Uwaga: Książka *APPC Programming* zawiera więcej informacji na temat wartości ochrony architektury.

Tabela 18. Wartości ochrony w architekturze APPC

Archtektura wartości ochrony	Identyfikator użytkownika wysyłany do systemu docelowego	Hasło wysyłane do systemu docelowego
brak	Nie	Nie
Same	Tak[1]	Patrz uwaga 2.
Program	Tak	Tak[3]

Tabela 18. Wartości ochrony w architekturze APPC (kontynuacja)

Archtektura wartości ochrony	Identyfikator użytkownika wysyłany do systemu docelowego	Hasło wysyłane do systemu docelowego

Uwagi:

1. System źródłowy wysyła identyfikator użytkownika, jeśli w systemie docelowym podano SECURELOC(*YES) lub SECURELOC(*VFYENCPWD).
2. Użytkownik nie wysyła hasła na żądanie, ponieważ zostało ono już sprawdzone przez system źródłowy. W przypadku, gdy podano SECURELOC(*YES) i SECURELOC(*NO) system źródłowy nie wysyła hasła. W przypadku SECURELOC(*VFYENCPWD) system źródłowy pobiera zapisane i zaszyfrowane hasło i wysyła je (w postaci zaszyfrowanej).
3. System wysyła zaszyfrowane hasło, jeśli zarówno systemy źródłowy, jak i docelowy obsługują szyfrowanie haseł. W przeciwnym przypadku hasło nie jest szyfrowane.

Aplikacja żądana przez użytkownika określa wartość ochrony architektury. Na przykład SNADS zawsze używa SECURITY(NONE). DDM używa SECURITY(SAME). W przypadku tranzytu terminalu użytkownik podaje wartość ochrony używając komendy STRPASTHR z parametrami.

We wszystkich przypadkach system docelowy określa, czy zaakceptować żądanie z wartością ochrony podaną w systemie źródłowym. W niektórych sytuacjach system docelowy może całkowicie odrzucić żądanie. W innych sytuacjach system docelowy może wymusić podanie innej wartości ochrony. Na przykład jeśli użytkownik podaje w komendzie STRPASTHR zarówno identyfikator użytkownika, jak i hasło, żądanie używa wartości ochrony SECURITY(PGM). Jednak jeśli wartość systemowa QRMTSIGN w systemie docelowym jest równa *FRCSIGNON, użytkownik nadal będzie używał ekranu Wpisanie się (Sign On). Przy ustawieniu *FRCSIGNON system zawsze używa wartości SECURITY(NONE), co jest jednoznaczne z niepodaniem identyfikatora użytkownika i hasła w komendzie STRPASTHR.

Uwagi:

1. Systemy źródłowy i docelowy negocjują wartość ochrony przed wysłaniem danych. W przypadku gdy w systemie docelowym podano SECURELOC(*NO), a żądanie to na przykład SECURITY(SAME), system docelowy informuje system docelowy, aby użył on SECURITY(NONE). System źródłowy nie wysyła identyfikatora użytkownika.
2. System docelowy odrzuca żądanie sesji, gdy hasło użytkownika w systemie docelowym wygasło. Ma to miejsce tylko w przypadku żądań połączeń wysyłających hasło, w tym:
   - żądania sesji typu SECURITY(PROGRAM),
   - żądania sesji typu SECURITY(SAME), gdy SECURELOC przyjmuje wartość *VFYENCPWD.

Opcje podziału odpowiedzialności za ochronę

Gdy system znajduje się w sieci, należy zdecydować, czy można zaufać innym systemom sprawdzającym tożsamość użytkownika próbującego uzyskać dostęp do systemu. Czy można zaufać systemowi SYSTEMA, że sprawdzi, czy użytkownik USERA to naprawdę USERA (lub czy użytkownik QSECOFR to naprawdę QSECOFR)? Czy może należy wymusić na użytkowniku, aby podał ponownie identyfikator i hasło?

Parametr Chronione miejsce (SECURELOC) w opisie urządzenia APPC w systemie docelowym określa, czy system źródłowy jest chronionym (zaufanym) miejscem.

Jeśli na obu systemach działa wersja, która obsługuje wartość *VFYENCPWD, SECURELOC(*VFYENCPWD) zapewnia dodatkową ochronę, gdy aplikacje używają

SECURITY(SAME). Mimo że osoba żądająca nie podaje hasła w żądaniu, system źródłowy pobiera hasło użytkownika i wysyła je z żądaniem. Aby żądanie powiodło się, użytkownik musi mieć w obu systemach te same identyfikator użytkownika oraz hasło.

W przypadku gdy w systemie docelowym podano SECURELOC(*VFYENCPWD), a system źródłowy nie obsługuje tej wartości, system docelowy obsługuje to żądanie jako SECURITY(NONE).

Tabela 19 pokazuje współdziałanie wartości ochrony architektury i wartości SECURELOC:

Tabela 19. Współdziałanie wartości ochrony APPC i wartości SECURELOC

System źródłowy	**System docelowy**	
Archtektura wartości ochrony	**Wartość SECURELOC**	**Zmiana profilu użytkownika dla zadania**
brak	Any (dowolna)	Użytkownik domyślny[1]
Same	*NO	Użytkownik domyślny[1]
	*YES	Nazwa profilu użytkownika i osoby żądającej z systemu źródłowego muszą być takie same
	*VFYENCPWD	Nazwa profilu użytkownika i osoby żądającej z systemu źródłowego muszą być takie same; użytkownik musi mieć to samo hasło w obu systemach
Program	Any (dowolna)	Profile użytkowników podane w żądaniu systemu źródłowego

Uwagi:

1. Użytkownik domyślny jest określany przez pozycję komunikacji w opisie podsystemu. Opisuje to poniższa sekcja “Przypisywanie profilu użytkownia dla zadań w systemie docelowym”.

Przypisywanie profilu użytkownia dla zadań w systemie docelowym

Gdy użytkownik żąda uruchomienia zadania APPC w innym systemie, z żądaniem tym powiązana jest nazwa trybu. Nazwa trybu może pochodzić z żądania użytkownika lub może być wartością domyślną pobraną z atrybutów sieciowych systemu źródłowego.

System docelowy używa nazwy trybu i nazwy urządzenia APPC do określenia sposobu uruchomienia zadania. System docelowy przeszukuje aktywne podsystemy, aby znaleźć pozycję komunikacji, która jest najbardziej zgodna z nazwą urządzenia APPC i nazwą trybu.

Pozycja komunikacji określa profil użytkownika, który zostanie użyty przez system dla żądań SECURITY(NONE). Poniżej podano przykład pozycji komunikacji w opisie podsystemu:

```
                        Wyświetlenie pozycji komunikacji
                        (Display Communications Entries)

Opis podsystemu:        QCMN            Status:   ACTIVE

                         Opis                          Użytkownik    Maks.
Opis          Tryb       zadania        Biblioteka     domyślny      aktywnych
*ALL          *ANY       *USRPRF                       *SYS          *NOMAX
*ALL          QPCSUPP    *USRPRF                       *NONE         *NOMAX
```

Tabela 20 na stronie 108 przedstawia dopuszczalne wartości dla parametru Użytkownik domyślny w pozycji komunikacji.

Tabela 20. Dopuszczalne wartości dla parametru określającego użytkownika domyślnego

Wartość	Rezultat
***NONE**	Brak użytkownika domyślnego. Jeśli system źródłowy nie dostarczy w żądaniu identyfikatora użytkownika, zadanie nie zostanie uruchomione.
***SYS**	Można uruchamiać tylko programy dostarczone przez IBM (zadania systemowe). Nie można uruchamiać aplikacji użytkowników.
nazwa-użytkownika	Jeśli system źródłowy nie wyśle identyfikatora użytkownika, zadanie jest uruchamiane z tym profilem użytkownika.

Aby wydrukować listę podsystemów, które mają pozycje komunikacji z profilem użytkownika domyślnego, można użyć komendy Drukowanie opisu podsystemu (Print Subsystem Description - PRTSBSDAUT).

Opcje tranzytu terminalu

Tranzyt terminalu jest przykładem aplikacji używającej komunikacji APPC. Tranzytu terminalu można użyć do wpisania się do innego systemu połączonego z używanym systemem poprzez sieć.

Tabela 21 zawiera przykłady żądań tranzytu (komenda STRPASTHR) i sposób ich obsługi przez system docelowy. W przypadku tranzytu terminalu system używa podstawowych elementów komunikacji APPC i wartości systemowej zdalnego wpisania się (QRMTSIGN).

Uwaga: Zadania tranzytu terminalu nie są już kierowane przez podsystemy QCMN i QBASE. Od wersji V4R1 są one kierowane przez podsystem QSYSWRK. W wersjach wcześniejszych od V4R1 można było przyjąć, że jeśli podsystem QCMD lub QBASE nie jest uruchomiony, to tranzyt terminalu nie będzie działał. Nie jest to już prawdą. Można wymusić, aby tranzyt terminalu przechodził przez podsystem QCMN (lub QBASE, jeśli jest aktywny) zmieniając wartość systemową QPASTHRSVR na 0.

Tabela 21. Przykład zadania tranzytu terminalu

Wartości w komendzie STRPASTH		**System docelowy**		
ID użytkownika	**Hasło**	**Wartość SECURELOC**	**Wartość QRMTSIGN**	**Wynik**
*NONE	*NONE	Any (dowolna)	Any (dowolna)	Użytkownik musi się wpisać w systemie docelowym.
Nazwa profilu użytkownika	Nie wpisano	Any (dowolna)	Any (dowolna)	Żądanie nie powiodło się.

Tabela 21. Przykład zadania tranzytu terminalu (kontynuacja)

Wartości w komendzie STRPASTH		**System docelowy**		
ID użytkownika	**Hasło**	**Wartość SECURELOC**	**Wartość QRMTSIGN**	**Wynik**
*CURRENT	Nie wpisano	*NO	Any (dowolna)	Żądanie nie powiodło się.
		*YES	*SAMEPRF	Zadanie interaktywne jest uruchamiane z tym samym profilem użytkownika, jak profil w systemie źródłowym. Do systemu zdalnego nie jest wysyłane hasło. Nazwa profilu użytkownika musi istnieć w systemie docelowym.
			*VERIFY	
			*FRCSIGNON	Użytkownik musi się wpisać w systemie docelowym.
		*VFYENCPWD	*SAMEPRF	Zadanie interaktywne jest uruchamiane z tym samym profilem użytkownika, jak profil w systemie źródłowym. System źródłowy pobiera hasło użytkownika i wysyła je do systemu zdalnego. Nazwa profilu użytkownika musi istnieć w systemie docelowym.
			*VERIFY	
			*FRCSIGNON	Użytkownik musi się wpisać w systemie docelowym.
*CURRENT (lub nazwa bieżącego profilu użytkownika dla zadania)	Wpisano	Any (dowolna)	*SAMEPRF	Zadanie interaktywne jest uruchamiane z tym samym profilem użytkownika, jak profil w systemie źródłowym. Hasło *jest* wysyłane do systemu zdalnego. Nazwa profilu użytkownika musi istnieć w systemie docelowym.
			*VERIFY	
			*FRCSIGNON	Użytkownik musi się wpisać w systemie docelowym.
Nazwa profilu użytkownika (nazwa inna niż bieżący profil użytkownika dla zadania)	Wpisano	Any (dowolna)	*SAMEPRF	Żądanie nie powiodło się.
			*VERIFY	Zadanie interaktywne jest uruchamiane z tym samym profilem użytkownika, jak profil w systemie źródłowym. Hasło *jest* wysyłane do systemu zdalnego. Nazwa profilu użytkownika musi istnieć w systemie docelowym.
			*FRCSIGNON	Zadanie interaktywne jest uruchamiane z podaną nazwą profilu użytkownika. Hasło jest wysyłane do systemu docelowego. Nazwa profilu użytkownika musi istnieć w systemie docelowym.

Unikanie nieoczekiwanego przypisania urządzenia

Gdy nastąpi awaria w aktywnym urządzeniu, system próbuje ją usunąć. W niektórych przypadkach, gdy zostaje przerwana komunikacja, inny użytkownik może niechcący ponownie ustanowić sesję, w której wystąpiła awaria. Na przykład przyjmijmy, że użytkownik USERA wyłączył stację roboczą bez wypisania się. USERB może włączyć tę stację roboczą i ponownie uruchomić sesję użytkownika USERA bez wpisywania się.

Aby to uniemożliwić, należy ustawić wartość systemową Działanie w przypadku błędu urządzenia we/wy (QDEVRCYACN) na *DSCMSG. Gdy urządzenie ulegnie awarii, system zakończy zadanie użytkownika.

Sterowanie komendami zdalnymi i zadaniami wsadowymi

Dostępnych jest kilka opcji pomocnych przy określaniu, które komendy i zadania zdalne mogą być uruchamiane w systemie. Niektóre z nich opisano poniżej.

- Jeśli system używa DDM, można ograniczyć dostęp do plików DDM, aby uniemożliwić użytkownikom używanie z innego systemu komendy Wprowadzenie komendy zdalnej (Submit Remote Command - SBMRMTCMD). Aby używać komendy SBMRMTCMD, użytkownik musi mieć możliwość otwarcia pliku DDM. Należy również ograniczyć możliwość tworzenia plików DDM.
- Można podać program obsługi wyjścia dla wartości systemowej Żądanie dostępu do DDM (DDMACC). W programie obsługi wyjścia można ocenić wszystkie żądania DDM przed ich udostępnieniem.
- Można użyć atrybutu sieciowego Działanie zadania sieciowego (JOBACN), aby uniemożliwić wprowadzanie zadań sieciowych i ich automatyczne uruchamianie.
- Można jawnie określić, które żądania programu mogą być uruchamiane w środowisku komunikacyjnym poprzez usunięcie pozycji routingu PGMEVOKE z opisów podsystemów. Pozycja routingu PGMEVOKE umożliwia requesterowi określenie uruchomionego programu. Jeśli usunie się tę pozycję routingu z opisów podsystemów, takich jak opis podsystemu QCMN, należy dodać pozycje routingu dla żądań routingu, które mają być pomyślnie uruchamiane.

  Sekcja “Żądania nazw TPN architektury” na stronie 87 zawiera nazwy programów dla żądań komunikacji pochodzących z aplikacji dostarczonych przez IBM. Dla każdego żądania, które ma być dozwolone, można dodać pozycję routingu z wartością porównywaną i nazwą programu takimi samymi jak nazwa programu.

  Gdy używa się tej metody, należy rozumieć środowisko zarządzania pracą w systemie oraz typy żądań komunikacji występującej w systemie. Po zmianie pozycji routingu należy, o ile to możliwe, przetestować wszystkie typy żądań komunikacji, aby sprawdzić, czy poprawnie działają. Gdy żądanie komunikacji nie znajdzie dostępnej pozycji routingu, zostanie wyświetlony komunikat CPF1269. Alternatywnym rozwiązaniem (powodującym mniej błędów, ale mniej efektywnym) jest ustawienie uprawnienia publicznego na *EXCLUDE dla programów transakcji, które mają nie być uruchamiane w systemie.

  Uwaga: Książka *Zarządzanie pracą w systemie AS/400* zawiera więcej informacji na temat pozycji routingu i sposobu obsługi przez system żądań uruchomienia programów.

Ocena konfiguracji APPC

Aby wydrukować wartości dotyczące ochrony podane w konfiguracji APPC, można użyć komendy Drukowanie ochrony komunikacji (Print Communications Security - PRTCMNSEC) lub opcji menu. Poniższe sekcje opisują informacje znajdujące się na raportach.

Parametry dotyczące urządzeń APPC

Rys. 9 zawiera przykład raportu z informacjami o komunikacji dla opisów urządzeń. Rys. 10 przedstawia przykładowy raport list konfiguracji. U dołu każdego raportu znajduje się objaśnienie pól zawartych w raportach.

```
                          Informacje o komunikacji - pełny raport
                        (Communications Information - Full Report)
                                                                                SYSTEM4
Typ obiektu  . . . . . . . . . :   *DEVD
Obiekt       Wstępne
ustanawia    uruchomienie    Kategoria      Chronione    Hasło        Obsługa     Pojedyncza
nazwę        typu            urządzenia
sesji        programu        SNUF           miejsce      miejsca      APPN        sesja

CDMDEV1        *DEVD          *APPC            *NO          *NO         *NO         *YES         *NO
CDMDEV2        *DEVD          *APPC            *NO          *NO         *NO         *YES         *NO
```

Rysunek 9. Przykładowy raport opisu urządzeń APPC

```
               Wyświetlenie listy konfiguracji
                (Display Configuration List)           Strona   1
                            SYSTEM4  12/17/95  07:24:36
Lista konfiguracji . . . . . . . . :   QAPPNRMT
Typ listy konfiguracji . . . . . . :   *APPNRMT
Tekst. . . . . . . . . . . . . . . :
-----------------Zdalne miejsca APPN-------------------------
          Ident.              Zdalny    Sieciowy
Zdalne    sieci     Lokalne   punkt     ident.     Chronione
miejsce   zdalnej   miejsce   kontrolny pun. kont. miejsce
SYSTEM36  APPN      SYSTEM4   SYSTEM36  APPN       *NO
SYSTEM32  APPN      SYSTEM4   SYSTEM32  APPN       *NO
SYSTEMU   APPN      SYSTEM4   SYSTEM33  APPN       *YES
SYSTEMJ   APPN      SYSTEM4   SYSTEMJ   APPN       *NO
SYSTEMR2  APPN      SYSTEM4   SYSTEM1   APPN       *NO
-----------------Zdalne miejsca APPN-----------------------------------------
          Ident.                                      Lokalny   Wstępne
Zdalne    sieci     Lokalne   Pojedyncza  Liczba     punkt     ustanowienie
miejsce   zdalnej   miejsce   sesja      konwersacji  kontrolny sesji
SYSTEM36  APPN      SYSTEM4    *NO             10      *NO        *NO
SYSTEM32  APPN      SYSTEM4    *NO             10      *NO        *NO
```

Rysunek 10. Przykładowy raport z listą konfiguracji

Pole Chronione miejsce

Pole Chronione miejsce (SECURELOC) określa, czy system lokalny ufa systemowi zdalnemu, jeśli chodzi o sprawdzenie hasła w imieniu systemu lokalnego. Pole SECURELOC jest stosowane tylko w przypadku aplikacji używających wartości SECURITY(SAME), takich jak DDM i aplikacji używających interfejsu API CPI-Communications.

Poprzez ustawienie SECURELOC(*YES) system lokalny staje się wrażliwy na możliwą niedoskonałość systemu zdalnego. Każdy użytkownik istniejący w obu systemach może wywołać programy w systemie lokalnym. Jest to szczególnie niebezpieczne, ponieważ profil użytkownika QSECOFR (szef ochrony) istnieje we wszystkich systemach iSeries i ma uprawnienie specjalne *ALLOBJ. Jeśli system w sieci dobrze nie zabezpieczy hasła QSECOFR, zagrożone są inne systemy traktujące ten system jako chronione miejsce.

Jeśli użyje się SECURELOC(*VFYENCPWD), system jest mniej wrażliwy na inne systemy, które nieodpowiednio chronią hasła. Użytkownik żądający aplikacji używającej SECURITY(SAME) musi mieć ten sam identyfikator użytkownika i hasło w obu systemach.

Ustawienie SECURELOC(*VFYENCPWD) wymaga strategii zarządzania hasłami w sieci, aby użytkownicy mieli te same hasła we wszystkich systemach.

Uwaga: Ustawienie SECURELOC(*VFYENCPWD) jest obsługiwane tylko między systemami w wersjach V3R2, V3R7 i V4R1. Jeśli w systemie docelowym podano SECURELOC(*VFYENCPWD) i system źródłowy nie obsługuje tej funkcji, żądanie jest obsługiwane jako SECURITY(NONE).

Jeśli w systemie podano SECURELOC(*NO), w zastosowaniach wykorzystujących SECURITY(SAME) do uruchamiania programów potrzebny jest użytkownik domyślny. Użytkownik domyślny zależy od opisu urządzenia i od trybu powiązanych z żądaniem. (Patrz sekcja “Przypisywanie profilu użytkownia dla zadań w systemie docelowym” na stronie 107.)

Pole Hasło miejsca

Pole Hasło miejsca określa, czy omawiane dwa systemy będą wymieniały hasła w celu sprawdzenia, czy system żądający nie jest oszustem. Więcej informacji na temat haseł miejsca zawiera sekcja “Przykład: podstawy sesji APPC” na stronie 104.

Pole Obsługa APPN

Pole Obsługa APPN (APPN) określa, czy system zdalny może obsługiwać zaawansowane funkcje sieciowe, czy jest ograniczony do połączeń o długości jeden hop. Ustawienie APPN(*YES) oznacza, że:

- Jeśli system zdalny jest węzłem sieci, system ten może połączyć system lokalny z innymi systemami. Jest to tak zwany **routing poprzez węzły pośrednie**. Oznacza to, że użytkownicy w systemie mogą używać systemu zdalnego jako trasy do większej sieci.
- Jeśli system lokalny jest węzłem sieci, system zdalny może użyć systemu lokalnego do połączenia się z innymi systemami. Użytkownicy w systemie zdalnym mogą używać systemu jako trasy do większej sieci.

  Uwaga: Aby określić, czy system jest węzłem sieci lub węzłem końcowym, można użyć komendy DSPNETA.

Pole Pojedyncza sesja

Pole Pojedyncza sesja (SNGSSN) określa, czy system zdalny może uruchomić w tym samym czasie więcej niż jedną sesję używając tego samego opisu urządzenia APPC. Powszechnie używane jest ustawienie SNGSSN(*NO), ponieważ stosując je nie trzeba tworzyć wielu opisów urządzeń dla systemu zdalnego. Na przykład użytkownik komputera PC często potrzebuje więcej niż jednej sesji emulacji terminalu 5250 i sesji dla funkcji serwera plików i serwera wydruków. Ustawienie SNGSSN(*NO) umożliwia udostępnienie tej funkcji z użyciem jednego opisu urządzenia dla komputera PC w systemie iSeries.

Ustawienie SNGSSN(*NO) oznacza, że trzeba polegać na procedurach działania świadomych ochrony użytkowników komputerów PC i użytkowników APPC. System jest wrażliwy na działania użytkownika z systemu zdalnego uruchamiającego nieautoryzowaną sesję używającą tego samego opisu urządzenia, co istniejąca sesja. (Taka praktyka bywa również nazywana **nakładaniem - piggy-backing**.)

Pole Wstępne ustanowienie sesji

Pole Wstępne ustanowienie sesji (PREESTSSN) dla urządzenia obsługującego pojedynczą sesję określa, czy system lokalny rozpoczyna sesję z systemem zdalnym gdy system zdalny jako pierwszy kontaktuje się z systemem lokalnym. Ustawienie PREESTSSN(*NO) oznacza, że system lokalny czeka z rozpoczęciem sesji, aż do momentu gdy aplikacja zażąda sesji z systemem. Ustawienie PREESTSSN(*YES) jest przydatne do zminimalizowania okresu czasu, którego potrzebuje aplikacja do zakończenia połączenia.

Ustawienie PREESTSSN(*YES) chroni system przed rozłączeniem linii komutowanej (dial-up), która nie jest już używana. Aplikacja lub użytkownik musi jawnie unieaktywnić linię. Ustawienie PREESTSSN(*YES) może wydłużyć okres czasu, przez który system lokalny jest wrażliwy na nakładanie sesji.

Pole Uruchomienie programu SNUF

Pole Uruchomienie programu SNUF określa, czy system zdalny może uruchamiać programy w systemie lokalnym. Wybranie *YES oznacza, że schemat uprawnień do obiektów w systemie lokalnym musi chronić obiekty, gdy użytkownicy w systemie zdalnym uruchamiają zadania i programy w systemie lokalnym.

Parametry dla kontrolerów APPC

Rys. 11 zawiera przykład raportu z informacjami o komunikacji dla opisów kontrolerów. Pod rysunkiem podano objaśnienie pól występujących w raporcie.

```
                          Informacje o komunikacji - pełny raport
                         (Communications Information - Full Report)
                                                                                SYSTEM4
Typ obiektu  . . . . . . . . . . :   *CTLD

Nazwa     Typ       Kategoria    Automat.  Kontroler   Kierunek    Obsługa   Sesje       Licznik cz.  Sekundy  Nazwa
obiektu   obiektu   kontrolera   tworzenie komutowany   wybierania  APPN      pkt. kon.   odłączenia   do usun. urządzenia
CTL01     *CTLD     *APPC         *YES       *YES        *DIAL      *YES       *YES           0       1440    AARON
CTL02     *CTLD     *APPC         *YES       *YES        *DIAL      *YES       *YES           0       1440    BASIC
CTL03     *CTLD     *APPC         *YES       *YES        *DIAL      *YES       *YES           0       1440    *NONE
```

Rysunek 11. Przykładowy raport opisu kontrolerów APPC

Pole Automatyczne tworzenie

W opisie linii pole Automatyczne tworzenie (AUTOCRTCTL) określa, czy system lokalny automatycznie tworzy opis kontrolera, gdy przychodzące żądanie nie może znaleźć swojego odpowiednika. W opisie kontrolera pole Automatyczne tworzenie (AUTOCRTDEV) określa, czy system lokalny automatycznie tworzy opis urządzenia, gdy przychodzące żądanie nie może znaleźć swojego odpowiednika.

W przypadku kontrolerów z obsługą APPN pole to nie ma żadnego znaczenia. System automatycznie tworzy opisy urządzeń, gdy jest to potrzebne bez względu na sposób ustawienia pola Automatyczne tworzenie.

Jeśli w opisie linii poda się *YES, wszyscy użytkownicy mający dostęp do linii mogą połączyć się z systemem. Dotyczy to również miejsc połączonych za pomocą mostów i routerów.

Pole Sesje punktów kontrolnych

W przypadku kontrolerów z obsługą APPN pole Sesje punktów kontrolnych (CPSSN) określa, czy system automatycznie ustanawia połączenie APPC z systemem zdalnym. System używa sesji punktów kontrolnych do wymiany informacji sieciowych i statusu z systemem zdalnym. Wymiana aktualnych informacji między węzłami sieci APPN jest szczególnie ważna we właściwym funkcjonowaniu sieci.

Jeśli poda się *YES, bezczynna linia komutowana nie rozłącza się automatycznie. Przez to system jest bardziej wrażliwy na nakładane sesje.

Pole Licznik czasu odłączenia

W przypadku kontrolera APPC pole Licznik czasu odłączenia określa, przez jaki czas kontroler musi być nieużywany (brak aktywnych sesji) zanim system odłączy linię od systemu zdalnego. W polu tym podaje się dwie wartości. Pierwsza wartość określa, jak długo

kontroler pozostanie aktywny od momentu, gdy nawiązano z nim początkowe połączenie. Druga wartość określa, jak długo system czeka po zakończeniu ostatniej sesji przy użyciu kontrolera przed usunięciem linii.

System używa licznika czasu odłączenia tylko wtedy, gdy pole Rozłączenie komutowane (SWTDSC) jest ustawione na *YES.

Jeśli zwiększy się omawiane wartości, system będzie bardziej wrażliwy na nakładanie sesji.

Parametry dla opisów linii

Rys. 12 zawiera przykład raportu z informacjami o komunikacji dla opisów linii. Pod rysunkiem podano objaśnienie pól występujących w raporcie.

```
                    Informacje o komunikacji - pełny raport
                  (Communications Information - Full Report)

Typ obiektu  . . . . . . . . . :   *LIND
Nazwa          Typ           Kategoria      Automat.   Sekundy     Automat.   Automat.
obiektu aut.   obiektu       linii          tworzenie  do usun.    odpowiedź  wybieranie
LINE01          *LIND         *SDLC           *NO           0       *NO       *NO
LINE02          *LIND         *SDLC           *NO           0       *YES      *NO
LINE03          *LIND         *SDLC           *NO           0       *NO       *NO
LINE04          *LIND         *SDLC           *NO           0       *YES      *NO
```

Rysunek 12. Przykładowy raport opisu linii APPC

Pole Automatyczna odpowiedź

Pole Automatyczna odpowiedź (AUTOANS) określa, czy linia komutowana będzie akceptowała połączenia przychodzące bez interwencji operatora.

Jeśli poda się *YES, system będzie mniej bezpieczny, ponieważ łatwiej będzie uzyskać do niego dostęp. Aby zminimalizować narażenie ochrony przez podanie wartości *YES, należy unieaktywnić linię, gdy nie jest potrzebna.

Pole Automatyczne wybieranie

Pole Automatyczne wybieranie (AUTODIAL) określa, czy linia komutowana może nawiązywać połączenia wychodzące bez interwencji operatora. Jeśli poda się wartość *YES, lokalni użytkownicy nie mający fizycznego dostępu do linii komunikacyjnych i modemów będą mogli połączyć się z innymi systemami.

Rozdział 13. Bezpieczna komunikacja TCP/IP

Komputery wszystkich typów powszechnie używają protokołu TCP/IP (Transmission Control Protocol/Internet Protocol) do komunikowania się. Aplikacje TCP/IP są ogólnie znane i szeroko stosowane na "infostradzie".

W tym rozdziale przedstawiono wskazówki dotyczące następujących zagadnień:

- zablokowanie możliwości uruchamiania aplikacji TCP/IP w systemie,
- ochrona zasobów systemowych przy odblokowanej możliwości uruchamiania aplikacji TCP/IP w systemie.

Strona WWW Centrum informacyjne iSeries—>Sieć—>TCP/IP jest kompletnym źródłem informacji o wszystkich aplikacjach TCP/IP. Sekcja *SecureWay: iSeries i Internet* (Centrum informacyjne iSeries—>Ochrona—>SecureWay) opisuje ochronę podczas połączenia serwera iSeries zarówno z Internetem (bardzo duża sieć oparta na protokole TCP/IP), jak i z intranetem. Informacje na temat dostępu do Centrum informacyjnego iSeries zawiera sekcja "Informacje wstępne i pokrewne" na stronie xii.

Należy pamiętać, że serwer iSeries obsługuje wiele różnych aplikacji TCP/IP. Po umożliwieniu działania jednej aplikacji TCP/IP w systemie, prawdopodobnie zapadnie decyzja o uaktywnieniu innych aplikacji TCP/IP. Administrator ochrony powinien znać różne aplikacje TCP/IP i ich wpływ na bezpieczeństwo systemu.

Uniemożliwienie przetwarzania protokołu TCP/IP

Zadania serwera TCP/IP są wykonywane w podsystemie QSYSWRK. Do uruchamiania przetwarzania TCP/IP służy komenda Uruchamianie TCP/IP (STRTCP). Aby uniemożliwić przetwarzanie TCP/IP oraz działanie aplikacji, nie należy używać komendy STRTCP. System dostarczany jest z publicznymi uprawnieniami do komendy STRTCP ustawionymi na *EXCLUDE.

W przypadku podejrzeń, że ktoś z prawami dostępu do komendy uruchamia przetwarzanie TCP/IP (na przykład po godzinach pracy), można zainstalować kontrolowanie obiektu dla komendy STRTCP. Za każdym razem, gdy użytkownik uruchomi komendę, system dokona wpisu do kroniki kontroli.

Komponenty ochrony protokołu TCP/IP

Można wykorzystać możliwości kilku komponentów ochrony TCP/IP, które podnoszą bezpieczeństwo sieci i zwiększają jej elastyczność. Chociaż niektóre z tych technologii zostały zastosowane w firewallach, to komponenty ochrony TCP/IP dla OS/400, nie są przewidziane do użycia jako oprogramowanie firewall. Czasem jednak możliwe jest wykorzystanie niektórych opcji, tak że nie jest potrzebne instalowanie osobnego oprogramowania firewall. Opisywane opcje TCP/IP mogą być użyte do zapewnienia dodatkowych zabezpieczeń w środowisku, w którym jest stosowany firewall.

Następujące komponenty można wykorzystać do wzmocnienia ochrony TCP/IP:

- reguły pakietów,
- serwer proxy HTTP,
- sieć VPN (Virtual Private Network),
- protokół SSL (Secure Sockets Layer).

Użycie reguł pakietów do ochrony obsługi protokołu TCP/IP

Reguły pakietów, na które składają się filtrowanie IP oraz translacja adresu sieciowego (NAT) zachowują się jak oprogramowanie firewall w celu zabezpieczenia sieci wewnętrzej przed intruzami. Filtrowanie IP pozwala na sterowanie ruchem protokołu IP do i z sieci. Generalnie, zabezpiecza ono sieć poprzez filtrowanie pakietów zgodnie ze zdefiniowanymi regułami. Z drugiej strony NAT umożliwia ukrycie niezarejestrowanych prywatnych adresów IP za zbiorem zarejestrowanych adresów IP. Pomaga to zabezpieczać sieć wewnętrzną od zagrożeń płynących z sieci zewnętrznych. NAT dodatkowo łagodzi problem z ograniczoną liczbą adresów IP, dzięki możliwości rezprezentowania adresów prywatnych prez mały zbiór zarejestrowanych adresów. Więcej informacji na ten temat znajduje się w Centrum informacyjnym iSeries.

Serwer proxy HTTP

Serwer proxy HTTP jest dostarczany wraz z serwerem IBM HTTP Server dla iSeries. Serwer HTTP jest częścią systemu OS/400. Serwer proxy otrzymuje żądania HTTP z przeglądarek WWW i wysyła je do serwerów WWW. Serwery WWW otrzymujące żądania znają jedynie adresy IP serwera proxy i nie mogą określić nazw ani adresów komputerów PC, z których pochodzą żądania. Serwer proxy może obsługiwać żądania adresów URL dla usług HTTP, FTP, Gopher i WAIS.

Serwer proxy przechowuje strony WWW zwracane na żądania wszystkich swoich użytkowników. W konsekwencji, gdy użytkownicy żądają strony WWW, serwer proxy sprawdza, czy strona jest już w pamięci podręcznej. Jeśli tak, serwer proxy zwraca stronę z pamięci podręcznej. Dzięki przechowywaniu stron w pamięci podręcznej serwer proxy szybciej obsługuje żądania WWW, eliminując potencjalnie czasochłonne żądania skierowane do serwera WWW.

Serwer proxy może również protokołować wszystkie żądania adresów URL. Protokołów można używać do monitorowania właściwego i niewłaściwego użytkowania zasobów sieciowych.

Aby skonsolidować dostęp do WWW, można także użyć obsługi proxy HTTP wbudowanej w IBM HTTP Server. Adresy komputerów PC klientów są ukryte przed serwerami WWW, mają one jedynie dostęp do serwera proxy. Umieszczanie stron WWW w pamięci podręcznej może również obniżyć wymagania co do przepustowości komunikacji i obciążenia firewallu. Więcej informacji na temat IBM HTTP Server dla iSeries znajduje się na stronie domowej, pod adresem: http://www-1.ibm.com/servers/eserver/iseries/software/http/index.html

Virtual Private Networking (VPN)

Sieć VPN umożliwia przedsiębiorstwu bezpieczne rozszerzenie prywatnego intranetu do istniejących struktur sieci publicznej, jaką jest Internet. Dzięki VPN firma może sterować ruchem w sieci przy jednoczesnym zapewnieniu ważnych opcji zabezpieczających, takich jak uwierzytelnianie i ochrona danych.

Program OS/400 VPN jest komponentem iSeries Navigator instalowanym opcjonalnie i stanowi graficzny interfejs użytkownika (GUI) systemu OS/400. Umożliwia utworzenie bezpiecznej ścieżki typu end-to-end pomiędzy hostem a gateway. Program OS/400 VPN wykorzystuje metody uwierzytelniania, algorytmy szyfrowania i inne zabezpieczenia zapewniające, że dane przesłane pomiędzy dwoma punktami końcowymi pozostają bezpieczne.

VPN uruchamiany jest w warstwie sieciowej protokołu TCP/IP. Wykorzystuje on otwartą strukturę IP Security Architecture. Architektura IPSec dotarcza zarówno podstawowe funkcje ochrony sieci Internet, jak i możliwość elastycznego tworzenia stabilnych, bezpiecznych wirtualnych sieci prywatnych.

VPN dodatkowo obsługuje rozwiązania protokołu Layer 2 Tunnel Protocol (L2TP) VPN. Połączenia L2TP, zwane również liniami wirtualnymi, dostarczają efektywnego dostępu do zdalnych użytkowników dzięki możliwości zarządzania sieciowym serwerem przedsiębiorstwa poprzez adresy IP przypisane do zdalnych użytkowników. Dodatkowo połączenia L2TP umożliwiają bezpieczny dostęp do systemu lub sieci, jeśli są chronione przez IPSec.

Ważne jest zrozumienie wpływu jaki, VPN będzie wywierał na całą sieć. Odpowiednie zaplanowanie i implementacja są kluczem do powodzenia. Należy przeglądnąć tematy związane z VPN w Centrum informacyjnym iSeries w celu upewnienia się o posiadaniu wiedzy na temat jak VPN działa i jak należy go używać. Więcej informacji na ten temat znajduje się w Centrum informacyjnym iSeries—Ochrona—>Virtual Private Networking. Informacje na temat dostępu do Centrum informacyjnego iSeries zawiera sekcja “Informacje wstępne i pokrewne” na stronie xii.

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) stał się standardem przemysłowym umożliwiającym bezpieczne komunikowanie się aplikacji poprzez niechronioną sieć jaką jest Internet. Protokół SSL ustanawia bezpieczne połączenie pomiędzy klintami i serwerem aplikacji, które wymaga uwierzytelnienia po jednej, lub po obydwu stronach sesji. SSL zapewnia również prywatność oraz integralność danych wymienianych przez klienta i serwer. Więcej informacji na ten temat znajduje się w Centrum informacyjnym iSeries–>Ochrona—>Secure Sockets Layer (SSL). Informacje na temat dostępu do Centrum informacyjnego iSeries zawiera sekcja “Informacje wstępne i pokrewne” na stronie xii.

Bezpieczne środowisko TCP/IP

W tej sekcji przedstawiono zalecane czynności, których wykonanie pozwoli zredukować zagrożenia dla bezpieczeństwa w systemowym środowisku TCP/IP. Wskazówki te odnoszą się kompleksowo do środowiska TPC/IP, a nie do konkretnych aplikacji, które omówiono w dalszych sekcjach.

- Tworząc aplikację dla portu TCP/IP, należy upewnić się, że jest ona odpowiednio chroniona. Należy założyć, że użytkownik zewnętrzny będzie próbował uzyskać dostęp do aplikacji poprzez ten port. Zaawansowany użytkownik może próbować dostępu do tej aplikacji poprzez port TELNET.
- Konieczne jest monitorowanie wykorzystania portów TCP/IP w systemie. Aplikacja użytkownika powiązana z portem TCP/IP może udostępnić “tylne wejście” do systemu bez konieczności podania identyfikatora użytkownika, czy hasła. Każdy użytkownik, który ma wystarczające uprawnienia w systemie, może powiązać aplikację z portem TCP lub UDP.
- Administrator ochrony powinien znać stosowaną przez hakerów technikę zwaną *fałszowaniem IP*. Każdy system w sieci TCP/IP ma adres IP. Osoba fałszująca IP konfiguruje system (zwykle komputer PC), tak aby udawał maszynę o istniejącym lub zaufanym adresie IP. W ten sposób oszust, udając system, z którym system lokalny łączy się normalnie, może połączyć się z systemem lokalnym.

  Systemy działające w sieciach, które nie są zabezpieczone fizycznie (wszystkie linie niekomutowane i wstępnie zdefiniowane dowiązania), narażone są na próby fałszowania adresów IP. Aby zabezpieczyć system przed uszkodzeniem przez “fałszerza”, należy zastosować sugestie opisane w tym rozdziale: ochronę wpisania się do systemu i ochronę obiektów. Ponadto należy upewnić się, że w systemie ustawione zostały rozsądne

ograniczenia pamięci dyskowej. Uniemożliwi to fałszerzowi zalanie systemu pocztą lub plikami buforowanymi w stopniu powodującym utratę zdolności systemu do działania.

Konieczne jest ponadto regularne monitorowanie aktywności TCP/IP w systemie. W przypadku wykrycia przypadków fałszowania IP należy spróbować zlokalizować słabe punkty w konfiguracji TCP/IP i dokonać poprawek.

- Dla celów intranetu (sieci lub systemów, które nie muszą bezpośrednio kontaktować się ze światem zewnętrznym) należy używać adresów IP, które mogą być wykorzystane wielokrotnie. Adresy wykorzystywane wielokrotnie są przeznaczone do użycia w sieciach prywatnych. Sieć szkieletowa Internetu nie kieruje pakietów mających adresy IP wielokrotnego użycia. Dlatego adresy te udostępniają dodatkową warstwę ochronną w obszarze objętym ochroną przez firewall.

  Więcej informacji na temat zarówno sposobu przypisywania adresów IP i ich zakresów, jak i informacje dotyczące ochrony TCP/IP znajdują się na stronie WWW Centrum informacyjnego iSeries —>Sieć—>TCP/IP.
- Decydując się na podłączenie systemu do Internetu lub intranetu, należy zapoznać się z informacjami o ochronie zawartymi w publikacji *SecureWay: iSeries i Internet* (Centrum informacyjne iSeries —>Security—>SecureWay). Informacje na temat dostępu do Centrum informacyjnego iSeries zawiera sekcja “Informacje wstępne i pokrewne” na stronie xii.

Kontrolowanie automatycznego uruchamiania serwerów TCP/IP

Administrator ochrony powinien kontrolować, które aplikacje TCP/IP są automatycznie uruchamiane po rozpoczęciu przetwarzania TCP/IP. Do uruchamiania przetwarzania TCP/IP służą dwie komendy. Dla każdej z nich system używa innej metody określenia, które aplikacje (serwery) mają zostać uruchomione.

Tabela 22 przedstawia obydwie komendy wraz z zaleceniami dotyczącymi bezpieczeństwa dla każdej z nich. Tabela 23 na stronie 119 przedstawia natomiast domyślne wartości autostartu dla serwerów. Aby zmienić wartości autostartu, należy użyć komendy CHGxxxA (Change xxx Attributes - Zmiana atrybutów xxx) dla danego serwera. Na przykład dla serwera TELNET odpowiednią komendą jest CHGTELNA.

Tabela 22. Komendy TCP/IP określające, które serwery TCP/IP mają zostać uruchomione

Komenda	**Które serwery mają zostać uruchomione**	**Zalecenia dotyczące ochrony**
Uruchomienie TCP/IP (Start TCP/IP - STRTCP)	System uruchamia każdy serwer z parametrem AUTOSTART(*YES). Tabela 23 na stronie 119 pokazuje ustawienia, z jakimi dostarczone zostały serwery TCP/IP.	• Ostrożnie przypisuj uprawnienia specjalne *IOSYSCFG, aby kontrolować osoby mogące zmieniać ustawienia autostartu. • Dokładnie sprawdź, kto ma uprawnienia do używania komendy STRTCP. Domyślne uprawnienia publiczne do tej komendy to *EXCLUDE. • Skonfiguruj kontrolowanie obiektów dla komend Zmiana atrybutów *nazwa serwera* (Change *nazwa serwera* Attributes), takich jak CHGTELNA, aby monitorować użytkowników próbujących zmieniać wartości parametru AUTOSTART dla serwera.

Tabela 22. Komendy TCP/IP określające, które serwery TCP/IP mają zostać uruchomione (kontynuacja)

Komenda	Które serwery mają zostać uruchomione	Zalecenia dotyczące ochrony
Uruchomienie serwera TCP/IP (Start TCP/IP Server - STRTCPSVR)	Aby określić serwery, które mają zostać uruchomione, należy użyć parametru. Komenda ta jest dostarczana z ustawieniem domyślnym uruchamiającym wszystkie serwery.	• Aby skonfigurować komendę STRTCPSVR, tak aby uruchamiała tylko określony serwer, użyj komendy Zmiana wartości domyślnych komendy (Change Command Default - CHGCMDDFT). Nie uniemożliwia to jednak użytkownikom uruchamiania innych serwerów. Zmiana wartości domyślnych komendy zmniejsza natomiast prawdopodobieństwo przypadkowego uruchomienia wszystkich serwerów. Aby na przykład zmienić wartość domyślną, tak aby uruchamiany był tylko serwer TELNET, użyj następującej komendy: CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)') **Uwaga:** Przy zmianie wartości domyślnej można określić tylko jeden serwer. Należy wybrać serwer używany regularnie lub taki, który stwarza najmniejsze zagrożenie dla bezpieczeństwa (na przykład TFTP). • Dokładnie sprawdź, kto ma uprawnienia do używania komendy STRTCPSVR. Domyślne uprawnienia publiczne do tej komendy to *EXCLUDE.

W poniższej tabeli znajdują się wartości startowe dla serwerów TCP/IP. Więcej informacji na temat każdego z serwerów znajduje się w Centrum informacyjnym iSeries (**Sieć—>TCP/IP**). Informacje na temat dostępu do Centrum informacyjnego iSeries (patrz "Informacje wstępne i pokrewne" na stronie xii).

Tabela 23. Wartości startowe dla serwerów TCP/IP

Serwer	Wartość domyślna	Wartość bieżąca
TELNET	AUTOSTART(*YES)	
FTP (file transfer protocol)	AUTOSTART(*YES)	
BOOTP (protokół Bootstrap)	AUTOSTART(*NO)	
TFTP (trivial file transfer protocol)	AUTOSTART(*NO)	
REXEC (Remote EXECution server)	AUTOSTART(*NO)	
RouteD (Route Daemon)	AUTOSTART(*NO)	
SMTP (simple mail transfer protocol)	AUTOSTART(*YES)	
POP (Post Office Protocol)	AUTOSTART(*NO)	
HTTP (Hypertext Transfer Protocol) [1]	AUTOSTART(*NO)	
ICS (Internet Connection Server)[1]	AUTOSTART(*NO)	
LPD (line printer daemon)	AUTOSTART(*YES)	
SNMP (Simple Network Management Protocol (SNMP))	AUTOSTART(*YES)	
DNS (domain name system)	AUTOSTART(*NO)	
DDM	AUTOSTART(*NO)	
DHCP (dynamic host configuration protocol)	AUTOSTART(*NO)	
NSMI	AUTOSTART(*NO)	
INETD	AUTOSTART(*NO)	

Tabela 23. Wartości startowe dla serwerów TCP/IP (kontynuacja)

Serwer	Wartość domyślna	Wartość bieżąca
Uwagi: 1. W serwerze IBM HTTP Server for iSeries, aby ustawić wartość AUTOSTART, można skorzystać z komendy CHGHTTPA.		

Bezpieczne używanie protokołu SLIP

Obsługa TCP/IP w serwerze iSeries obejmuje również Serial Line Interface Protocol (SLIP). Protokół SLIP udostępnia tanią łączność typu punkt z punktem. Użytkownik protokołu SLIP może połączyć się z siecią LAN lub WAN, ustanawiając z systemem, który jest częścią sieci LAN lub WAN, połączenie typu punkt z punktem.

Protokół SLIP działa przy połączeniach asynchronicznych. Można go używać w przypadku połączeń modemowych przychodzących do serwera iSeries i wychodzących z niego. Używając protokołu SLIP można na przykład połączyć komputer PC z systemem iSeries. Po nawiązaniu połączenia na komputerze PC można uruchomić klienta TELNET, aby połączyć się z serwerem TELNET w systemie iSeries. Można także użyć aplikacji FTP do przesłania plików pomiędzy tymi dwoma systemami.

W dostarczanym systemie protokół SLIP nie jest skonfigurowany. Dlatego jeśli protokół SLIP (ani połączenia modemowe TCP/IP) nie będzie używany w systemie, nie ma potrzeby tworzenia żadnych profili konfiguracyjnych SLIP. Aby utworzyć konfiguracje protokołu SLIP, należy użyć komendy Praca z połączeniami modemowymi TCP/IP (Work with TCP/IP Point-to-Point - WRKTCPPTP). Aby używać komendy WRKTCPPTP, należy mieć uprawnienia *IOSYSCFG.

Aby używać w systemie protokołu SLIP, należy utworzyć jeden lub kilka profili konfiguracyjnych SLIP (punkt z punktem). Można utworzyć profile konfiguracyjne z następującymi trybami pracy:
- odbieranie (*ANS),
- wybieranie (*DIAL).

W poniższych sekcjach omówiono konfigurowanie ochrony dla profili konfiguracyjnych SLIP.

Uwaga: **Profil użytkownika** jest obiektem serwera systemu iSeries, umożliwiającym wpisanie się do systemu. Każde zadanie w serwerze iSeries musi mieć profil użytkownika, aby mogło zostać uruchomione. **Profil konfiguracyjny** przechowuje dane używane podczas nawiązywania połączenia SLIP z systemem iSeries. Uruchomienie połączenia SLIP z serwerem iSeries oznacza jedynie ustanowienie łącza. Nie powoduje natomiast wpisania się do serwera iSeries i uruchomienia w nim zadania. Dlatego do uruchomienia połączenia SLIP z serwerem iSeries nie jest konieczny profil użytkownika. Profil konfiguracyjny SLIP może jednak wymagać profilu użytkownika do określenia, czy połączenie jest dozwolone. Zostanie to opisane w dalszej części.

Kontrolowanie przychodzących połączeń SLIP

Zanim ktokolwiek będzie mógł nawiązać połączenie SLIP z systemem lokalnym, należy uruchomić profil konfiguracyjny SLIP *ANS. Aby utworzyć lub zmienić profile konfiguracyjne SLIP, należy użyć komendy Praca z połączeniami modemowymi TCP/IP (Work with TCP/IP Point-to-Point - WRKTCPPTP). Do uruchamiania profilu konfiguracyjnego służy komenda Uruchomienie połączenia modemowego TCP/IP (Start TCP/IP Point-to-Point - STRTCPPTP) lub opcja ekranu WRKTCPPTP. W dostarczanym

systemie uprawnienie publiczne do komend STRTCPPTP i ENDTCPPTP ma wartość *EXCLUDE. Opcje dodawania, zmiany i usuwania profili konfiguracyjnych SLIP są dostępne tylko dla użytkowników z uprawnieniami specjalnymi *IOSYSCFG. Administrator ochrony może stosować zarówno uprawnienia do komend, jak i uprawnienia specjalne w celu określenia użytkowników, którzy mogą konfigurować system, tak aby dozwolone było odbieranie połączeń przychodzących.

Ochrona przychodzących połączeń SLIP

Aby sprawdzić system, który próbuje połączyć się z systemem lokalnym, należy spowodować, aby system wywołujący przesłał identyfikator użytkownika i hasło. System lokalny będzie mógł je wówczas zweryfikować. Jeśli identyfikator użytkownika i hasło nie są poprawne, system lokalny może odrzucić żądanie sesji.

Aby skonfigurować sprawdzanie poprawności przy odbieraniu połączeń, wykonaj następujące czynności:

__ Krok 1. Utwórz profil użytkownika, który będzie używany przez system wywołujący przy nawiązywaniu połączenia. Identyfikator użytkownika i hasło wysyłane przez system wywołujący muszą być zgodne z nazwą i hasłem dla tego profilu.

Uwaga: Aby system wykonał potwierdzenie hasła, wartość systemowa QSECURITY musi wynosić 20 lub więcej.

Dodatkowym zabezpieczeniem będzie utworzenie profili użytkownika dedykowanych do połączeń SLIP. Profile takie powinny mieć ograniczone uprawnienia w systemie. Jeśli nie będą one spełniać żadnych innych funkcji poza nawiązywaniem połączeń SLIP, to poniższym parametrom tych profili można nadać następujące wartości:

- Menu początkowe (INLMNU) - *SIGNOFF,
- Program początkowy (INLPGM) - *NONE,
- Ograniczenie możliwości (LMTCPB) - *YES.

Wartości te uniemożliwią interaktywne wpisanie się do systemu z takim profilem użytkownika.

__ Krok 2. Utwórz listę autoryzacji dla systemu, która będzie sprawdzana, gdy system wywołujący będzie próbował nawiązać połączenie SLIP.

Uwaga: Lista autoryzacji jest określana w polu *Lista autoryzacji dostępu do systemu (System access authorization list)* podczas tworzenia lub zmiany profilu SLIP. (Patrz krok 4).

__ Krok 3. Aby dodać utworzony w kroku 1 profil użytkownika do listy autoryzacji, użyj komendy Dodanie pozycji listy autoryzacji (Add Authorization List Entry - ADDAUTLE). Możesz utworzyć unikalne listy autoryzacji osobno dla każdego profilu konfiguracyjnego połączenia punkt z punktem lub wspólną listę używaną przez kilka profili.

__ Krok 4. Użyj komendy WRKTCPPTP, aby zdefiniować profil połączenia TCP/IP *ANS o następujących charakterystykach:

- Profil połączenia musi używać skryptu dialogowego obejmującego funkcję potwierdzenia użytkownika. Potwierdzenie użytkownika obejmuje akceptację identyfikatora i hasła użytkownika z systemu wywołującego oraz sprawdzenie ich poprawności. System jest dostarczany z kilkoma przykładowymi skryptami dialogowymi, które udostępniają tę funkcję.
- Profil konfiguracyjny musi określać nazwę listy autoryzacji utworzonej w kroku 2. Z kolei odebrany przez skrypt dialogowy identyfikator użytkownika musi znajdować się na liście autoryzacji.

Należy wziąć pod uwagę, że na stopień ochrony profilu odbierającego ma także wpływ ochrona stosowana w systemie nawiązującym połączenie. Jeśli w systemie lokalnym wymagane jest podanie identyfikatora użytkownika i hasła, to skrypt dialogowy połączenia na systemie wywołującym musi wysyłać te dane. Niektóre systemy, w tym serwery iSeries, udostępniają bezpieczną metodę przechowywania identyfikatorów i haseł użytkowników. (Sekcja "Ochrona i sesje połączeń wychodzących" zawiera opis tej metody). W innych systemach identyfikator i hasło użytkownika są przechowywane w skrypcie, który może być dostępny dla każdego, kto wie, gdzie w systemie znajdują się skrypty.

Z uwagi na różnice w praktycznym stosowaniu ochrony przez partnerów komunikacyjnych oraz różnice w możliwościach tej ochrony, może być wskazane utworzenie różnych profili konfiguracyjnych dla różnych środowisk wywołujących. Za pomocą komendy STRTCPPTP można skonfigurować system, tak aby akceptował sesję dla konkretnego profilu konfiguracyjnego. Można na przykład uruchamiać sesje dla niektórych profili konfiguracyjnych tylko w określonych godzinach. Do protokołowania aktywności powiązanych profili użytkownika można użyć kontroli ochrony.

Uniemożliwianie zdalnym użytkownikom dostępu do innych systemów

W zależności od systemu lokalnego i konfiguracji sieci, użytkownik, który uruchomił połączenie SLIP, może mieć dostęp do innych systemów w sieci lokalnej, bez wpisania się do systemu. Na przykład użytkownik po nawiązaniu połączenia SLIP z systemem lokalnym, może nawiązać połączenie FTP z innymi systemami w sieci lokalnej, które nie zezwalają na odbieranie połączeń modemowych.

Wpisując N (Nie) w polu *Zezwól na przekazywanie datagramów IP (Allow IP datagram forwarding)* w profilu konfiguracyjnym, można zablokować dostęp użytkowników połączeń SLIP do innych systemów w sieci lokalnej. Blokada ta uniemożliwia dostęp do sieci tylko użytkownikom, którzy nie zalogowali się systemie. Jednak po pomyślnym zalogowaniu się użytkownika w systemie, przekazywanie datagramów nie ma znaczenia. Nie ogranicza ono możliwości użycia aplikacji TCP/IP (na przykład FTP czy TELNET) w systemie iSeries do nawiązywania połączenia z innym systemem w sieci.

Sterowanie sesjami połączeń wychodzących

Zanim będzie można użyć protokołu SLIP do nawiązywania połączeń wychodzących z systemu lokalnego, należy uruchomić profil konfiguracyjny SLIP *DIAL. Aby utworzyć lub zmienić profil konfiguracyjny SLIP, należy użyć komendy WRKTCPPTP. Do uruchamiania profilu konfiguracyjnego służy komenda Uruchomienie połączenia modemowego TCP/IP (Start TCP/IP Point-to-Point - STRTCPPTP) lub opcja ekranu WRKTCPPTP. W dostarczanym systemie uprawnienie publiczne do komend STRTCPPTP i ENDTCPPTP ma wartość *EXCLUDE. Opcje dodawania, zmiany i usuwania profili konfiguracyjnych SLIP są dostępne tylko dla użytkowników z uprawnieniami specjalnymi *IOSYSCFG. Administrator ochrony może stosować zarówno uprawnienia do komend, jak i uprawnienia specjalne w celu określenia użytkowników, którzy mogą konfigurować system, tak aby dozwolone było nawiązywanie połączeń wychodzących.

Ochrona i sesje połączeń wychodzących

Może się zdarzyć, że użytkownicy danego systemu iSeries będą chcieli nawiązać połączenie modemowe z systemem, który wymaga potwierdzenia użytkownika. Skrypt dialogowy połączenia w serwerze iSeries musi wówczas przesłać identyfikator i hasło użytkownika do systemu zdalnego. Serwer iSeries udostępnia bezpieczną metodę przechowywania hasła. Nie jest ono przechowywane w skrypcie dialogowym połączenia.

Uwagi:

1. Choć system przechowuje hasło połączenia w postaci zaszyfrowanej, to przed przesłaniem musi je zdeszyfrować. W przypadku połączeń SLIP, podobnie jak przy

połączeniach FTP i TELNET, hasła są przesyłane w postaci niezaszyfrowanej (“otwartym tekstem”). Jednak odmiennie niż w przypadku połączeń FTP i TELNET, hasło w połączeniu SLIP jest przesyłane przed przejściem obydwu systemów w tryb TCP/IP.

Ponieważ protokół SLIP używa asynchronicznego połączenia typu punkt z punktem, zagrożenie dla bezpieczeństwa podczas przesyłania niezaszyfrowanego hasła jest inne niż w przypadku haseł połączeń FTP i TELNET. Niezaszyfrowane hasła połączeń FTP i TELNET mogą być przesyłane w sieci jako ruch pakietów IP, przez co narażone są na podsłuch elektroniczny. Transmisja hasła połączenia SLIP jest tak bezpieczna, jak połączenie telefoniczne pomiędzy obydwoma systemami.

2. Domyślnym plikiem, w którym przechowywany jest skrypt dialogowy połączenia SLIP, jest QUSRSYS/QATOCPPSCR. Uprawnienia publiczne do tego pliku to *USE. Uniemożliwiają one użytkownikom publicznym zmianę domyślnych dialogowych skryptów połączenia.

Podczas tworzenia profilu połączenia dla sesji zdalnej wymagającej potwierdzenia wykonaj poniższe czynności:

__ Krok 1. Upewnij się, że wartość systemowa Zachowaj dane ochrony serwera (Retain Server Security Data - QRETSVRSEC) jest równa 1 (Tak). Wartość ta decyduje, czy dozwolone będzie przechowywanie zdeszyfrowanych haseł w zabezpieczonym obszarze systemu lokalnego.

__ Krok 2. Użyj komendy WRKTCPPTP, aby zdefiniować profil konfiguracyjny o następujących charakterystykach:

- Podaj *DIAL jako tryb pracy profilu konfiguracyjnego.
- W polu *Nazwa dostępu do usługi zdalnej* wpisz identyfikator użytkownika, którego oczekuje zdalny system. Łącząc się na przykład z innym serwerem iSeries, podaj nazwę profilu użytkownika w tym serwerze iSeries.
- W polu *Hasło dostępu do usługi zdalnej* wpisz hasło, które w zdalnym systemie odpowiada danemu identyfikatorowi użytkownika. W lokalnym serwerze iSeries hasło to jest przechowywane w obszarze zabezpieczonym, w postaci, która może być zdeszyfrowana. Podane nazwy i hasła przypisane profilowi konfiguracyjnemu są powiązane z profilem użytkownika QTCP. Nie są one dostępne dla użytkownika poprzez żadne komendy ani interfejsy. Tylko zarejestrowane programy systemowe mają dostęp do tych informacji o hasłach.

  Uwaga: Należy mieć na uwadze, że hasła dla profili konfiguracyjnych nie są składowane podczas składowania profili konfiguracyjnych TCP/IP. W celu składowania haseł połączeń SLIP do składowania profilu QTCP należy użyć komendy Składowanie danych ochrony (Save Security Data - SAVSECDTA).
- Jako skrypt dialogowy połączenia podaj skrypt, który wysyła identyfikator i hasło użytkownika. System jest dostarczany z kilkoma przykładowymi skryptami dialogowymi, które udostępniają tę funkcję. System, wykonując skrypt, wczytuje hasło, deszyfruje je i przesyła do systemu zdalnego.

Bezpieczne używanie protokołu PPP (Point-to-Point Protocol)

Protokół PPP (point-to-point protocol) jest dostępny jako część protokołu TCP/IP. Protokół PPP jest standardem przemysłowym dla połączeń typu punkt z punktem i udostępnia dodatkową funkcję w porównaniu z protokołem SLIP.

Dzięki protokołowi PPP serwer iSeries może nawiązywać szybkie połączenia bezpośrednio z dostawcą usług internetowych lub z innymi systemami w sieci intranet lub ekstranet. Zdalne sieci LAN rzeczywiście mogą inicjować połączenia z lokalnym serwerem iSeries.

Należy pamiętać, że protokół PPP, podobnie jak protokół SLIP, udostępnia sieciowe połączenia z lokalnym serwerem iSeries. Można powiedzieć, że połączenie PPP w zasadzie doprowadza system wywołujący do bram systemu lokalnego. Użytkownik systemu wywołującego musi w dalszym ciągu podawać identyfikator użytkownika i hasło, aby dostać się do systemu i połączyć z serwerem TCP/IP, takim jak TELNET lub FTP. Poniżej przedstawiono zagadnienia dotyczące ochrony związane z tą nową możliwością nawiązywania połączeń:

Uwaga: Protokół PPP konfiguruje się za pomocą programu iSeries Navigator na stacji roboczej IBM iSeries Access for Windows.

- Protokół PPP udostępnia połączenia dedykowane (ten sam użytkownik ma zawsze taki sam adres IP). W przypadku adresów dedykowanych potencjalnym zagrożeniem dla bezpieczeństwa może być fałszowanie adresu IP (próby połączenia z systemem o adresie IP zmienionym na adres IP systemu zaufanego). Jednakże rozszerzone możliwości uwierzytelniania udostępniane przez protokół PPP umożliwiają zabezpieczenie się przed fałszowaniem adresu IP.
- W przypadku protokołu PPP, podobnie jak w przypadku protokołu SLIP, można tworzyć profile połączeń posiadające nazwę użytkownika i powiązane hasło. Użytkownik jednak nie musi mieć poprawnego profilu użytkownika ani hasła. Ani nazwa użytkownika, ani hasło nie są powiązane z profilem użytkownika. Zamiast tego do uwierzytelniania używana jest lista autoryzacji. Ponadto protokół PPP nie wymaga skryptu połączenia. Uwierzytelnianie (wymienianie nazwy i hasła użytkownika) jest elementem architektury PPP i odbywa się na poziomie niższym niż w przypadku protokołu SLIP.
- W przypadku protokołu PPP użytkownik może opcjonalnie skorzystać z protokołu CHAP (challenge handshake authentication protocol). Ponieważ protokół CHAP szyfruje nazwy i hasła użytkowników, nie ma potrzeby obawiać się osób, które chcą podsłuchać hasło.

  Połączenie PPP używa protokołu CHAP tylko wtedy, gdy obydwa systemy go obsługują. Podczas wymiany sygnałów w celu nawiązania komunikacji pomiędzy modemami odbywają się także negocjacje pomiędzy obydwoma systemami. Jeśli na przykład SYSTEMA obsługuje CHAP a SYSTEMB nie, SYSTEMA może albo odmówić sesji, albo zgodzić się na niezaszyfrowaną nazwę użytkownika i hasło. Zgoda na używanie niezaszyfrowanej nazwy i hasła nazywa się negocjowaniem w dół. Decyzja o negocjowaniu w dół zależy od opcji konfiguracyjnej. Na przykład dla sieci intranet, w której wszystkie systemy obsługują protokół CHAP, należy tak skonfigurować profil połączenia, aby nie dopuszczał on negocjowania w dół. W przypadku połączeń publicznych, kiedy system nawiązuje połączenie wychodzące, można dopuścić negocjowanie w dół.

  Profil połączenia PPP udostępnia możliwość określenia poprawnych adresów IP. Można na przykład wskazać konkretny adres lub zakres adresów dla konkretnego użytkownika. Ta możliwość wraz z możliwością szyfrowania haseł stanowi kolejny stopień ochrony przed oszustwami.

  Dodatkowym zabezpieczeniem aktywnej sesji przed fałszowaniem lub próbami wejścia do systemu może być takie skonfigurowanie protokołu PPP, aby powtarzał on wezwanie do uwierzytelnienia w określonych odstępach czasu. W przypadku aktywnej sesji PPP lokalny system może wzywać inne systemy do przedstawienia identyfikatora i hasła użytkownika. Może to robić co 15 minut, aby upewnić się, że jest to wciąż ten sam profil połączenia. (Użytkownik końcowy nie zauważy czynności ponownego wzywania, systemy wymieniają nazwy i hasła poniżej poziomu widocznego dla użytkownika końcowego).

  W przypadku protokołu PPP można oczekiwać, że zdalne sieci LAN będą mogły nawiązywać połączenia modemowe z lokalnym serwerem iSeries oraz z siecią rozległą. W takim środowisku prawdopodobnie niezbędne jest włączenie przekazywania IP. Stwarza to jednak potencjalne możliwości penetracji sieci przez intruzów. Jednak protokół PPP wyposażony jest w mocniejsze zabezpieczenia (na przykład szyfrowanie haseł lub

potwierdzanie adresów IP). Przede wszystkim zmniejszają one prawdopodobieństwo nawiązania połączenia sieciowego przez osoby niepożądane.

Więcej informacji o protokole PPP znajduje się w Centrum informacyjnym iSeries..

Bezpieczne używanie serwera protokołu Bootstrap

Protokół Bootstrap (BOOTP) udostępnia dynamiczną metodę powiązania stacji roboczych z serwerami i przypisywania stacjom roboczym adresów IP oraz źródeł ładowania programu początkowego (IPL).

Protokół BOOTP jest protokołem TCP/IP umożliwiającym stacjom roboczym bez nośników (klientom) realizację żądania pobrania z serwera sieciowego pliku zawierającego kod początkowy. Serwer BOOTP nasłuchuje, wykorzystując ogólnie znany port serwera BOOTP nr 67. Po odebraniu żądania klienta system znajduje adres IP zdefiniowany dla klienta i zwraca odpowiedź z adresem IP i nazwą pliku do załadowania. Następnie klient inicjuje żądanie TFTP do serwera w celu załadowania pliku. W tabeli BOOTP, w serwerze iSeries przechowywane jest odwzorowanie adresu sprzętowego klienta na adres IP.

Zabezpieczenie przed dostępem do serwera BOOTP

Jeśli żadna stacja typu thin client nie jest przyłączana do lokalnej sieci, nie ma potrzeby uruchamiania serwera BOOTP. Można go również używać dla innych urządzeń, ale zaleca się raczej zastosowanie protokołu DHCP. Aby zablokować działanie serwera BOOTP, wykonaj następujące czynności:

__ Krok 1. Aby uniemożliwić automatyczne uruchamianie zadań serwera BOOTP podczas uruchamiania przetwarzania TCP/IP, wpisz:

```
CHGBPA AUTOSTART(*NO)
```

Uwagi:

1. Wartością domyślną jest AUTOSTART(*NO).
2. Sekcja “Kontrolowanie automatycznego uruchamiania serwerów TCP/IP” na stronie 118 zawiera więcej informacji dotyczących sterowania automatycznym uruchamianiem serwerów TCP/IP.

__ Krok 2. Aby uniemożliwić powiązanie aplikacji użytkownika, na przykład aplikacji używającej gniazda, z portem używanym normalnie przez system na potrzeby BOOTP, wykonaj poniższe czynności:

Uwaga: Ponieważ protokoły DHCP i BOOTP używają tego samego numeru portu, powyższa czynność uniemożliwi także korzystanie z DHCP. Jeśli protokół DHCP ma być używany, nie należy ograniczać dostępu do portu.

__ Krok a. Wpisz GO CFGTCP, aby wyświetlić menu Konfigurowanie TCP/IP (Configure TCP/IP).

__ Krok b. Wybierz opcję 4 (Praca z ograniczeniami portu TCP/IP).

__ Krok c. Na ekranie Praca z ograniczeniami portu TCP/IP (Work with TCP/IP Port Restrictions) wybierz opcję 1 (Dodaj).

__ Krok d. Jako dolny zakres portu podaj 67.

__ Krok e. Jako górny zakres portu podaj *ONLY.

Uwagi:

1. Ograniczenie dostępu do portu zostanie zastosowane przy następnym uruchomieniu TCP/IP. Jeśli przetwarzanie TCP/IP jest włączone podczas ograniczania dostępu do portu, należy je zakończyć i uruchomić ponownie.

2. RFC1700 udostępnia informacje o powszechnych przypisaniach numerów portów.

__ Krok f. Jako protokół podaj *UDP.

__ Krok g. W polu Profil użytkownika należy podać nazwę profilu użytkownika, który jest chroniony w systemie. (Zabezpieczony profil użytkownika to profil użytkownika, który nie jest właścicielem programów adoptujących uprawnienia i nie ma hasła znanego innym użytkownikom.) Ograniczając port do konkretnego użytkownika automatycznie wyłącza się wszystkich pozostałych użytkowników.

Ochrona serwera BOOTP

Ponieważ serwer protokołu BOOTP nie zapewnia bezpośredniego dostępu do systemu iSeries, wiąże się z nim niewielkie zagrożenie bezpieczeństwa. Podstawowym zadaniem administratora ochrony jest zapewnienie poprawnego powiązania informacji ze stacji typu thin client. (Zmiana w tabeli BOOTP może spowodować, że stacja typu thin client będzie pracowała niepoprawnie lub nie będzie pracowała w ogóle).

Aby administrować serwerem BOOTP i tabelą BOOTP, należy mieć uprawnienia specjalne *IOSYSCFG. Szczególną uwagę należy zwrócić na użytkowników posiadających uprawnienia specjalne *IOSYSCFG.

Bezpieczne używanie serwera DHCP

Serwer DHCP (Dynamic Host Configuration Protocol) udostępnia środowisko, w którym mogą być przesyłane informacje konfiguracyjne do hostów w sieci TCP/IP. Dla stacji roboczych klientów protokół DHCP udostępnia funkcje przypominające automatyczną konfigurację. Program z włączoną obsługą DHCP na stacji klienta rozsyła żądanie informacji konfiguracyjnych. Jeśli w lokalnym systemie iSeries działa serwer DHCP, odpowiada on na to żądanie, wysyłając informacje potrzebne klienckiej stacji roboczej do poprawnego skonfigurowania protokołu TCP/IP.

DHCP może ułatwiać użytkownikom pierwsze połączenie z serwerem iSeries. Dzięki niemu bowiem użytkownik nie musi wprowadzać informacji konfiguracyjnych protokołu TCP/IP. Serwer DHCP umożliwia także zmniejszenie liczby wewnętrznych adresów IP, potrzebnych w podsieci. Serwer DHCP może tymczasowo przydzielać adresy IP (ze swojej puli adresów IP) aktywnym użytkownikom.

W przypadku stacji typu thin client można użyć protokołu DHCP zamiast protokołu BOOTP. Protokół DHCP udostępnia więcej funkcji niż BOOTP i może obsługiwać dynamiczną konfigurację zarówno stacji typu thin client jak i komputerów PC.

Zabezpieczenie przed dostępem do serwera DHCP

Jeśli w systemie serwer DHCP ma być *niedostępny*, wykonaj następujące czynności:

1. Aby uniemożliwić automatyczne uruchamianie zadań serwera DHCP podczas uruchamiania przetwarzania TCP/IP, wpisz:

   ```
   CHGDHCPA AUTOSTART(*NO)
   ```

   Uwagi:

   1. Wartością domyślną jest AUTOSTART(*NO).
   2. Sekcja “Kontrolowanie automatycznego uruchamiania serwerów TCP/IP” na stronie 118 zawiera więcej informacji dotyczących sterowania automatycznym uruchamianiem serwerów TCP/IP.

2. Aby uniemożliwić powiązanie aplikacji użytkownika, na przykład aplikacji używającej gniazda, z portem używanym normalnie przez system na potrzeby DHCP, wykonaj poniższe czynności:
   a. Wpisz GO CFGTCP, aby wyświetlić menu Konfigurowanie TCP/IP (Configure TCP/IP).
   b. Wybierz opcję 4 (Praca z ograniczeniami portu TCP/IP).
   c. Na ekranie Praca z ograniczeniami portu TCP/IP (Work with TCP/IP Port Restrictions) wybierz opcję 1 (Dodaj).
   d. Jako dolny zakres portu podaj 67.
   e. Jako górny zakres portu podaj 68.

      Uwagi:

      1. Ograniczenie dostępu do portu zostanie zastosowane przy następnym uruchomieniu TCP/IP. Jeśli przetwarzanie TCP/IP jest włączone podczas ograniczania dostępu do portu, należy je zakończyć i uruchomić ponownie.
      2. RFC1700 udostępnia informacje o powszechnych przypisaniach numerów portów.

   f. Jako protokół podaj *UDP.
   g. W polu Profil użytkownika należy podać nazwę profilu użytkownika, który jest chroniony w systemie. (Zabezpieczony profil użytkownika to profil użytkownika, który nie jest właścicielem programów adoptujących uprawnienia i nie ma hasła znanego innym użytkownikom.) Ograniczając port do konkretnego użytkownika automatycznie wyłącza się wszystkich pozostałych użytkowników.

Ochrona serwera DHCP

Decydując się na uruchomienie w systemie iSeries serwera DHCP, należy uwzględnić następujące zagadnienia ochrony:

- Należy ograniczyć liczbę użytkowników, którzy mają uprawnienia do administrowania serwerem DHCP. Administrowanie serwerem DHCP wymaga następujących uprawnień:
  - uprawnienia specjalnego *IOSYSCFG,
  - uprawnienia *RW do następujących plików:

    ```
    /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
    /QIBM/UserData/OS400/DHCP/dhcprd.cfg
    ```
- Należy ocenić fizyczną dostępność lokalnej sieci LAN. Czy osoba z zewnątrz może łatwo dostać się na teren przedsiębiorstwa z laptopem i fizycznie podłączyć do sieci? Jeśli występuje takie zagrożenie, serwer DHCP umożliwia utworzenie listy klientów (adresy sprzętowe), którzy będą konfigurowani przez serwer DHCP. Używając tej funkcji zmniejsza się co prawda korzyści, jakie DHCP daje administratorom sieci. Jednak w ten sposób uniemożliwia się konfigurowanie nieznanych stacji roboczych.
- Jeśli to możliwe, należy używać puli adresów, które mogą być wykorzystane ponownie (nie są przeznaczone do Internetu). Pozwala to zabezpieczyć stacje robocze przed dostępem z zewnątrz i wyklucza możliwość przechwycenia i użycia informacji konfiguracyjnych z serwera.
- Dodatkowe zabezpieczenie dają punkty wyjścia DHCP. Poniżej przedstawiono przegląd punktów wyjścia i ich możliwości. W książce *iSeries System API Reference* opisano sposoby wykorzystania tych punktów wyjścia.

  Punkt wejścia do portu

  System wywołuje program obsługi wyjścia za każdym razem, gdy odczytuje pakiet danych z portu 67 (port DHCP). Program obsługi wyjścia otrzymuje pełen pakiet danych, a następnie decyduje, czy pakiet powinien być przetworzony przez system czy usunięty. Tego punktu wyjścia można użyć, gdy istniejące funkcje ekranujące DHCP nie spełniają wymagań.

Przypisanie adresu
System wywołuje program obsługi wyjścia za każdym razem, gdy serwer DHCP formalnie przypisuje klientowi adres.

Zwolnienie adresu
System wywołuje program obsługi wyjścia za każdym razem, gdy serwer DHCP formalnie zwalnia przypisany klientowi adres i umieszcza go z powrotem w puli adresów.

Bezpieczne używanie serwera TFTP

Serwer TFTP (Trivial file transfer protocol) umożliwia podstawowe przesyłanie plików bez uwierzytelniania użytkownika. Serwer TFTP współpracuje zarówno z protokołem protokół Bootstrap (BOOTP) jak i Dynamic Host Configuration Protocol (DHCP).

Klient łączy się na początkowo z serwerem BOOTP lub DHCP. Serwer BOOTP lub DHCP odpowiada, przesyłając adres IP stacji klienckiej i nazwę pliku do załadowania. Następnie klient inicjuje żądanie TFTP do serwera w celu załadowania pliku. Kiedy klient kończy pobieranie pliku ładowania, kończy również sesję TFTP.

Zabezpieczenie przed dostępem do serwera TFTP

Jeśli żadna stacja typu thin client nie jest przyłączana do lokalnej sieci, nie ma potrzeby uruchamiania serwera TFTP. Aby zablokować działanie serwera TFTP, wykonaj następujące czynności:

__ Krok 1. Aby uniemożliwić automatyczne uruchamianie zadań serwera TFTP podczas uruchamiania przetwarzania TCP/IP, wpisz:

```
CHGTFTPA AUTOSTART(*NO)
```

Uwagi:

1. Wartością domyślną jest AUTOSTART(*NO).
2. Sekcja “Kontrolowanie automatycznego uruchamiania serwerów TCP/IP” na stronie 118 zawiera więcej informacji dotyczących sterowania automatycznym uruchamianiem serwerów TCP/IP.

__ Krok 2. Aby uniemożliwić powiązanie aplikacji użytkownika, na przykład aplikacji używającej gniazda, z portem używanym normalnie przez system na potrzeby TFTP, wykonaj poniższe czynności:

__ Krok a. Wpisz GO CFGTCP, aby wyświetlić menu Konfigurowanie TCP/IP (Configure TCP/IP).

__ Krok b. Wybierz opcję 4 (Praca z ograniczeniami portu TCP/IP).

__ Krok c. Na ekranie Praca z ograniczeniami portu TCP/IP (Work with TCP/IP Port Restrictions) wybierz opcję 1 (Dodaj).

__ Krok d. Jako dolny zakres portu podaj 69.

__ Krok e. Jako górny zakres portu podaj *ONLY.

Uwagi:

1. Ograniczenie dostępu do portu zostanie zastosowane przy następnym uruchomieniu TCP/IP. Jeśli przetwarzanie TCP/IP jest włączone podczas ograniczania dostępu do portu, należy je zakończyć i uruchomić ponownie.
2. RFC1700 udostępnia informacje o powszechnych przypisaniach numerów portów.

__ Krok f. Jako protokół podaj *UDP.

__ Krok g. W polu Profil użytkownika należy podać nazwę profilu użytkownika, który jest chroniony w systemie. (Zabezpieczony profil użytkownika to profil użytkownika, który nie jest właścicielem programów adoptujących uprawnienia i nie ma hasła znanego innym użytkownikom.) Ograniczając port do konkretnego użytkownika automatycznie wyłącza się wszystkich pozostałych użytkowników.

Ochrona serwera TFTP

Domyślnie serwer TFTP umożliwia dostęp do lokalnego systemu iSeries w bardzo ograniczonym zakresie. Jest on skonfigurowany tak, aby udostępniać stacjom typu thin client kod początkowy. Administrator ochrony powinien znać przedstawione poniżej charakterystyki serwera TFTP:

- Serwer TFTP nie wymaga uwierzytelniania (identyfikatora użytkownika i hasła). Wszystkie zadania TFTP wykonywane są z profilem użytkownika QTFTP. Profil QTFTP nie ma hasła. Dlatego nie jest możliwe interaktywne wpisanie się. Profil QTFTP nie ma także żadnych specjalnych uprawnień, nie jest również uprawniony do zasobów systemowych. W celu uzyskania dostępu do zasobów stacji typu thin client profil ten używa uprawnień publicznych.
- Serwer TFTP jest dostarczany ze skonfigurowanym dostępem do katalogu zawierającego informacje dla stacji typu thin client. Do zapisu lub odczytu informacji w tym katalogu potrzebne są uprawnienia *PUBLIC lub QTFTP. Aby zapisywać dane w tym katalogu, parametr ″Zezwól na zapis do plików (Allow file writes)″ komendy CHGTFTPA musi mieć wartość *CREATE. Aby zapisywać dane w tym katalogu w istniejącym pliku, parametr ″Zezwól na zapis do plików (Allow file writes)″ komendy CHGTFTPA musi mieć wartość *REPLACE. Ustawienie *CREATE pozwala zastąpić istniejące pliki lub utworzyć nowe. Ustawienie *REPLACE umożliwia jedynie zastąpienie istniejących plików.

  Klient TFTP nie ma dostępu do żadnego innego katalogu, o ile dostęp taki nie zostanie mu przydzielony w sposób jawny komendą Zmiana atrybutów TFTP (Change TFTP Attributes - CHGTFTPA). Dlatego jeśli lokalny lub zdalny użytkownik podejmie próbę uruchomienia sesji TFTP w systemie lokalnym, jego możliwości dostępu do danych lub spowodowania awarii są bardzo ograniczone.
- Jeśli serwer TFTP zostanie skonfigurowany tak, aby udostępniać inne usługi oprócz obsługi stacji typu thin client, należy zdefiniować program obsługi wyjścia, który będzie oceniał i uwierzytelniał każde żądanie TFTP. Serwer TFTP udostępnia wyjście potwierdzenia żądania, podobnie jak serwer FTP. Więcej informacji na ten temat znajduje się w Centrum informacyjnym iSeries —>Sieci—>TCP/IP—>TFTP. Informacje na temat dostępu do Centrum informacyjnego iSeries zawiera sekcja “Informacje wstępne i pokrewne” na stronie xii.

Bezpieczne używanie serwera REXEC

Program Remote EXECution server (REXEC) otrzymuje i uruchamia komendy klienta REXEC. Klient REXEC to zazwyczaj aplikacja PC lub UNIX, która obsługuje wysyłanie komend REXEC. Obsługa zapewniana przez ten serwer jest pod względem możliwości podobna do użycia podkomendy RCMD (Remote Command - komenda zdalna) dla serwera FTP.

Zabezpieczenie przed dostępem serwera REXEC

Aby zablokować działanie serwera REXEC i uniemożliwić systemowi iSeries akceptowanie komend od klienta REXEC, należy wykonać poniższe kroki:

__ Krok 1. Aby uniemożliwić automatyczne uruchamianie zadań serwera REXEC podczas uruchamiania przetwarzania TCP/IP, wpisz:

```
CHGRXCA AUTOSTART(*NO)
```

Uwagi:

1. Wartością domyślną jest AUTOSTART(*NO).
2. Sekcja “Kontrolowanie automatycznego uruchamiania serwerów TCP/IP” na stronie 118 zawiera więcej informacji dotyczących sterowania automatycznym uruchamianiem serwerów TCP/IP.

__ Krok 2. Aby uniemożliwić powiązanie aplikacji użytkownika, na przykład aplikacji używającej gniazda, z portem używanym normalnie przez system dla serwera REXEC, wykonaj poniższe czynności:

__ Krok a. Wpisz GO CFGTCP, aby wyświetlić menu Konfigurowanie TCP/IP (Configure TCP/IP).

__ Krok b. Wybierz opcję 4 (Praca z ograniczeniami portu TCP/IP).

__ Krok c. Na ekranie Praca z ograniczeniami portu TCP/IP (Work with TCP/IP Port Restrictions) wybierz opcję 1 (Dodaj).

__ Krok d. Jako dolny zakres portu podaj 512.

__ Krok e. Jako górny zakres portu podaj *ONLY.

__ Krok f. Jako protokół podaj *TCP.

__ Krok g. W polu Profil użytkownika należy podać nazwę profilu użytkownika, który jest chroniony w systemie. (Zabezpieczony profil użytkownika to profil użytkownika, który nie jest właścicielem programów adoptujących uprawnienia i nie ma hasła znanego innym użytkownikom.) Ograniczając port do konkretnego użytkownika automatycznie wyłącza się wszystkich pozostałych użytkowników.

Uwagi:

1. Ograniczenie dostępu do portu zostanie zastosowane przy następnym uruchomieniu TCP/IP. Jeśli przetwarzanie TCP/IP jest włączone podczas ograniczania dostępu do portu, należy je zakończyć i uruchomić ponownie.
2. RFC1700 udostępnia informacje o powszechnych przypisaniach numerów portów.

Ochrona serwera REXEC

Decydując się na uruchamianie w systemie programu Remote EXECution server, należy wziąć pod uwagę poniższe uwagi:

- Zgłoszenie REXCD obejmuje identyfikator użytkownika, hasło i komendę do wykonania. Stosowane jest standardowe uwierzytelnianie i sprawdzanie uprawnień serwera iSeries:
  - profil użytkownika i hasło muszą być poprawne,
  - system wymusza dla profilu użytkownika wartość *Ograniczenie możliwości (Limit capabilities - LMTCPB)*,
  - użytkownik musi mieć uprawnienia do komendy i do wszystkich zasobów używanych przez komendę.
- Serwer REXEC udostępnia punkty wyjścia podobne do punktów wyjścia dostępnych dla serwera FTP. Przed podjęciem decyzji o udostępnieniu komendy, do jej oceny, można użyć punktu wyjścia Potwierdzenie. Więcej informacji na ten temat znajduje się w Centrum informacyjnym iSeries —>Sieci—>TCP/IP—>REXEC. Informacje na temat dostępu do Centrum informacyjnego iSeries zawiera sekcja “Informacje wstępne i pokrewne” na stronie xii.
- Uruchamianie serwera REXEC powoduje utratę kontroli dostępu do menu obecnej w systemie. Konieczne jest wówczas zastosowanie schematu uprawnień do obiektów, które zapewni ochronę zasobów.

Bezpieczne używanie demona RouteD

Demon Route Daemon (RouteD) obsługuje w serwerze iSeries protokół RIP (Routing Information Protocol). Protokół RIP jest najpowszechniej stosowanym protokołem routingu. Jest on protokołem Interior Gateway Protocol, wspomagającym protokół TCP/IP w routingu pakietów IP w obrębie systemu autonomicznego.

Zadaniem demona RouteD jest zwiększenie efektywności ruchu pakietów poprzez umożliwienie systemom w ramach zaufanej sieci wzajemnej aktualizacji informacji o routingu. Kiedy działa demon RouteD, system lokalny otrzymuje od innych systemów uczestniczących aktualne informacje o tym, jak powinna być rutowana transmisja (pakiety). Dlatego jeśli demon RouteD jest dostępny dla hakera, może on wykorzystać go do przekierowania pakietów, tak że będzie je mógł przechwycić lub zmodyfikować. Poniżej przedstawiono zalecenia dotyczące ochrony demona RouteD.

- Serwery iSeries używają protokołu RIPv1, który nie udostępnia żadnej metody wierzytelniania routerów. Jest on przeznaczony do pracy w obrębie zaufanej sieci. Jeśli system lokalny działa w sieci z innymi systemami, które nie należą do ″zaufanych″, nie należy uruchamiać demona RouteD. Aby demon RouteD nie uruchamiał się automatycznie, wpisz:

  ```
  CHGRTDA AUTOSTART(*NO)
  ```

  Uwagi:

  1. Wartością domyślną jest AUTOSTART(*NO).
  2. Sekcja “Kontrolowanie automatycznego uruchamiania serwerów TCP/IP” na stronie 118 zawiera więcej informacji dotyczących sterowania automatycznym uruchamianiem serwerów TCP/IP.
- Administrator ochrony powinien kontrolować użytkowników, którzy mogą zmieniać konfigurację serwera RouteD, co wymaga uprawnień specjalnych *IOSYSCFG.
- Jeśli system lokalny pracuje w kilku sieciach (na przykład w intranecie i w Internecie), można skonfigurować serwer RouteD tak, aby wysyłał i akceptował aktualizacje tylko w obrębie chronionej sieci.

Bezpieczne używanie serwera DNS

Serwer DNS (Domain Name System) umożliwia translację nazw hostów na adresy IP i odwrotnie. Serwer DNS w systemie iSeries udostępnia translację adresów dla wewnętrznej sieci chronionej (intranet).

Zabezpieczenie przed dostępem do serwera DNS

Jeśli w systemie serwer DNS ma być *niedostępny*, wykonaj następujące czynności:

1. Aby uniemożliwić automatyczne uruchamianie zadań serwera DNS podczas uruchamiania przetwarzania TCP/IP, wpisz:

   ```
   CHGDNSA AUTOSTART(*NO)
   ```

   Uwagi:

   1. Wartością domyślną jest AUTOSTART(*NO).
   2. Sekcja “Kontrolowanie automatycznego uruchamiania serwerów TCP/IP” na stronie 118 zawiera więcej informacji dotyczących sterowania automatycznym uruchamianiem serwerów TCP/IP.
2. Aby uniemożliwić powiązanie aplikacji użytkownika, na przykład aplikacji używającej gniazda, z portem używanym normalnie przez system na potrzeby DNS, wykonaj poniższe czynności:

a. Wpisz GO CFGTCP, aby wyświetlić menu Konfigurowanie TCP/IP (Configure TCP/IP).
b. Wybierz opcję 4 (Praca z ograniczeniami portu TCP/IP).
c. Na ekranie Praca z ograniczeniami portu TCP/IP (Work with TCP/IP Port Restrictions) wybierz opcję 1 (Dodaj).
d. Jako dolny zakres portu podaj 53.
e. Jako górny zakres portu podaj *ONLY.

Uwagi:

1. Ograniczenie dostępu do portu zostanie zastosowane przy następnym uruchomieniu TCP/IP. Jeśli przetwarzanie TCP/IP jest włączone podczas ograniczania dostępu do portu, należy je zakończyć i uruchomić ponownie.
2. RFC1700 udostępnia informacje o powszechnych przypisaniach numerów portów.

f. Jako protokół podaj *TCP.
g. W polu Profil użytkownika należy podać nazwę profilu użytkownika, który jest chroniony w systemie. (Zabezpieczony profil użytkownika to profil użytkownika, który nie jest właścicielem programów adoptujących uprawnienia i nie ma hasła znanego innym użytkownikom.) Ograniczając port do konkretnego użytkownika automatycznie wyłącza się wszystkich pozostałych użytkowników.
h. Powtórz kroki od 2c do 2g dla protokołu *UDP (datagram użytkownika).

Ochrona serwera DNS

Decydując się na uruchomienie w systemie iSeries serwera DNS, należy uwzględnić następujące zagadnienia ochrony:

- Funkcją udostępnianą przez serwer DNS jest translacja adresów IP i translacja nazw. Nie daje on żadnego dostępu do obiektów w lokalnym systemie iSeries. Zagrożenie związane z nieupoważnionym dostępem do serwera DNS to łatwy wgląd w topologię sieci lokalnej. Serwer DNS może ułatwić hakerowi określenie adresów potencjalnych celów. Nie udostępnia on jednak informacji, które pomogą włamać się do tych systemów.
- Zazwyczaj serwera DNS w systemie iSeries używa się na potrzeby intranetu. Dlatego prawdopodobnie nie jest konieczne ograniczanie możliwości kierowania zapytań do serwera DNS. Możliwe jest jednak istnienie kilku podsieci w ramach intranetu. Pożądane może być wówczas uniemożliwienie użytkownikom z innych podsieci korzystania z serwera DNS w lokalnym serwerze iSeries. Opcja ochrony serwera DNS umożliwia ograniczenie dostępu do domeny podstawowej. Za pomocą programu iSeries Navigator należy określić adresy IP, na które serwer DNS powienien odpowiadać.

  Inna opcja ochrony pozwala określić, które serwery dodatkowe mogą kopiować informacje z podstawowego serwera DNS. Po zastosowaniu tej opcji serwer lokalny będzie akceptował żądania przesyłania strefowego (żądania kopiowania informacji) tylko z serwerów, które zostaną wymienione.
- Szczególną uwagę należy poświęcić ograniczeniu możliwości zmian pliku konfiguracyjnego serwera DNS. W przeciwnym razie ktoś mógłby na przykład zmienić plik DNS, tak aby wskazywał adres IP na zewnątrz sieci lokalnej. Następnie mógłby zasymulować serwer sieci lokalnej i w ten sposób uzyskać dostęp do poufnych informacji użytkowników, którzy chcieliby skorzystać z tego serwera.

Bezpieczne używanie serwera HTTP server w iSeries

Serwer HTTP umożliwia klientom przeglądarek WWW dostęp do obiektów multimedialnych serwera iSeries, na przykład dokumentów HTML (Hypertext Markup Language). Serwer ten obsługuje także specyfikację interfejsu *Common Gateway Interface (CGI)*. Programiści aplikacji mogą pisać programy CGI rozszerzające funkcjonalność serwera.

Możliwe jest użycie produktu Internet Connection Server lub IBM do jednoczesnego uruchomienia wielu serwerów w tym samym iSeries. Każdy uruchomiony serwer jest nazywany **instancją serwera**. Każda instancja serwera ma swoją unikalną nazwę. Administrator kontroluje, które instancje są uruchomione i co każda instancja może robić.

Uwaga: Aby za pomocą przeglądarki WWW konfigurować poniższe usługi lub administrować nimi, musi być uruchomiona instancja *ADMIN serwera HTTP:

- Firewall for iSeries
- Internet Connection Server
- Internet Connection Secure Server
- IBM HTTP Server for iSeries

Użytkownik (korzystający z serwisu WWW) nigdy nie widzi ekranu Wpisanie się (Sign On) serwera iSeries. Administrator serwera iSeries musi jawnie nadać uprawnienia wszystkim dokumentom HTML i programom CGI, definiując je w dyrektywach HTTP. Ponadto administrator może skonfigurować zarówno ochronę zasobów, jak i uwierzytelnianie użytkownika (identyfikator użytkownika i hasło) dla niektórych lub dla wszystkich żądań.

Skutkiem ataku hakerów może być odmowa usług serwera WWW. Serwer może wykryć atak typu ″denial-of-service″ (odmowa usługi), mierząc czas oczekiwania dla pewnych żądań klienta. Jeśli serwer nie odbiera żądań od klienta, może to oznaczać atak typu ″denial-of-service″. Dzieje się tak po nawiązaniu przez klienta początkowego połączenia z serwerem. Domyślnym zadaniem serwera jest wykrycie ataku i jego unieszkodliwienie.

Zabezpieczenie przed dostępem przez HTTP

Jeśli system ma być *niedostępny* dla użytkowników programów, należy zablokować możliwość uruchamiania serwera HTTP, wykonując poniższe czynności:

__ Krok 1. Aby uniemożliwić automatyczne uruchamianie zadań serwera HTTP podczas uruchamiania przetwarzania TCP/IP, wpisz:

```
CHGHTTPA AUTOSTART(*NO)
```

Uwagi:

1. Wartością domyślną jest AUTOSTART(*NO).
2. Sekcja “Kontrolowanie automatycznego uruchamiania serwerów TCP/IP” na stronie 118 zawiera więcej informacji dotyczących sterowania automatycznym uruchamianiem serwerów TCP/IP.

__ Krok 2. Domyślnie zadania serwera HTTP używają profilu użytkownika QTMHHTTP. Aby uniemożliwić uruchamianie serwera HTTP, należy profilowi użytkownika QTMHHTTP nadać status *DISABLED.

Kontrola praw dostępu do serwera HTTP

Podstawowym celem uruchamiania serwera HTTP jest udostępnienie użytkownikom serwisu WWW prowadzonego w systemie iSeries. Użytkowników takich można traktować jak osoby przeglądające reklamy w piśmie handlowym. Nie są oni świadomi sprzętu i oprogramowania działającego na potrzeby serwisu WWW, nie wiedzą, jaki typ serwera jest używany i gdzie się on fizycznie znajduje. Zwykle nie ma potrzeby stawiania barier (takich jak ekran Wpisanie się (Sign On)) pomiędzy potencjalnymi gośćmi i serwisem WWW. Wskazane może być jednak ograniczenie dostępu do niektórych dokumentów lub programów CGI udostępnianych przez serwis WWW.

Możliwe jest także udostępnienie wielu serwisów WWW w jednym systemie iSeries. Na przykład system iSeries może obsługiwać różne branże prowadzonej działalności, które mają odrębne grupy klientów. Dla każdej z tych branż można utworzyć osobny serwis WWW,

który dla gościa będzie zupełnie niezależny od pozostałych. Możliwe jest ponadto udostępnienie wewnętrznych serwisów WWW (intranet) z poufnymi informacjami gospodarczymi.

Administrator ochrony musi chronić zawartość serwisu WWW, uważając jednocześnie, aby zastosowane zabezpieczenia nie wpłynęły negatywnie na jego wydajność. Ponadto nie może on dopuścić, aby aktywność związana z HTTP nie zagroziła integralności lokalnego systemu lub lokalnej sieci. W poniższych sekcjach opisano sugestie dotyczące ochrony w przypadku korzystania z programu.

Zagadnienia związane z administrowaniem

Poniżej przedstawiono niektóre zagadnienia dotyczące ochrony przy administrowaniu serwerem internetowym.

- Funkcje instalacyjne i konfiguracyjne wykonuje się korzystając z przeglądarki WWW i instancji *ADMIN. Dla niektórych funkcji, jak na przykład tworzenie dodatkowych instancji serwera, *konieczne jest* użycie serwera *ADMIN.
- Domyślny adres URL strony głównej administratora (strona główna serwera *ADMIN) jest podany w dokumentacji produktów udostępniających funkcje administracyjne poprzez przeglądarkę. Dlatego adres ten jest najprawdopodobniej znany hakerom i publikowany w ich serwisach, tak jak znane i publikowane są domyślne hasła profili użytkowników IBM. Przed tym zagrożeniem można się zabezpieczyć na kilka sposobów:
  - Uruchamiaj instancję *ADMIN serwera HTTP tylko wtedy, kiedy masz do wykonania funkcje administracyjne. Nie pozwól, aby instancja *ADMIN działała bez przerwy.
  - Uaktywnij obsługę warstwy SSL dla instancji *ADMIN (używając programu Menedżer certyfikatów cyfrowych). Instancja *ADMIN używa dyrektyw ochrony HTTP przy żądaniu identyfikatora użytkownika i hasła. Kiedy używana jest warstwa SSL, identyfikator użytkownika i hasło są zaszyfrowane (a także inne informacje o konfiguracji, które pojawiają się na formularzach administracyjnych).
  - Aby uniemożliwić dostęp z Internetu do serwera *ADMIN oraz ukryć nazwy systemu i domeny, które są częścią adresu URL, używaj programu firewall.
- W celu wykonania funkcji administracyjnych należy wpisać się z profilem użytkownika o uprawnieniach specjalnych *IOSYSCFG. Ponadto konieczne mogą być uprawnienia do konkretnych obiektów systemu, takich jak:
  - biblioteki lub katalogi zawierające dokumenty HTML i programy CGI,
  - wszystkie profile użytkownika, które mają być przełączone w ramach dyrektyw dla serwera,
  - listy kontroli dostępu (ACL) do wszystkich katalogów używanych przez dyrektywy,
  - obiekty listy weryfikacji do tworzenia i obsługi identyfikatorów użytkowników i haseł.

  Serwer *ADMIN w połączeniu z programem TELNET daje możliwość zdalnego wykonywania funkcji administracyjnych, nawet poprzez połączenie internetowe. Należy jednak mieć świadomość, że wykonywanie funkcji administracyjnych poprzez łącza publiczne (Internet) oznacza narażanie identyfikatora i hasła administratora na przechwycenie. ″Podsłuchiwacz″ może użyć tego identyfikatora i hasła, aby spróbować włamać się do systemu poprzez na przykład TELNET lub FTP.

  Uwagi:

  1. W przypadku programu TELNET ekran Wpisanie się (Sign On) jest traktowany jak każdy inny ekran. Hasło nie jest wyświetlane na ekranie podczas wpisywania, ale system przesyła je bez żadnego szyfrowania czy kodowania.
  2. W przypadku serwera *ADMIN hasło jest kodowane, nie szyfrowane. Schemat kodowania jest standardem przemysłowym, powszechnie znanym w społeczności

hakerów. Chociaż kodowanie nie jest łatwym problemem dla doraźnego ″podsłuchiwacza″, zaawansowany haker prawdopodobnie dysponuje narzędziem do podjęcia próby odkodowania hasła.

Wskazówka dotycząca ochrony

Jeśli planowane jest zdalne administrowanie poprzez Internet, należy używać instancji *ADMIN wraz z warstwą SSL, dzięki której transmisja będzie szyfrowana. Nie należy używać niezabezpieczonych aplikacji, takich jak program TELNET w wersji wcześniejszej niż V4R4 (TELNET obsługuje SSL począwszy od wersji V4R4). Jeśli serwer *ADMIN używany jest w sieci intranet składającej się z *zaufanych* użytkowników, można prawdopodobnie używać tego programu do administrowania.

- Dyrektywy HTTP stanowią podstawę wszelkiego działania serwera. W dostarczanej konfiguracji serwer udostępnia domyślną stronę powitalną. Klient nie może zobaczyć żadnych innych dokumentów oprócz strony powitalnej, dopóki administrator serwera nie zdefiniuje dyrektyw dla serwera. Aby je zdefiniować, należy użyć przeglądarki WWW i serwera *ADMIN lub komendy Praca z konfiguracją HTTP (Work with HTTP Configuration - WRKHTTPCFG). Obie metody wymagają uprawnień specjalnych *IOSYSCFG. Po podłączeniu lokalnego serwera iSeries do Internetu newralgiczną kwestią staje się oszacowanie i kontrolowanie liczby użytkowników w ramach organizacji, którzy mają uprawnienia specjalne *IOSYSCFG.

Zasoby zabezpieczone

Produkt IBM HTTP Server for iSeries zawiera dyrektywy HTTP umożliwiające szczegółową kontrolę używanych przez serwer informacji. Dyrektywy służące do sterowania, z których katalogów serwer WWW udostępnia zarówno pliki HTML, jak i programy CGI, można stosować do przełączania się na inny profil użytkownika i do żądania uwierzytelniania dla niektórych zasobów.

Uwaga: W Centrum informacyjnym iSeries znajduje się artykuł ″Obsługa serwisów WWW″, w którym przedstawiono kompletne opisy dostępnych dyrektyw HTTP i sposobów ich użycia. Poniżej przedstawiono kilka sugestii dotyczących tej obsługi:

- Serwer HTTP działa na podstawie ″uprawnień jawnych″. Serwer nie zaakceptuje żądania, jeśli nie zostało ono w sposób jawny zdefiniowane w dyrektywach. Innymi słowy serwer natychmiast odrzuca każde żądanie danego adresu URL, chyba że adres ten został zdefiniowany w dyrektywach (poprzez nazwę lub w sposób ogólny).
- Aby zażądać podania identyfikatora użytkownika i hasła przed zaakceptowaniem żądania dotyczącego wybranych lub wszystkich zasobów, należy użyć dyrektyw ochrony.
  - Kiedy użytkownik (klient) żąda dostępu do zasobu zabezpieczonego, serwer żąda od przeglądarki podania identyfikatora użytkownika i hasła. Przeglądarka pyta użytkownika o identyfikator i hasło i przesyła te dane do serwera. Niektóre przeglądarki przechowują identyfikator użytkownika i hasło, i wysyłają je automatycznie na kolejne żądania. Oszczędza to użytkownikowi konieczności wpisywania identyfikatora i hasła przy każdym żądaniu.

    Z drugiej strony trzeba poinformować użytkowników o możliwych zagrożeniach stosowania tej metody, podobnie jak w przypadku wchodzenia do serwera iSeries za pośrednictwem ekranu Wpisanie się (Sign On) lub routera. Pozostawiona bez dozoru sesja przeglądarki stanowi potencjalne zagrożenie bezpieczeństwa.
  - System obsługuje identyfikator użytkownika i hasło na trzy sposoby (określane w dyrektywach ochrony):
    1. Można używać normalnego potwierdzania profilu użytkownika i hasła w serwerze iSeries. Jest to rozwiązanie powszechnie stosowane do zabezpieczania zasobów w intranecie (bezpieczna sieć).

2. Można utworzyć ″użytkowników internetowych″: użytkowników, których potwierdzenie przebiega pomyślnie, ale nie mających profilu użytkownika w serwerze iSeries. Użytkowników internetowych definiuje się za pomocą obiektu serwera iSeries zwanego ″listą weryfikacji″. Obiekty list weryfikacji zawierają listy użytkowników i haseł zdefiniowanych dla konkretnej aplikacji.

   Decyzja o tym, jak przekazywać identyfikatory i hasła (na przykład za pomocą aplikacji lub przez administratora w odpowiedzi na zgłoszenie pocztą elektroniczną) oraz jak zarządzać użytkownikami internetowymi, należy do administratora ochrony. Do odpowiedniego skonfigurowania systemu należy użyć interfejsu serwera HTTP opartego na przeglądarce.

   W przypadku sieci niechronionych (Internet) wprowadzenie użytkowników internetowych daje lepsze ogólne zabezpieczenie niż użycie standardowych profili użytkownika i haseł. Unikalny zestaw identyfikatorów i haseł tworzy wbudowane ograniczenie na dostępne dla użytkowników działania. Identyfikatory użytkowników i hasła nie pozwalają na zwykłe wpisanie się do systemu (na przykład przez TELNET lub przez FTP). Ponadto zwykli użytkownicy nie są narażeni na podsłuchanie identyfikatorów i haseł.

3. Protokół LDAP (Lightweight Directory Access Protocol) jest protokołem usług katalogowych, który udostępnia katalog za pośrednictwem protokołu TCP. Umożliwia on zapisywanie i wyszukiwanie danych w katalogu. Protokół LDAP jest obecnie obsługiwany jako jedna z możliwości uwierzytelniania użytkowników.

Uwagi:

1. Przesyłane przez przeglądarkę identyfikator użytkownika i hasło (dla profilu użytkownika lub dla użytkownika internetowego) nie są zaszyfrowane, tylko zakodowane. Schemat kodowania jest standardem przemysłowym, powszechnie znanym w społeczności hakerów. Chociaż kodowanie nie jest łatwą sprawą dla doraźnego ″podsłuchiwacza″, zaawansowany haker prawdopodobnie dysponuje narzędziem umożliwiającym odkodowanie hasła.
2. Serwer iSeries przechowuje obiekty potwierdzania w chronionym obszarze systemowym. Dostęp do nich możliwy jest tylko przez określone interfejsy systemowe (API) i przy odpowiedniej autoryzacji.

– Aby utworzyć własny intranetowy ośrodek certyfikujący, można użyć programu Menedżer certyfikatów cyfrowych (DCM). Wykonuje on automatyczne kojarzenie certyfikatu z profilem użytkownika jego właściciela. Certyfikat ma takie same autoryzacje i uprawnienia jak skojarzony z nim profil.

- Po zaakceptowaniu żądania przez serwer, kontrolę przejmuje zwykła ochrona zasobów serwera iSeries. Profil użytkownika, który zażądał dostępu do zasobu, musi mieć uprawnienia do tego zasobu (na przykład do folderu lub źródłowego zbioru fizycznego zawierającego dokument HTML). Domyślnie zadania wykonywane są dla profilu użytkownika QTMHHTTP. Aby przełączyć się do innego profilu użytkownika, można skorzystać z dyrektywy. System używa wtedy uprawnień do obiektów tego profilu użytkownika. Poniżej przedstawiono niektóre zagadnienia związane z tą obsługą:
  – Przełączanie profili użytkowników może być szczególnie przydatne, gdy serwer udostępnia kilka logicznych serwisów WWW. Za pomocą dyrektyw z każdym z nich można powiązać różne profile użytkowników i w ten sposób wykorzystać standardową ochronę zasobów serwera iSeries, aby zabezpieczyć dokumenty każdego serwisu.
  – Z możliwości przełączania profili użytkowników można skorzystać w połączeniu z potwierdzeniem obiektu. Do oceny początkowego żądania serwer używa unikalnego identyfikatora użytkownika i hasła (innego niż normalny identyfikator użytkownika i hasło). Po uwierzytelnieniu użytkownika system przełącza go do innego profilu użytkownika, wykorzystując w ten sposób ochronę zasobów. W takiej sytuacji użytkownik nie zna prawdziwej nazwy profilu użytkownika i nie może spróbować wykorzystać jej w inny sposób (na przykład poprzez FTP).

- Niektóre żądania serwera HTTP wymagają uruchomienia programu na serwerze HTTP. Na przykład program może pobierać dane z systemu lokalnego. Zanim program zostanie uruchomiony, administrator serwera musi odwzorować żądanie (URL) na określony, zdefiniowany przez użytkownika program, który spełnia standardy interfejsu użytkownika CGI. Poniżej przedstawiono niektóre zagadnienia dotyczące programów CGI:
  - W stosunku do programów CGI można używać dyrektyw ochrony, tak jak dla dokumentów HTML. Dzięki temu przed uruchomieniem programu można zażądać identyfikatora użytkownika i hasła.
  - Domyślnie programy CGI wykonywane są z profilami użytkownika QTMHHTP1. Przed uruchomieniem programu możliwe jest także przełączenie się do innego profilu użytkownika. Dzięki temu możliwe jest skonfigurowanie standardowej ochrony serwera iSeries dla zasobów, z których korzystają programy CGI.
  - Przed nadaniem uprawnień do użycia programów CGI w systemie administrator ochrony powinien dokonać przeglądu ochrony. Powinien także dowiedzieć się, skąd pochodzi program i jakie funkcje wykonuje oraz skontrolować możliwości profili użytkowników, dla których program jest wykonywany. Należy również przetestować programy CGI, sprawdzając na przykład, czy można z ich pomocą uzyskać dostęp do wiersza komend. Programy CGI powinny być traktowane z taką samą ostrożnością, z jaką traktowane są inne programy, które adoptują uprawnienia.
  - Dodatkowo konieczna jest ocena, które z newralgicznych obiektów mogą mieć nieodpowiednie uprawnienia publiczne. Źle zaprojektowany program CGI może czasami umożliwiać użytkownikom o odpowiedniej wiedzy przeglądanie zasobów systemu.
  - Do przechowywania wszystkich programów CGI należy używać określonej biblioteki użytkownika, na przykład CGILIB. Aby kontrolować, kto może umieszczać w tej bibliotece nowe obiekty i kto może uruchamiać znajdujące się w niej programy, można posłużyć się uprawnieniami do obiektów. Za pomocą dyrektyw można ograniczyć uprawnienia serwera HTTP do uruchamiania tylko programów CGI znajdujących się w tej bibliotece.

    Uwaga: Jeśli serwer udostępnia wiele logicznych serwisów WWW, można zdefiniować osobne biblioteki dla programów CGI dla każdego serwisu.

Pozostałe zagadnienia dotyczące ochrony

Poniżej przedstawiono dodatkowe zagadnienia dotyczące ochrony:

- HTTP zapewnia dostęp do systemu iSeries w trybie tylko do odczytu. Zadania serwera HTTP nie mogą bezpośrednio aktualizować ani usuwać danych w systemie. Jednakże dane można aktualizować za pomocą programów CGI. Dodatkowo można umożliwić programowi CGI Net.Data dostęp do bazy danych serwera iSeries. Do oceny żądań programu Net.Data system korzysta ze skryptu (podobnego do programu obsługi wyjścia). Dzięki niemu administrator systemu może kontrolować czynności wykonywane przez program Net.Data.
- Serwer HTTP utrzymuje protokół dostępu, którego można używać do monitorowania zarówno pomyślnych, jak i niepomyślnych prób dostępu do serwera.

Bezpieczne używanie SSL z IBM HTTP Server for iSeries

IBM HTTP Server for iSeries udostępnia chronione połączenia WWW z serwerem iSeries. W **chronionym serwisie WWW** transmisja pomiędzy klientem a serwerem (w obydwu kierunkach) jest zaszyfrowana. Takie zaszyfrowane transmisje są chronione przed zarówno podsłuchiwaczami, jak i hakerami, którzy chcą je przechwycić lub zmienić.

Uwaga: Należy zwrócić uwagę, że termin chroniony serwis WWW odnosi się wprost do bezpieczeństwa informacji, które są przesyłane pomiędzy klientem i serwerem.

Pojęcie to nie obejmuje natomiast odporności na ataki hakerów. Jednakże w takim przypadku z pewnością ograniczona jest informacja, którą mógłby przechwycić haker.

Artykuły poświęcone SSL i serwerom WWW (HTTP) w Centrum informacyjnym zawierają kompletne informacje dotyczące instalowania, konfigurowania i zarządzania procesem szyfrowania. Artykuły te udostępniają zarówno przegląd funkcji serwera, jak i nieco rozważań dotyczących używania serwera.

Produkt Internet Connection Server udostępnia obsługę protokołów HTTP i HTTPS, kiedy zainstalowany jest jeden z poniższych programów licencjonowanych:

- 5722–NC1
- 5722–NCE

Kiedy powyższe opcje są zainstalowane, produkt nazywany jest Internet Connection Secure Server.

IBM HTTP Server for iSeries (5722–DG1) obsługuje protokoły HTTP i HTTPS. Aby uaktywnić warstwę SSL, należy zainstalować jeden z następujących produktów szyfrujących:

- 5722–AC2
- 5722–AC3

Ochrona, polegająca na szyfrowaniu narzuca kilka wymagań:

- Zarówno nadawca, jak i odbiorca (serwer i klient) muszą ″rozumieć″ mechanizm szyfrowania oraz muszą być w stanie wykonać szyfrowanie i deszyfrowanie. Serwer HTTP wymaga klienta z włączoną obsługą SSL. (Najbardziej popularne przeglądarki WWW obsługują SSL). Licencjonowane programy szyfrujące w systemie iSeries obsługują kilka standardów przemysłowych szyfrowania. Kiedy klient próbuje nawiązać chronione połączenie, serwer i klient negocjują w celu znalezienia najbezpieczniejszej metody szyfrowania obsługiwanej przez obydwa systemy.
- Transmisja nie może być podatna na próby deszyfrowania przez podsłuchiwaczy. Dlatego metody szyfrowania wymagają, aby obie strony posiadały znany tylko im **prywatny klucz** szyfrowania/deszyfrowania. Chcąc prowadzić bezpieczny *zewnętrzny* serwis WWW, należy skorzystać z niezależnego ośrodka certyfikacji w celu utworzenia i wydawania certyfikatów cyfrowych dla użytkowników i serwerów. Ośrodek certyfikacji jest nazywany firmą zaufaną.

Szyfrowanie chroni poufność transmitowanych informacji. Jednak w niektórych przypadkach, na przykład informacji finansowych, oprócz poufności wymagana jest integralność i wiarygodność informacji. Innymi słowy, klient i (opcjonalnie) serwer muszą ufać drugiej stronie (poprzez niezależne referencje) oraz muszą mieć pewność, że transmisja nie została zmieniona. Dostarczany przez ośrodek certyfikacji podpis cyfrowy daje gwarancję wiarygodności i integralności. Poprzez weryfikację podpisu cyfrowego certyfikatu serwera (i opcjonalnie klienta) protokół SSL zapewnia uwierzytelnienie.

Szyfrowanie i deszyfrowanie wymagają dodatkowego przetwarzania i wpływają na wydajność transmisji. Dlatego serwery iSeries umożliwiają jednoczesne wykonywanie programów dla połączeń chronionych i niechronionych. Do udostępniania informacji, które nie wymagają ochrony, na przykład katalogu produktów, można używać niechronionego serwera WWW. Dokumenty te będą mieć adres URL rozpoczynający się od http://. W przypadku newralgicznych informacji, na przykład formularzy, w które klienci wpisują numery kart kredytowych, konieczne jest użycie chronionego serwera WWW. Program ten może udostępniać dokumenty, których adresy URL zaczynają się od http:// lub od https://.

Przypomnienie

Dobrym zwyczajem internetowej etykiety jest informowanie klientów, kiedy transmisja jest chroniona, a kiedy nie, szczególnie gdy serwis WWW używa chronionego serwera tylko w przypadku niektórych dokumentów.

Należy zwrócić uwagę, że szyfrowanie wymaga zarówno chronionego klienta, jak i chronionego serwera. Chronione przeglądarki (klienci HTTP) są obecnie bardzo popularne.

Ochrona LDAP

Opcje zabezpieczające protokołu LDAP obejmują obsługę SSL, listy kontroli dostępu i szyfrowanie haseł CRAM-MD5. W wersji V5R1 wzmocniono ochronę LDAP, dodając obsługę połączeń Kerberos i kontrolę ochrony.

Więcej informacji na ten temat zawiera sekcja iSeries Centrum informacyjne—>Sieć–>TCP/IP–>Directory Services (LDAP). Informacje na temat dostępu do Centrum informacyjnego iSeries zawiera sekcja “Informacje wstępne i pokrewne” na stronie xii.

Ochrona LPD

Demon drukarki (LPD - line printer daemon) umożliwia systemowi dystrybucję wydruków. W przypadku demona LPD system nie wykonuje żadnego przetwarzania wpisywania się.

Zabezpieczenie przed dostępem do LPD

Jeśli system ma być *niedostępny* dla użytkowników demona LPD, należy zablokować możliwość uruchamiania serwera LPD, wykonując poniższe czynności:

__ Krok 1. Aby uniemożliwić automatyczne uruchamianie zadań serwera LPD podczas uruchamiania przetwarzania TCP/IP, wpisz:

```
CHGLPDA AUTOSTART(*NO)
```

Uwagi:

1. Wartością domyślną jest AUTOSTART(*YES).
2. Sekcja “Kontrolowanie automatycznego uruchamiania serwerów TCP/IP” na stronie 118 zawiera więcej informacji dotyczących sterowania automatycznym uruchamianiem serwerów TCP/IP.

__ Krok 2. Aby uniemożliwić powiązanie aplikacji użytkownika, na przykład aplikacji używającej gniazda, z portem używanym normalnie przez system na potrzeby LPD, wykonaj poniższe czynności:

__ Krok a. Wpisz GO CFGTCP, aby wyświetlić menu Konfigurowanie TCP/IP (Configure TCP/IP).

__ Krok b. Wybierz opcję 4 (Praca z ograniczeniami portu TCP/IP).

__ Krok c. Na ekranie Praca z ograniczeniami portu TCP/IP (Work with TCP/IP Port Restrictions) wybierz opcję 1 (Dodaj).

__ Krok d. Jako dolny zakres portu podaj 515.

__ Krok e. Jako górny zakres portu podaj *ONLY.

Uwagi:

1. Ograniczenie dostępu do portu zostanie zastosowane przy następnym uruchomieniu TCP/IP. Jeśli przetwarzanie TCP/IP

jest włączone podczas ograniczania dostępu do portu, należy je zakończyć i uruchomić ponownie.

2. RFC1700 udostępnia informacje o powszechnych przypisaniach numerów portów.

__ Krok f. Jako protokół podaj *TCP.

__ Krok g. W polu Profil użytkownika należy podać nazwę profilu użytkownika, który jest chroniony w systemie. (Zabezpieczony profil użytkownika to profil użytkownika, który nie jest właścicielem programów adoptujących uprawnienia i nie ma hasła znanego innym użytkownikom.) Ograniczając port do konkretnego użytkownika automatycznie wyłącza się wszystkich pozostałych użytkowników.

__ Krok h. Powtórz kroki od 2c do 2g dla protokołu *UDP.

Sterowanie dostępem do LPD

Jeśli potrzebny jest dostęp klientów LPD do systemu, należy zwrócić uwagę na następujące zagadnienia dotyczące ochrony:

- Aby uniemożliwić użytkownikom zasypywanie systemu niechcianymi obiektami, należy ustawić odpowiednie limity progowe dla pul pamięci dyskowej (ASP). Wartości progowe dla pul ASP można wyświetlić i ustawić za pomocą systemowych narzędzi serwisowych (SST) lub narzędzi Dedicated Service Tools (DST). Książka *Składowanie i odtwarzanie* dostarcza więcej informacji o wartościach progowych pul ASP.
- Za pomocą uprawnień do kolejek wyjściowych można ograniczyć liczbę użytkowników, którzy mogą przesyłać zbiory buforowane do systemu lokalnego. Dla użytkowników demona LPD, którzy nie maja identyfikatora użytkownika, stosowany jest profil użytkownika QTMPLPD. Profilowi temu można przyznać dostęp tylko do kilku kolejek wyjściowych.

Ochrona SNMP

Serwer iSeries może działać w sieci jako agent protokołu SNMP (Simple Network Management Protocol). Protokół SNMP udostępnia środki do zarządzania bramami, routerami i hostami w środowisku sieciowym. Agent SNMP zbiera informacje o systemie i wykonuje funkcje żądane przez zdalne menedżery sieci SNMP.

Zabezpieczenie przed dostępem do SNMP

Jeśli system ma być *niedostępny* dla użytkowników protokołu SNMP, należy zablokować możliwość uruchamiania serwera SNMP, wykonując poniższe czynności:

__ Krok 1. Aby uniemożliwić automatyczne uruchamianie zadań serwera SNMP podczas uruchamiania przetwarzania TCP/IP, wpisz:

```
CHGSNMPA AUTOSTART(*NO)
```

Uwagi:

1. Wartością domyślną jest AUTOSTART(*YES).
2. Sekcja “Kontrolowanie automatycznego uruchamiania serwerów TCP/IP” na stronie 118 zawiera więcej informacji dotyczących sterowania automatycznym uruchamianiem serwerów TCP/IP.

__ Krok 2. Aby uniemożliwić powiązanie aplikacji użytkownika, na przykład aplikacji używającej gniazda, z portem używanym normalnie przez system na potrzeby SNMP, wykonaj poniższe czynności:

__ Krok a. Wpisz GO CFGTCP, aby wyświetlić menu Konfigurowanie TCP/IP (Configure TCP/IP).

__ Krok b. Wybierz opcję 4 (Praca z ograniczeniami portu TCP/IP).

__ Krok c. Na ekranie Praca z ograniczeniami portu TCP/IP (Work with TCP/IP Port Restrictions) wybierz opcję 1 (Dodaj).

__ Krok d. Jako dolny zakres portu podaj 161.

__ Krok e. Jako górny zakres portu podaj *ONLY.

Uwagi:

1. Ograniczenie dostępu do portu zostanie zastosowane przy następnym uruchomieniu TCP/IP. Jeśli przetwarzanie TCP/IP jest włączone podczas ograniczania dostępu do portu, należy je zakończyć i uruchomić ponownie.
2. RFC1700 udostępnia informacje o powszechnych przypisaniach numerów portów.

__ Krok f. Jako protokół podaj *TCP.

__ Krok g. W polu Profil użytkownika należy podać nazwę profilu użytkownika, który jest chroniony w systemie. (Zabezpieczony profil użytkownika to profil użytkownika, który nie jest właścicielem programów adoptujących uprawnienia i nie ma hasła znanego innym użytkownikom.) Ograniczając port do konkretnego użytkownika automatycznie wyłącza się wszystkich pozostałych użytkowników.

__ Krok h. Powtórz kroki od 2c do 2g dla protokołu *UDP.

Zabezpieczenie przed dostępem do SNMP

Jeśli potrzebny jest dostęp menedżerów SNMP do systemu, należy zwrócić uwagę na następujące zagadnienia dotyczące ochrony:

- Każdy kto ma dostęp do sieci lokalnej poprzez protokół SNMP może uzyskać informacje o tej sieci. Dzięki SNMP informacja ukrywana przez stosowanie aliasów i serwerów nazw domen jest dostępna dla intruza. Może on ponadto użyć SNMP do zmiany konfiguracji sieciowej i zakłócenia komunikacji.
- Dostęp do SNMP opiera się na nazwie grupy. Ideowo nazwa grupy jest zbliżona do hasła. Nazwa ta nie jest zaszyfrowana, przez co jest narażona na przechwycenie. Aby parametrowi INTNETADR (adres internetowy menedżera) przypisać jeden lub więcej adresów, zamiast wartości *ANY, należy użyć komendy Dodanie grupy SNMP (Add Community for SNMP - ADDCOMSNMP). Dodatkowo, aby uniemożliwić menedżerom w grupie dostęp do obiektów MIB, można parametrowi OBJACC komend ADDCOMSNMP lub CHGCOMSNMP nadać wartość *NONE. Jest to działanie tymczasowe, służące zablokowaniu dostępu do menedżerów w grupie, bez usuwania grupy.

Ochrona serwera INETD

W przeciwieństwie do większości serwerów TCP/IP, serwer INETD nie udostępnia klientom ani jednej usługi. Udostępnia natomiast wiele różnych usług, które mogą być dostosowywane przez administratorów. Z tego powodu serwer INETD jest często nazywany ″super serwerem″. Serwer INETD ma wbudowane następujące usługi:

- time,
- daytime,
- echo,
- discard,
- changed.

Usługi te są obsługiwane zarówno dla protokołu TCP, jak i dla protokołu UDP. W przypadku protokołu UDP, usługi echo, time, daytime i changed odbierają pakiety UDP, a następnie

przesyłają je z powrotem do nadawcy. Serwer echo odsyła z powrotem odebrane pakiety, serwery time i daytime generują czas w specyficznym formacie i odsyłają z powrotem, a serwer changed generuje znaki ASCII, które mogą być wydrukowane, i wysyła je z powrotem.

Natura tych usług UDP stwarza dla systemu zagrożenie atakiem typu ″denial of service″. Załóżmy na przykład, że istnieją dwa serwery iSeries: SYSTEM A i SYSTEM B. Nieuczciwy programista może sfałszować nagłówek IP i nagłówek UDP podając adres źródłowy SYSTEMU A i numer portu UDP serwera time. Następnie może wysłać ten pakiet do serwera time SYSTEMU B, który odeśle czas do SYSTEMU A, a ten z powrotem do SYSTEMU B i tak dalej, generując ciągłą pętlę pochłaniającą zasoby procesora w obydwu systemach, a także zajmującą pasmo sieciowe.

Dlatego należy ocenić ryzyko takiego ataku w przypadku danego systemu iSeries i uruchamiać te usługi tylko w sieci chronionej. Dostarczany serwer INETD jest skonfigurowany tak, aby nie uruchamiać się automatycznie wraz z TCP/IP. Można skonfigurować uruchamianie poszczególnych usług wraz z uruchomieniem serwera INETD. Domyślnie wraz z uruchomieniem serwera INETD uruchamiane są serwery time i daytime dla TCP i UDP.

Istnieją dwa pliki konfiguracyjne serwera INETD:

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

Pliki te określają, które programy są uruchamiane wraz z uruchomieniem serwera INEDT. Określają one również, z jakim profilem użytkownika wykonywane są te programy, gdy uruchamia je serwer INETD.

Uwaga: Plik konfiguracyjny w katalogu ProdData nie powinien być nigdy modyfikowany. Jest on wymieniany przy każdym przeładowaniu systemu. Zmiany konfiguracji dokonane przez użytkownika powinny być zapisane w pliku w katalogu UserData, ponieważ ten plik **nie** jest aktualizowany podczas aktualizowania wersji.

Nieuczciwy programista, mając dostęp do tych plików, mógłby skonfigurować je tak, aby wraz ze startem serwera INETD uruchamiany był dowolny program. Dlatego bardzo ważne jest zabezpieczenie tych plików. Domyślnie, do zmiany tych plików wymagane są uprawnienia QSECOFR. Nie należy zmniejszać uprawnień umożliwiających dostęp do tych plików.

Uwaga: Nie wolno modyfikować pliku konfiguracyjnego w katalogu ProdData. Jest on wymieniany przy każdym przeładowaniu systemu. Zmiany konfiguracji dokonane przez użytkownika powinny być zapisane w pliku w katalogu UserData, ponieważ ten plik nie jest aktualizowany podczas aktualizowania wersji.

Ochrona ograniczania swobodnego dostępu TCP/IP

W przypadku, gdy system lokalny jest podłączony do sieci, może być użyteczne ograniczenie swobodnego dostępu użytkowników do sieci poprzez aplikacje TCP/IP. Jedną z metod jest ograniczenie dostępu do następujących komend klientów TCP/IP:

Uwaga: Komendy te mogą znajdować się w kilku bibliotekach w systemie lokalnym. Między innymi są one na pewno w bibliotekach QSYS i QTCP. Należy zlokalizować i zabezpieczyć te komendy wszędzie tam, gdzie się znajdują.

- STRTCPFTP
- FTP
- STRTCPTELN

- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD (klient REXEC)

Możliwe cele wędrówek sieciowych użytkowników to:

- Pozycje lokalnej tabeli hostów TCP/IP.
- Pozycja *DFTROUTE w tabeli trasy TCP/IP. Pozwala to użytkownikom podać adres IP następnego z kolei systemu, gdy ich celem jest nieznana sieć. Użytkownik może dotrzeć do zdalnej sieci, korzystając z domyślnej trasy.
- Konfiguracja zdalnego serwera nazw. Obsługa ta umożliwia innemu serwerowi w sieci określić nazwy hostów dla lokalnych użytkowników.
- Tabela zdalnego systemu.

Należy kontrolować użytkowników uprawnionych do dodawania pozycji do tych tabel i zmiany konfiguracji. Trzeba także zdawać sobie sprawę z implikacji pozycji lokalnych tabel i konfiguracji.

Zaawansowany użytkownik, który ma dostęp do kompilatora ILE C, może utworzyć program gniazda umożliwiający podłączenie do portu TCP lub UDP. Można to utrudnić, ograniczając dostęp do następujących zbiorów interfejsu gniazd w bibliotece QSYSINC:
- SYS,
- NETINET,
- H,
- ARPA,
- gniazda i warstwa SSL.

Można ograniczyć użycie aplikacji gniazd i SSL, które są już skompilowane, ograniczając użycie następujących programów serwisowych:
- QSOSRV1,
- QSOSRV2,
- QSOSKIT(SSL),
- QSOSSLSR(SSL).

Programy serwisowe są dostarczane z uprawnieniami publicznymi *USE, ale można je zmienić na *EXCLUDE (lub inne, zgodnie z potrzebami).

Rozdział 14. Ochrona dostępu do stacji roboczych

Wielu użytkowników systemu dysponuje komputerami osobistymi (PC) i wykorzystuje je jako stacje robocze. Użytkownicy ci używają narzędzi, które działają na komputerze PC, i używają komputera PC do połączenia się z serwerem iSeries.

Większość metod połączenia komputera PC z serwerem iSeries udostępnia więcej funkcji niż emulacja stacji roboczej. Komputer PC może być traktowany jak terminal iSeries i, po wpisaniu się użytkownika, uruchamiać interaktywne sesje. Ponadto komputer PC może być traktowany przez serwer iSeries jako inny komputer i dostarczać funkcji, takich jak przesyłanie plików i zdalne wywoływanie procedur.

Administrator ochrony serwera iSeries musi znać:

- funkcje dostępne dla użytkowników komputerów PC, którzy są połączeni z systemem,
- zasoby serwera iSeries dostępne dla użytkowników komputerów PC.

Jeśli schemat ochrony serwera iSeries nie jest jeszcze odpowiednio przygotowany, korzystne może być zablokowanie zaawansowanych funkcji PC, takich jak przesyłanie plików i zdalne wywoływanie procedur. Zazwyczaj długofalowym celem jest udostępnienie zaawansowanych funkcji PC z jednoczesną ochroną informacji w systemie. Poniższe sekcje przedstawiają niektóre zagadnienia związane z ochroną dotyczące dostępu do systemu za pomocą komputera PC.

Blokowanie wirusów na stacjach roboczych

W sekcji tej opisano możliwe sposoby ochrony przed wirusami pochodzącymi z komputerów PC.

Ochrona dostępu do danych stacji roboczych

Niektóre aplikacje klientów PC zapisują informacje w serwerze w folderach współużytkowanych. Aby uzyskać dostęp do zbiorów baz danych iSeries, użytkownik PC korzysta z ograniczonego, dokładnie zdefiniowanego zestawu interfejsów. Za pomocą oprogramowania służącego do przesyłania plików, dostępnego w większości systemów klient/serwer, użytkownik komputera PC może kopiować pliki między serwerem a komputerem PC. Dzięki możliwościom dostępu do baz danych poprzez plik DDM, zdalny SQL lub sterownik ODBC, użytkownik komputera PC ma dostęp do danych w serwerze.

W takim środowisku można utworzyć programy służące do przechwytywania i oceniania żądań użytkownika komputera PC, kierowanych do zasobów serwera. Jeśli żądania wykorzystują plik DDM, program obsługi wyjścia można określić w atrybucie sieciowym dostępu do zarządzania danymi rozproszonymi (DDMACC). W przypadku niektórych metod przesyłania plików PC, program obsługi wyjścia można określić w atrybucie sieciowym żądania dostępu klienta (PCSACC). Można również podać atrybut PCSACC (*REGFAC), aby wykorzystywana była funkcja rejestracji. Jeśli do dostępu do danych żądania używają innych funkcji serwera, można użyć komendy WRKREGINF do zarejestrowania programów obsługi wyjścia dla tych funkcji.

Czasami jednak trudno zaprojektować programy obsługi wyjścia tak, aby w pełni zabezpieczały dane. Programy obsługi wyjścia nie zastępują uprawnień do obiektów, które zostały zaprojektowane do zabezpieczania obiektów przed nieuprawnionym dostępem z dowolnego źródła.

Niektóre aplikacje klienckie, na przykład IBM iSeries Access for Windows, używają zintegrowanego systemu plików do przechowywania i dostępu do danych w serwerze iSeries. Dzięki zintegrowanemu systemowi plików cały serwer staje się dużo dostępniejszy dla użytkowników komputerów PC. Uprawnienia do obiektów stają się jeszcze ważniejsze. Za pomocą zintegrowanego systemu plików użytkownik o odpowiednich uprawnieniach może przeglądać bibliotekę serwera tak, jakby była katalogiem na komputerze PC. Za pomocą prostych komend przenoszenia i kopiowania można przenosić dane między biblioteką serwera iSeries a katalogiem PC. System automatycznie zmienia format danych.

Uwagi:

1. Do sterowania użyciem obiektów w systemie plików QSYS.LIB można użyć listy autoryzacji. Więcej informacji na ten temat zawiera sekcja “Ograniczanie dostępu do systemu plików QSYS.LIB” na stronie 97.
2. Rozdział 11, “Używanie Zintegrowanego systemu plików do ochrony plików”, na stronie 91 zawiera więcej informacji dotyczących ochrony w zintegrowanym systemie plików.

Siłą zintegrowanego systemu plików jest jego prostota dla użytkowników i projektantów. Za pomocą pojedynczego interfejsu użytkownik może pracować z obiektami w wielu środowiskach. Aby uzyskać dostęp do obiektów, użytkownik komputera PC nie potrzebuje specjalnego oprogramowania ani funkcji API. Zamiast tego może on korzystać ze znanych komend używanych na komputerach PC lub użyć metody “wskazywania i kliknięcia”, aby pracować bezpośrednio z obiektami.

W przypadku wszystkich systemów, do których są podłączone komputery PC, a w szczególności w przypadku systemów z oprogramowaniem klienta wykorzystującym zintegrowany system plików, posiadanie dobrego schematu uprawnień do obiektów jest bardzo ważne. Ponieważ ochrona jest zintegrowana z OS/400, wszystkie żądania dostępu do danych muszą przechodzić przez proces sprawdzania uprawnień. Sprawdzanie uprawnień ma miejsce w przypadku żądań kierowanych z każdego źródła i w przypadku każdej metody dostępu do danych.

Uprawnienia do obiektów z dostępem do stacji roboczej

W czasie konfigurowania uprawnień do obiektów należy ocenić, co dane uprawnienie daje użytkownikowi komputera PC. Na przykład gdy użytkownik ma uprawnienie *USE do zbioru, to może on przeglądać lub drukować dane z tego zbioru. Użytkownik ten nie może zmieniać informacji w zbiorze ani go usunąć. W przypadku użytkownika komputera PC przeglądanie jest równoznaczne z “odczytem”, co oznacza, że ma on wystarczające uprawnienia do wykonania kopii tego zbioru na komputerze PC. Taka sytuacja może być niepożądana.

W przypadku niektórych newralgicznych zbiorów konieczne jest ustawienie uprawnienia publicznego *EXCLUDE, aby zapobiec pobieraniu zbioru. Następnie można udostępnić inną metodę “przeglądania” zbioru w serwerze. Może to być na przykład użycie menu i programów wykorzystujących uprawnienie adoptowane.

Innym sposobem zapobiegającym pobieraniu zbioru jest użycie programu obsługi wyjścia, który jest uruchamiany za każdym razem, gdy użytkownik komputera PC uruchamia funkcję serwera (inną niż interaktywne wpisanie się). Program obsługi wyjścia można podać w atrybucie sieciowym PCSACC poprzez użycie komendy Zmiana atrybutów sieciowych (Change Network Attribute - CHGNETA). Programy obsługi wyjścia można też rejestrować za pomocą komendy Praca z informacją rejestracyjną (Work with Registration Information - WRKREGINF). Wybór odpowiedniej metody zależy od tego, w jaki sposób komputery PC uzyskują dostęp do danych w systemie i jakie programy klienta są do tego celu wykorzystywane. Program obsługi wyjścia (QIBM_QPWFS_FILE_SERV) jest wykorzystywany w przypadku dostępu do zintegrowanego systemu plików z oprogramowania

iSeries Access i Net Server. Nie chroni on przed dostępem z komputera PC dysponującego innymi mechanizmami, takimi jak FTP i ODBC.

Oprogramowanie komputera PC zazwyczaj udostępnia także opcję przesyłania danych, dzięki której użytkownik może kopiować dane z komputera PC do zbioru bazy danych serwera. Jeśli nie skonfiguruje się odpowiednio uprawnień, użytkownik ten ma możliwość nadpisania wszystkich danych znajdujących się w zbiorze danymi pochodzącymi z komputera PC. Uprawnienie *CHANGE należy nadawać bardzo ostrożnie. Aby zrozumieć, jakie uprawnienia są wymagane do działania na zbiorach, należy przeczytać Dodatek D w książce *iSeries Ochrona*.

Więcej informacji na temat uprawnień dla funkcji PC i korzystania z programów obsługi wyjścia zawiera Centrum informacyjne iSeries. Więcej informacji na ten temat zawiera sekcja “Informacje wstępne i pokrewne” na stronie xii.

Administrowanie aplikacjami

Administrowanie aplikacjami jest komponentem iSeries Navigator, instalowanym opcjonalnie i stanowi graficzny interfejs użytkownika serwera iSeries. Administrowanie aplikacjami umożliwia administratorom systemu sterowanie udostępnianiem funkcji i aplikacji użytkownikom i grupom w danym serwerze. Umożliwia ona między innymi sterowanie dostępem do funkcji użytkowników uzyskujących dostęp do serwera z aplikacji klientów. Należy być świadomym, że jeżeli korzysta się z serwera iSeries za pośrednictwem klienta dla Windows, dostępne funkcje zależą od uprawnień użytkownika serwera iSeries, a nie od uprawnień użytkownika Windows.

Kompletna dokumentacja na temat Administracji aplikacji iSeries Navigator, znajduje się w Centrum informacyjnym iSeries –>Connecting to iSeries—>What to connect with—>iSeries Navigator (../html/as400/v5r2/ic2924/info/rzaj3/rzaj3overview.htm).

Administrowanie strategiami

Strategie są narzędziem wykorzystywanym przez administratorów do konfiguracji oprogramowania na komputerach PC. Mogą one ograniczać funkcje i aplikacje dostępne dla użytkownika komputera PC. Strategie mogą także sugerować lub narzucać konfiguracje wykorzystywane przez określonych użytkowników lub na określonych komputerach.

Uwaga: Strategie nie umożliwiają kontroli zasobów serwera. Nie zastępują też jego ochrony. Strategii można użyć do określenia sposobu, w jaki użytkownik iSeries Access może korzystać z serwera na określonym komputerze PC. Nie wpływają one na inne mechanizmy dostępu do zasobów serwera.

Strategie są przechowywane na serwerze plików. Za każdym razem, gdy użytkownik wpisuje się do systemu na stacji roboczej Windows, strategie, które się do niego odnoszą, są ładowane z serwera plików. Zostają one zastosowane do rejestru systemowego, zanim użytkownik będzie mógł podjąć jakiekolwiek działanie.

Strategie Microsoft a Administrowanie aplikacjami

iSeries Access Express obsługuje dwie strategie implementacji kontroli administracyjnej w sieci: strategie systemowe firmy Microsoft i Administrowanie aplikacjami w programie iSeries Navigator. Przy podejmowaniu decyzji o wyborze strategii warto rozważyć poniższe uwagi.

Strategie systemowe Microsoft

Strategie są związane z komputerem PC, nie zależą od konkretnego wydania systemu OS/400. Strategie mogą odnosić się do komputerów PC lub do użytkowników Windows. Użytkownicy

oznaczają w tym przypadku profile użytkowników Windows, a nie profile użytkowników serwera. Strategii można użyć do ″konfigurowania″ i ograniczania uprawnień. Strategie umożliwiają zazwyczaj dokładniejsze określanie uprawnień niż Administrowanie aplikacjami i udostępniają szerszy zakres funkcji. Wynika to z faktu, że połączenie z serwerem nie jest konieczne, aby ustalić, czy użytkownik może korzystać z określonej funkcji. Implementowanie strategii jest bardziej skomplikowane niż implementowanie Administracji aplikacji, wymaga bowiem wykorzystania edytora strategii systemowych Microsoft, a każdy z komputerów PC musi zostać osobno skonfigurowany do pobierania strategii.

Administrowanie aplikacjami w programie iSeries Navigator

Administrowanie aplikacjami, w przeciwieństwie do systemowych strategii firmy Microsoft, czerpie dane z profilu użytkownika serwera, a nie z profilu użytkownika Windows. Administrowanie aplikacjami jest dostępne na serwerach iSeries z systemami operacyjnymi OS/400 w wersji V4R3 lub nowszej, lecz niektóre funkcje są dostępne dopiero od wersji V4R4. Administrowanie aplikacjami wykorzystuje graficzny interfejs użytkownika programu iSeries Navigator, który jest o wiele łatwiejszy w użyciu niż edytor strategii. Dane wykorzystywane przez Administrację aplikacji stosują się do użytkownika niezależnie od tego, z którego komputera PC wpisuje się on do systemu. Można ograniczyć dostęp użytkowników do określonych funkcji programu iSeries Navigator. Wykorzystanie Administracji aplikacji zaleca się w przypadku, gdy wszystkie funkcje, które mają zostać ograniczone, są dostępne dla Administracji aplikacji i jeśli używana wersja OS/400 obsługuje to oprogramowanie.

Używanie SSL z iSeries Access for Windows

Więcej informacji na temat korzystania z SSL w aplikacji iSeries Access Express zawierają tematy Centrum informacyjnego iSeries *Administrowanie SSL, Ochrona iSeries Access Express i iSeries Navigator, iSeries Developer Kit for Java , i iSeries Java Toolbox* w głównej sekcji Java. Informacje te dostępne są również na dysku CD-ROM dostarczanym z danym systemem iSeries.

Ochrona iSeries Navigator

iSeries Navigator to wygodny interfejs serwera, przeznaczony dla użytkowników iSeries Access. Każda nowa wersja OS/400 udostępnia więcej funkcji serwera iSeries poprzez iSeries Navigator. Korzystanie z wygodnego interfejsu daje wiele korzyści, w tym ograniczenie kosztów obsługi technicznej i lepszy obraz danego systemu. Z drugiej strony nakłada on na administratora pewne obowiązki związane z ochroną.

Administrator ochrony nie może już zakładać, że niewiedza użytkowników stanowi wystarczające zabezpieczenie zasobów. Za pomocą aplikacji iSeries Navigator wiele funkcji staje się widocznych i prostych w użyciu dla użytkowników. Należy zgodnie z potrzebami zaprojektować i zaimplementować strategie ochrony dla profili użytkowników i obiektów.

Wersja V4R4 i poźniejsze oprogramowania IBM e(logo)server iSeries Access for Windows zawiera następujące metody do sterowania funkcjami, które użytkownicy mogą wykonywać poprzez iSeries Navigator:

- instalacja selektywna,
- Administrowanie aplikacjami,
- obsługa strategii systemowych Windows NT.

iSeries Navigator jest podzielony na wiele komponentów, które można oddzielnie instalować. Umożliwia to zainstalowanie tylko wymaganych funkcji. Administrowanie aplikacjami umożliwia administratorowi sterowanie funkcjami, do których użytkownik lub grupa może mieć dostęp poprzez iSeries Navigator. Administrowanie aplikacjami dzieli aplikacje na następujące kategorie:

iSeries Navigator
Kategoria ta obejmuje oprogramowanie iSeries Navigator i moduły dodatkowe.

Aplikacje klienckie
Kategoria ta obejmuje wszystkie pozostałe aplikacje klienckie, w tym iSeries Access, udostępniające funkcje do pracy z klientami, którzy są administrowani przez komponent Administrowanie aplikacjami.

Aplikacje hosta
Ta kategoria obejmuje wszystkie aplikacje, które są zainstalowane w całości w serwerze i dostarczają funkcji, które są administrowane za pomocą Administracji aplikacji.

Instalacji selektywnej, Administracji aplikacji i strategii ochrony można używać do ograniczania funkcji iSeries Navigator dostępnych dla użytkownika. Elementów tych nie można jednak używać do ochrony zasobów.

Począwszy od wersji V4R4, IBM e(logo)server iSeries Access for Windows umożliwia również wykorzystanie edytora strategii systemowych Windows NT do określenia, które funkcje mogą być wykonywane z danego komputera PC, niezależnie od użytkownika, który go używa.

Centrum informacyjne iSeries zawiera pozostałe informacje na temat instalacji selektywnej, Administracji aplikacji i Administracji strategiami. Sekcja “Ograniczenie dostępu do funkcji programu” na stronie 5 również zawiera częściowe omówienie Administracji aplikacji.

Zabezpieczenie przed dostępem interfejsu ODBC

Technologia ODBC jest narzędziem, którego aplikacje PC mogą używać w celu uzyskania dostępu do danych iSeries tak, jakby dane były danymi komputera PC. Programista ODBC może sprawić, że fizyczne położenie danych będzie niewidoczne dla użytkownika aplikacji PC. Więcej informacji na temat ochrony interfejsu ODBC znajduje się w Centrum informacyjnym iSeries w artykule ″Ochrona ODBC w iSeries Access for Windows″ (/rzaii/rzaiiodbc09.HTM).

Ochrona haseł sesji stacji roboczej

Zazwyczaj gdy użytkownik PC uruchamia oprogramowanie nawiązujące połączenie, takie jak iSeries Access, podaje tylko raz identyfikator użytkownika i hasło dostępu do serwera. Hasło jest zaszyfrowane i przechowywane w pamięci komputera PC. Za każdym razem, gdy użytkownik ustanawia nową sesję z tym samym serwerem, komputer PC wysyła automatycznie identyfikator użytkownika i hasło.

Niektóre oprogramowanie klient/serwer umożliwia również ominięcie ekranu wpisania się w przypadku sesji interaktywnych. Oprogramowanie wysyła identyfikator użytkownika i zaszyfrowane hasło, gdy użytkownik uruchamia interaktywną sesję (emulacja terminalu 5250). Aby ta opcja była obsługiwana, wartość systemowa QRMTSIGN na serwerze musi być ustawiona na *VERIFY.

Jeśli wybiera się omijanie ekranu wpisania się, należy pamiętać o wynikających z tego konsekwencjach.

Ryzyko naruszenia ochrony: W przypadku emulacji terminalu 5250 lub jakiejkolwiek innego typu interaktywnej sesji, ekran Wpisanie się (Sign On) jest traktowany jak każdy inny ekran. Pomimo, że podczas wpisywania hasło nie jest widoczne na ekranie, jest ono przesyłane łączem w postaci niezaszyfrowanej, tak jak ma to miejsce dla każdego innego pola danych. W przypadku niektórych łącz może to stwarzać potencjalnemu intruzowi możliwość

monitorowania łącza i wykrycia identyfikatora i hasła użytkownika. Monitorowanie łącza za pomocą urządzenia elektronicznego bywa często nazywane **węszeniem**. Począwszy od wersji V4R4 można używać warstwy SSL do szyfrowania komunikacji między aplikacją iSeries Access i serwerem iSeries. Dzięki temu dane, łącznie z hasłami, są zabezpieczone przed węszeniem.

Jeśli wybierana jest opcja ominięcia ekranu wpisania się, komputer PC szyfruje hasło przed wysłaniem. Szyfrowanie zabezpiecza przed możliwością wykradzenia hasła poprzez węszenie. Należy jednak sprawdzić, czy użytkownicy PC sami zapewniają rzeczywistą ochronę. Nienadzorowany komputer PC z aktywną sesją w systemie iSeries umożliwia niepowołanej osobie rozpoczęcie innej sesji bez znajomości identyfikatora i hasła użytkownika. Należy skonfigurować blokowanie komputerów PC, gdy system jest nieaktywny przez pewien czas, i wymusić podawanie hasła w celu przywrócenia sesji.

Nawet jeśli nie wybrano opcji ominięcia ekranu wpisania się, komputer PC z aktywną sesją pozostawiony bez nadzoru stanowi zagrożenie ochrony. Za pomocą oprogramowania PC niepowołana osoba może uruchomić sesję z serwerem i mieć dostęp do danych, również bez znajomości identyfikatora i hasła użytkownika. Zagrożenie w przypadku emulacji terminalu 5250 jest większe, ponieważ do uruchomienia sesji i uzyskania dostępu do danych wymagana jest mniejsza wiedza.

Należy także uświadomić użytkownikom skutki rozłączenia sesji iSeries Access. Wielu użytkowników zakłada (co jest logiczne, ale błędne), że opcja odłączenia całkowicie zatrzymuje połączenie z serwerem. W rzeczywistości, gdy użytkownik odłącza się, serwer udostępnia sesję użytkownika (licencję) innemu użytkownikowi. Połączenie użytkownika z serwerem pozostaje jednak nadal otwarte. Inny użytkownik może wykorzystać niezabezpieczony komputer PC i uzyskać dostęp do zasobów serwera bez wprowadzania identyfikatora i hasła użytkownika.

Użytkownikom, którzy chcą odłączyć aktywne sesje, można zasugerować jedną z poniższych możliwości:

- Powinni oni uaktywnić funkcję blokowania na komputerze PC wymagającą podania hasła. Dzięki temu komputer PC pozostawiony bez nadzoru jest niedostępny dla osób nie znających hasła.
- Mogą oni całkowicie odłączyć sesję, wylogowując się z systemu Windows lub restartując (ponownie uruchamiając) komputer PC. Powoduje to zakończenie sesji z systemem iSeries.

Należy również uświadomić użytkownikom potencjalne zagrożenia związane z używaniem oprogramowania iSeries Access for Windows. Gdy użytkownik określa UNC (universal naming convention) w celu zidentyfikowania zasobu iSeries, klient Windows 95 lub Windows NT tworzy połączenie sieciowe, aby połączyć się z serwerem. Ponieważ użytkownik podaje nazwę UNC, nie widzi zasobu jako odwzorowanego dysku sieciowego. Często nie jest on nawet świadomy istnienia połączenia sieciowego. W przypadku nienadzorowanego komputera PC to połączenie sieciowe stanowi zagrożenie ochrony, ponieważ serwer pojawia się w drzewie katalogów na tym komputerze. Jeśli sesję serwera uruchomił użytkownik o dużych uprawnieniach, zasoby stają się łatwo dostępne. Tak jak w poprzednim przykładzie, środkiem zaradczym jest sprawdzenie, czy użytkownicy rozumieją potrzebę ochrony i czy używają funkcji blokowania używanych komputerów PC.

Zabezpieczenie serwera przed zdalnymi komendami i procedurami

Użytkownik PC mający odpowiednią wiedzę i dysponujący oprogramowaniem, takim jak iSeries Access, może uruchamiać komendy w systemie iSeries bez konieczności wpisania się do systemu. Poniżej podano kilka metod, które mogą być stosowane przez użytkowników PC do uruchamiania komend serwera. Oprogramowanie klient/serwer określa metody, którymi dysponują użytkownicy.

- Użytkownik może otworzyć plik DDM i użyć funkcji komendy zdalnej do uruchomienia komendy.
- Niektóre programy, takie jak zoptymalizowani klienci iSeries Access, udostępniają funkcję komendy zdalnej poprzez funkcje API rozproszonego wywołania programu (DPC), bez konieczności używania DDM.
- Niektóre programy, takie jak zdalny SQL i ODBC, udostępniają funkcję komendy zdalnej bez użycia DDM i DPC.

W przypadku oprogramowania klient/serwer używającego DDM do obsługi komend zdalnych do całkowitego zabezpieczenia przed używaniem takich komend można użyć atrybutu sieciowego DDMACC. W przypadku oprogramowania klient/serwer używającego obsługi innego serwera, można zarejestrować programy obsługi wyjścia dla tego serwera. Jeśli użycie komend zdalnych ma być dopuszczalne, należy sprawdzić, czy schemat uprawnień do obiektów odpowiednio zabezpiecza dane. Możliwość używania komend zdalnych jest równoznaczna z udostępnieniem użytkownikowi wiersza komend. Ponadto, gdy iSeries otrzymuje komendę zdalną poprzez DDM, system nie wymusza ustawienia w profilach użytkowników parametru Ograniczone możliwości (Limited capability - LMTCPB).

Zabezpieczenie stacji roboczych przed zdalnymi komendami i procedurami

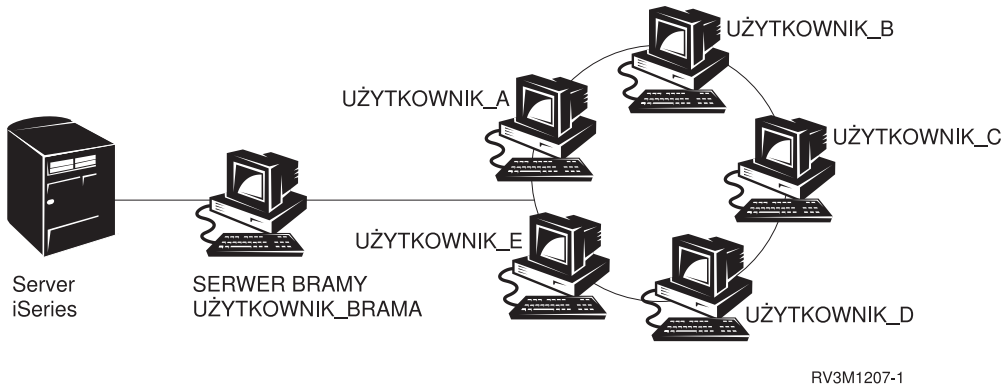
Oprogramowanie IBM iSeries Access for Windows jest przykładem oprogramowania umożliwiającego odbieranie zdalnych komend na komputerze PC. Aby uruchomić procedurę na podłączonym komputerze PC, można użyć komendy Uruchomienie zdalnej komendy (Run Remote Command - RUNRMTCMD) w serwerze. Komenda RUNRMTCMD jest cennym narzędziem dla administratorów systemów i personelu pomocy telefonicznej. Daje ona również możliwość uszkodzenia danych na komputerze PC, albo w sposób zamierzony, albo przypadkowo.

Komputery PC nie mają takich samych funkcji uprawnień do obiektów, jak serwer iSeries. Najlepszą ochroną przed problemami związanymi z użyciem komendy RUNRMTCMD jest ścisłe określenie użytkowników serwera iSeries, mających do niego dostęp. Oprogramowanie IBM iSeries Access for Windows jest przykładem oprogramowania umożliwiającego uruchamianie zdalnych komend na komputerze PC. Jeśli połączenie jest nawiązywane poprzez protokół TCP/IP, można użyć po stronie klienta panelu sterowania, na którym są dostępne właściwości, aby sterować dostępem do zdalnych komend. Uprawnienie do używania zdalnych komend można nadawać podając ID użytkownika lub nazwę systemu zdalnego. Jeśli połączenie jest nawiązywane poprzez sieć SNA, niektóre oprogramowanie klienta umożliwia skonfigurowanie ochrony dla konwersacji. W przypadku pozostałego oprogramowania klienta użytkownik decyduje, czy skonfigurować obsługę komend przychodzących.

W przypadku każdej kombinacji oprogramowania klienta i typu połączenia należy rozważyć możliwość potencjalnego użycia komend przychodzących na podłączonych komputerach PC. Należy zapoznać się z dokumentacją klienta wyszukując terminów “komenda przychodząca” “(incoming command)” i “RUNRMTCMD”. Należy również doradzić użytkownikom komputerów PC i administratorom sieci, jak poprawnie (bezpiecznie) skonfigurować klientów, aby umożliwiali lub uniemożliwiali korzystanie z tej funkcji.

Serwery bram

W sieci między systemem iSeries a komputerami PC może znajdować się serwer pośredni lub serwer bramy. Na przykład system iSeries może być podłączony do sieci LAN z serwerem PC, do którego są podłączone komputery PC. W takim przypadku sposób ochrony zależy od możliwości oprogramowania działającego na serwerze bramy. Rys. 13 przedstawia przykład konfiguracji z serwerem bramy:



Rysunek 13. System iSeries z serwerem bramy

W przypadku niektórych programów system iSeries nie będzie wiedział o użytkownikach (na przykład o UŻYTKOWNIK_A i UŻYTKOWNIK_B) znajdujących się za serwerem bramy. Serwer zostanie wpisany do systemu jako pojedynczy użytkownik (UŻYTKOWNIK_BRAMA). Użyje on identyfikatora użytkownika UŻYTKOWNIK_BRAMA do obsługi żądań kierowanych przez podlegających mu użytkowników. Żądanie kierowane przez użytkownika UŻYTKOWNIK_A jest widoczne dla serwera jako żądanie od użytkownika UŻYTKOWNIK_BRAMA.

W takim przypadku należy polegać na serwerze bramy, że zapewni on odpowiednią ochronę. Należy rozumieć i zarządzać możliwościami zapewnienia ochrony przez serwer bramy. Z perspektywy serwera iSeries każdy użytkownik ma takie same uprawnienia, jak użytkownik o identyfikatorze używanym przez serwer bramy. Sytuację tę można porównać do uruchomienia programu przejmującego uprawnienia i udostępniającego wiersz komend.

W przypadku pozostałego oprogramowania serwer bramy przekazuje do serwera iSeries żądania od pojedynczych użytkowników. Serwer iSeries wie, że UŻYTKOWNIK_A żąda dostępu do danego obiektu. Brama jest prawie przezroczysta dla serwera iSeries.

Jeśli system znajduje się w sieci z serwerami bram, należy oszacować, jak szerokie uprawnienia nadać identyfikatorom użytkowników używanym przez serwery bram. Należy również rozumieć:
- mechanizm ochrony wymuszany przez serwery bram,
- sposób widzenia użytkowników znajdujących się za serwerem bramy przez system iSeries.

Bezprzewodowa komunikacja w sieci LAN

Niektórzy klienci mogą używać do komunikacji z systemem bezprzewodowej sieci LAN iSeries. Bezprzewodowa sieć LAN iSeries wykorzystuje technologię komunikacji na częstotliwościach radiowych. Administrator ochrony powinien znać przedstawione poniżej charakterystyki produktów sieci bezprzewodowych LAN iSeries.

- Omawiane produkty bezprzewodowych sieci LAN używają technologii rozszerzonego spektrum. Ta sama technologia była używana w przeszłości przez rząd do zapewniania

ochrony transmisjom radiowym. Osoby usiłujące elektronicznie monitorować transmisje danych odbierają szumy, a nie rzeczywistą transmisję.

- Połączenie bezprzewodowe charakteryzują trzy parametry konfiguracyjne dotyczące ochrony:
  - szybkość transmisji (dwie możliwe szybkości transmisji),
  - częstotliwość (pięć możliwych częstotliwości),
  - identyfikator systemu (8 milionów możliwych identyfikatorów).

  Podane elementy konfiguracyjne stosowane łącznie dają 80 milionów możliwych konfiguracji, przez co prawdopodobieństwo odgadnięcia przez hakera poprawnej konfiguracji staje się bardzo małe.
- Tak jak w przypadku innych metod komunikacji, ochrona komunikacji bezprzewodowej zależy od ochrony urządzenia klienta. Informacja o identyfikatorze systemu i inne parametry konfiguracji są zapisane w pliku na urządzeniu klienta i powinny być zabezpieczone.
- Jeśli urządzenie bezprzewodowe zostanie zagubione lub skradzione, normalne procedury ochrony serwera, takie jak hasła wpisania się i ochrona obiektu zapewniają ochronę, gdy nieuprawniony użytkownik będzie próbował użyć zagubionej lub skradzionej jednostki w celu uzyskania dostępu do systemu.
- Jeśli jednostka klienta bezprzewodowego zostanie zagubiona lub skradziona, należy wziąć pod uwagę zmianę informacji o identyfikatorach w systemie dla wszystkich użytkowników, punktów dostępu i systemów. Przypomina to zmianę zamków w drzwiach, gdy skradziono klucze.
- Należy rozważyć podział serwera na grupy klientów dysponujących unikalnymi identyfikatorami systemowymi. Ogranicza to problemy, gdy jednostka zostanie zagubiona lub skradziona. Metoda ta jest skuteczna tylko wtedy, gdy można ograniczyć grupę użytkowników do konkretnej części instalacji.
- W przeciwieństwie do technologii LAN, technologia bezprzewodowych sieci LAN jest prawnie zastrzeżona. Tak więc w przypadku sieci bezprzewodowych tego typu nie są ogólnie dostępne żadne narzędzia do podsłuchiwania. Narzędzie służące do podsłuchiwania jest urządzeniem elektronicznym służącym do nieuprawnionego monitorowania transmisji.

Rozdział 15. Ochrona za pomocą programów obsługi wyjścia

Niektóre funkcje serwera iSeries udostępniają punkt wyjścia, aby system mógł uruchomić program utworzony przez użytkownika w celu wykonania dodatkowej kontroli i weryfikacji. Na przykład można skonfigurować system tak, aby uruchamiał program obsługi wyjścia za każdym razem, gdy ktoś spróbuje otworzyć plik DDM (distributed data management) w systemie. Aby określić program obsługi wyjścia, który jest uruchamiany po spełnieniu konkretnych warunków, można użyć funkcji rejestrowania.

Wiele publikacji na temat systemu iSeries zawiera przykłady programów obsługi wyjścia realizujących funkcje ochrony. Tabela 24 zawiera listę takich programów obsługi wyjścia oraz informacje o tym, gdzie można znaleźć kody źródłowe przykładowych programów.

Tabela 24. Kody źródłowe przykładowych programów obsługi wyjścia

Typ programu obsługi wyjścia	**Składnik**	**Gdzie można znaleźć przykład**
Weryfikacja hasła	Wartość systemowa QPWDVLDPGM może określać nazwę programu. Może też informować o tym, że programy weryfikujące, zarejestrowane dla punktu wyjścia QIBM_QSY_VLD_PASSWRD, mają być używane do sprawdzania, czy nowe hasło spełnia dodatkowe wymagania, nieobsługiwane przez wartości systemowe QPWDxxx. Używanie tego programu powinno być bardzo dokładnie monitorowane, ponieważ pobiera on nieszyfrowane hasła. Program ten **nie powinien** przechowywać haseł w pliku ani przesyłać ich do innego programu.	• *Książka Implementation Guide for iSeries Security and Auditing, GG24–4200* • *iSeries Ochrona*, SC85-0124-07
Dostęp do PC Support/400 lub Client Access[1]	Nazwę tego pliku należy podać jako wartość parametru atrybutów sieciowych żądanie dostępu klienta (PCSACC). Umożliwia on kontrolę następujących funkcji: • drukarki wirtualnej, • przesyłania plików, • folderów współużytkowanych typu 2, • komunikatów Client Access, • kolejek danych, • zdalnego SQL.	*Książka Implementation Guide for iSeries Security and Auditing, GG24–4200*
Dostęp DDM (Distributed Data Management)	Nazwę tego programu można podać jako wartość parametru żądania dostępu DDM (DDMACC) atrubutów sieciowych, aby sterować następującymi funkcjami: • folderów współużytkowanych typu 0 i 1, • wprowadzania komend zdalnych.	*Książka Implementation Guide for iSeries Security and Auditing, GG24–4200*
Zdalne wpisywanie się	W wartości systemowej QRMTSIGN można określić program umożliwiający sterowanie użytkownikami, którzy mogą się automatycznie wpisywać do systemu z określonego miejsca (tranzyt).	*Książka Implementation Guide for iSeries Security and Auditing, GG24–4200*

Tabela 24. Kody źródłowe przykładowych programów obsługi wyjścia (kontynuacja)

Typ programu obsługi wyjścia	**Składnik**	**Gdzie można znaleźć przykład**
Open Database Connectivity (ODBC) with iSeries Access[1]	Steruje następującymi funkcjami ODBC: • czy ODBC jest udostępnione, • jakie funkcje są dostępne dla zbiorów bazy danych iSeries, • jakie instrukcje SQL są dostępne, • jakie informacje można uzyskać na temat obiektów serwera bazy danych, • jakie funkcje katalogowe SQL są dostępne.	Żadne nie są dostępne.
Program obsługi przerwania QSYSMSG	Można utworzyć program do monitorowania kolejki komunikatów QSYSMSG i do wykonywania odpowiednich działań (takich jak powiadamianie administratora ochrony) w zależności od typu komunikatu.	*Książka Implementation Guide for iSeries Security and Auditing, GG24–4200*
TCP/IP	Wiele serwerów TCP/IP (takich jak FTP, TFTP, TELNET i REXEC) dostępnia punkty wyjścia. Można dodać program obsługi wyjścia do obsługi logowania i do weryfikacji żądań użytkowników, takich jak żądania pobrania lub wysłania konkretnego pliku. Można ich także użyć w celu udostępnienia w danym systemie anonimowego FTP.	"Punkty wyjścia TCP/IP w książce *iSeries System API Reference*"
Zmiany profilu użytkownika	Można utworzyć programy obsługi wyjścia dla następujących komend dotyczących profilu użytkownika: CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• *iSeries Ochrona*, SC85-0124-07 • "Punkty wyjścia TCP/IP w książce *iSeries System API Reference*"

Uwagi:

1. Pozostałe informacje na ten temat zawiera Centrum informacyjne systemu iSeries (patrz "Informacje wstępne i pokrewne" na stronie xii).

Rozdział 16. Ochrona przeglądarek internetowych

Wielu użytkowników komputerów PC w danej organizacji ma na swoich stacjach roboczych zainstalowane przeglądarki. Mogą się oni łączyć z Internetem. Mogą się także łączyć z danym serwerem iSeries. Poniżej przedstawiono uwagi na temat ochrony dotyczące zarówno komputerów PC, jak i serwera iSeries.

Ryzyko: uszkodzenia stacji roboczej

Strona WWW odwiedzana przez użytkownika może zawierać ″program″, na przykład aplet w języku Java, element sterujący Active-X lub innego rodzaju komponenty włączalne. Chociaż jest to rzadkością, tego typu ″program″ po uruchomieniu na komputerze PC może uszkodzić informacje, które się w nim znajdują. Administrator ochrony powinien wziąć pod uwagę poniższe uwagi umożliwiające ochronę komputera PC w danej organizacji.

- Zrozumienie opcji ochrony różnych przeglądarek wykorzystywanych przez użytkowników. Na przykład w niektórych przeglądarkach można kontrolować dostęp apletów w języku Java do elementów poza przeglądarką (ograniczone środowisko pracy apletów w języku Java nosi nazwę *klienta testowego*). Uniemożliwia to uszkodzenie przez aplety danych znajdujących się w komputerze PC.

  Uwaga: Idea sandbox i związane z tym ograniczenia dotyczące ochrony nie mają zastosowania dla Active-X i innych dodatków.
- Użytkownikom należy zalecić odpowiednie skonfigurowanie przeglądarek. Prawdopodobnie administrator nie ma czasu i możliwości, aby sprawdzić, czy użytkownicy stosują się do jego zaleceń. Dlatego należy ich poinformować o potencjalnym ryzyku, jakie niesie ze sobą niewłaściwe skonfigurowanie przeglądarki.
- Należy wziąć pod uwagę standaryzację przeglądarek WWW udostępniających potrzebne opcje ochrony.
- Należy poinstruować użytkowników, aby informowali o każdym podejrzanym zachowaniu lub objawach, które można powiązać z konkretnym serwisem WWW.

Ryzyko: dostęp do katalogów iSeries poprzez odwzorowane napędy

Załóżmy, że komputer PC jest połączony z serwerem w sesji IBM iSeries Access dla Windows. Sesja konfiguruje odwzorowane napędy tak, aby je połączyć ze zintegrowanym systemem plików iSeries. Na przykład dysk **G** komputera PC może być odwzorowany w sieci przez zintegrowany system plików jako SYSTEM1.

Przyjmijmy teraz, że ten sam użytkownik PC ma przeglądarkę i dostęp do Internetu. Użytkownik żąda pobrania strony WWW, z której jest uruchamiany szkodliwy ″program″, na przykład aplet w języku Java lub element sterujący Active-X. Nie jest wykluczone, że program mógł podjąć próbę usunięcia wszystkich informacji z dysku G komputera PC.

Aby uniknąć uszkodzeń odwzorowanych napędów, można użyć szeregu zabezpieczeń:

- Najważniejszym zabezpieczeniem jest ochrona zasobów w serwerze iSeries. Aplet w języku Java lub element sterujący Active-X łączy się z serwerem iSeries tak jak użytkownik, który ustanawia sesję PC. Należy zwracać szczególną uwagę podczas nadawania użytkownikom PC uprawnień do pracy w serwerze iSeries.

- Należy poinformować użytkowników PC, aby skonfigurowali swoje przeglądarki tak, aby uniemożliwiały dostęp do odwzorowanych napędów. Działa to tylko w przypadku apletów w języku Java, nie działa natomiast w przypadku elementów sterujących Active-X, które nie mają klienta testowego.
- Należy poinformować użytkowników o niebezpieczeństwch, jakie niesie ze sobą łączenie się z serwerem iSeries i Internetem w tej samej sesji. Należy się także upewnić, czy użytkownicy PC (uruchamiający na przykład klientów Windows 95) są świadomi, że odwzorowanie dysków nie jest przerywane po zakończeniu sesji iSeries Access.

Ryzyko: zaufanie do podpisanych apletów

Użytkownicy mogą postępować zgodnie ze wskazówkami administratora i skonfigurować przeglądarki tak, aby uniemożliwiały zapisywanie apletów na dyski komputera PC. Jednakże użytkownicy komputerów PC muszą postępować ostrożnie, ponieważ *podpisany aplet* może nadpisać ustawienia przeglądarki.

Podpisany aplet ma przypisany podpis cyfrowy umożliwiający jego weryfikację. Gdy użytkownik uzyskuje dostęp do strony WWW zawierającej podpisany aplet, wyświetlany jest komunikat. Określa on podpis apletu (kto go podpisał i kiedy). Po zaakceptowaniu apletu użytkownik pobiera go i zmienia ustawienia ochrony w przeglądarce. Podpisany aplet ma uprawnienia do zapisu na lokalnym napędzie komputera osobistego, nawet jeśli domyślne ustawienia przeglądarki zabraniają tego. Podpisany aplet może także pisać na odwzorowanych dyskach serwera, ponieważ komputer osobisty traktuje je jak napędy lokalne.

W przypadku apletów w języku Java pochodzących z serwera iSeries, może zajść potrzeba wykorzystania podpisów. Należy jednak pouczyć użytkowników, aby nie akceptowali podpisanych apletów pochodzących z nieznanych źródeł.

Rozdział 17. Informacje pokrewne

Podręczniki

- *APPC Programming*, SC41-5443-00, opisuje zaawansowaną obsługę komunikacji pomiędzy programami (APPC) dla systemu iSeries. Książka ta zawiera wskazówki dotyczące tworzenia aplikacji używających APPC i definiowania środowiska komunikacyjnego APPC, a także rozważania dotyczące aplikacji, opis komend i wymagań dotyczących konfiguracji, omówienie zagadnień dotyczących zarządzania problemami dla APPC i ogólne rozważania dotyczące sieci. Więcej informacji na ten temat znajduje się na dysku CD-ROM Centrum Informacyjne iSeries.
- Dokumentacja techniczna *AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet*, SG24-4929, omawia kwestie związane z ochroną i ryzyko związane z podłączaniem serwera iSeries do Internetu. Zawiera przykłady, zalecenia, wskazówki i techniki dotyczące aplikacji TCP/IP.
- *Składowanie i odtwarzanie*, SA12-7269-07, dostarcza informacje na temat planowania strategii składowania i odzyskiwania, składowania danych z systemu i ich odzyskiwania. Więcej informacji na ten temat znajduje się w Centrum informacyjnym iSeries. Dodatkowe informacje na ten temat zawiera także Centrum informacyjne iSeries. Szczegóły znajdują się w sekcji “Informacje wstępne i pokrewne” na stronie xii.
- *CL Programming*, SC41-5721-06, zawiera szczegółowy opis kodowania DDS (data description specifications) dla zbiorów, które mogą mieć zewnętrzny opis. Zbiory te mogą być fizyczne, logiczne, ekranowe, drukarkowe i ICF (intersystem communication function). Więcej informacji na ten temat znajduje się w Centrum informacyjnym iSeries.
- Artykuł CL w Centrum informacyjnym (szczegółowe informacje zawiera sekcja “Informacje wstępne i pokrewne” na stronie xii.) Znajduje się tam opis języka CL (control language) iSeries i komend OS/400. Komendy OS/400 są używane do zgłaszania żądania uruchomienia funkcji programu licencjonowanego (5722-SS1) Operating System/400. Wszystkie pozostałe komendy CL systemów innych niż OS/400, które są powiązane z innymi programami licencjonowanymi, są opisane w książkach dotyczących tych programów licencjonowanych.
- *Implementing iSeries Security, 3rd Edition* by Wayne Madden and Carol Woodbury. Loveland, Colorado: 29th Street Press, oddział Duke Communications International, 1998. Zawiera wskazówki i praktyczne sugestie dotyczące planowania, konfigurowania i zarządzania ochroną iSeries.

  Numer zamówienia ISBN:

  1-882419-78-2
- Więcej informacji na temat serwera HTTTP, znajduje się na stronie WWW pod następującym adresem:

  `http://www.ibm.com/eserver/iseries/software/http/docs/doc.htm`
- *iSeries Ochrona*, SC85-0124-07, zawiera kompletne informacje na temat wartości systemowych ochrony, profili użytkowników, ochrony zasobów i kontroli ochrony. Podręcznik ten nie opisuje ochrony dla konkretnych programów licencjonowanych, języków ani programów użytkowych. Więcej informacji na ten temat znajduje się w Centrum informacyjnym iSeries.
- Informacje na temat podstawowych operacji serwera iSeries znajdują się w Centrum informacyjnym w artykule ″Podstawowe operacje systemowe″. Szczegóły znajdują się w sekcji “Informacje wstępne i pokrewne” na stronie xii.
- W Centrum informacyjnym opisane jest, w jaki sposób skonfigurowaćTCP/IP i wiele protokołów TCP/IP, takich jak: FTP, SMTP i TELNET. Szczegóły znajdują się w sekcji “Informacje wstępne i pokrewne” na stronie xii.

- *TCP/IP File Server Support for OS/400 Installation and User's Guide*, SC41-0125, zawiera wstępne informacje, instrukcje instalacyjne oraz procedury konfiguracyjne dla programu licencjonowanego File Server Support. Wyjaśnia funkcje dostępne w produkcie i zawiera przykłady oraz wskazówki dotyczące ich używania w innych systemach.
- *Trusted Computer Systems Evaluation Criteria* DoD 5200.28.STD opisuje kryteria dotyczące poziomów zaufania dla systemów komputerowych. TCSEC jest publikacją wydaną przez rząd Stanów Zjednoczonych. Jego kopię można uzyskać pod adresem:

  Office of Standards and Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 USA
  Attention: Chief, Computer Security Standards
- W Centrum informacyjnym znajduje się wiele artykułów dotyczących Zarządzania systemem i Zarządzania pracą w sererwach iSeries. Niektóre z nich zawierają informacje na temat: danych dotyczących wydajności, zarządzania wartościami i zarządzania pamięcią. Informacje na temat Centrum informacyjnego znajdują się w sekcji "Informacje wstępne i pokrewne" na stronie xii. Publikacja Zarządzanie pracą, SA12-7276-03, dostarcza informacji na temat tworzenia i zmiany środowiska zarządzania pracą. Więcej informacji na ten temat znajduje się w Centrum informacyjnym iSeries.

Jako dodatkowe źródla informacji w stosunku do tematów poruszanych w Centrum informacyjnym oraz na dysku CD-ROM Podręczniki uzupełniające, można wykorzystać:

- **IBM SecureWay**
  IBM SecureWay obejmuje szeroki zakres opcji ochrony oferowanych przez firmę IBM: sprzęt, oprogramowanie, konsultacje i inne usługi, których celem jest pomoc klientom w ochronie ich informacji. Niezależnie od tego, czy chodzi o indywidualne potrzeby, czy o stworzenie rozwiązania dla całego przedsiębiorstwa, IBM SecureWay spełnia wysokie wymagania dotyczące planowania, projektowania, wdrażania i pracy rozwiązań ochrony dla firm. Więcej informacji na temat możliwości IBM SecureWay zawiera strona główna IBM SecureWay:

  `http://www.ibm.com/secureway`
- **Oferty usług**
  Instalacja nowego sprzętu i oprogramowania może w dużym stopniu zwiększyć wydajność działań w przedsiębiorstwie. Może jednak zaistnieć zagrożenie powstania zakłóceń i przerwy w działaniu, co obciąży wewnętrzne zasoby w firmie. Usługi powiązane z ochroną serwera iSeries znajdują się w IBM Global Services. Na poniższej stronie WWW znajduje się kompletna lista usług serwera iSeries:

  `http://www.as.ibm.com/asus`

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 IBM. 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 tej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przesyłać na adres:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
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
Tokyo 106, Japan

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 TAKIM STANIE, W JAKIM SIĘ OBECNIE ZNAJDUJE (“AS IS”) BEZ JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ANI TEŻ GWARANCJI, ŻE PUBLIKACJA TA NIE NARUSZA PRAW OSÓB TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych i domniemanych w odniesieniu od 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 użytkownika i w żadnym wypadku nie stanowią zachęty

do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych do tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

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

Informacje na temat możliwości stosowania tego programu, takie jak: (i) wymiana informacji między niezależnie tworzonymi programami a innymi programami (włącznie z tym programem) czy (ii) wspólne używanie wymienianych informacji, można uzyskać pod adresem:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
USA

Informacje takie mogą zostać udostępnione na określonych warunkach, co w niektórych przypadkach może oznaczać opłatę.

Licencjonowany program opisany w tej publikacji i 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 lub w innych podobnych umowach zawartych między IBM a 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 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.

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 NA PRAWA AUTORSKIE

Publikacja ta zawiera przykładowe aplikacje w kodzie źródłowym, które ilustrują techniki programowania na różnych platformach systemowych. Aplikacje te można bezpłatnie

kopiować, modyfikować i rozpowszechniać w dowolnej formie w celu tworzenia, używania lub rozpowszechniania aplikacji przeznaczonych dla interfejsu programowania aplikacji systemu operacyjnego, dla którego zostały napisane . Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować lub sugerować niezawodności, użyteczności czy funkcjonalności tych programów. Użytkownik może kopiować, modyfikować i rozpowszechniać te programy przykładowe w dowolnej formie bez uiszczania opłat w celu rozbudowy, używania, handlowym lub w celu rozpowszechniania aplikacji zgodnych z aplikacyjnym interfejsem programowym IBM.

Przy przeglądaniu tych informacji w formie elektronicznej, fotografie i ilustracje kolorowe mogą się nie pojawić.

Znaki towarowe

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

Advanced Peer-to-Peer Networking
APPN
AS/400
DB2
DRDA
e (logo)
IBM
iSeries
Net.Data
Operating System/400
OS/400
PowerPC
SecureWay
System/36
System/38
400

ActionMedia, LANDesk, MMX, Pentium oraz ProShare są znakami towarowymi lub zastrzeżonymi 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 i wszystkie znaki towarowe dotyczące języka Java są znakami towarowymi Sun Microsystems, Inc. w Stanach Zjednoczonych i/lub w innych krajach.

UNIX jest zastrzeżonym znakiem towarowym The Open Group w Stanach Zjednoczonych i w innych krajach.

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

Indeks

Znaki specjalne

A

B

C

D

L

M

N

O

P

Q

R

S

Ś

T

U

W

Z

Ź

Ż

SC85-0032-07