IBM

eserver

iSeries

Suggerimenti e strumenti per la sicurezza di iSeries

Versione 5

SC13-3198-07

IBM

@server

iSeries

Suggerimenti e strumenti per la sicurezza di iSeries

Versione 5

SC13-3198-07

Nota

Prima di utilizzare queste informazioni e il prodotto a cui si riferiscono, leggere la sezione “Informazioni particolari” a pagina 175.

Ottava Edizione (Aprile 2004)

Questa edizione si applica alla versione 5, release 3, livello di modifica 0 di IBM Operating System/400 (numero prodotto 5722-SS1) ed a tutti i successivi release e livelli di modifica se non altrimenti indicato nelle nuove edizioni. Questa versione non si applica ai modelli RISC (reduced instruction set computer) né ai modelli CISC.

Questa edizione sostituisce SC41-5300-06.

© Copyright International Business Machines Corporation 1996, 2004. Tutti i diritti riservati.

Indice

Figure vii

Tabelle ix

Informazioni su Suggerimenti e strumenti per la sicurezza di iSeries (SC13-3198-07) xi

A chi è rivolto questo manuale xi
Come utilizzare queste informazioni xii
Requisiti necessari e informazioni correlate xii
Come inviare i propri commenti xiii

Parte 1. Sicurezza iSeries di base . . 1

Capitolo 1. Elementi di base della sicurezza iSeries 3

Livelli di sicurezza 3
Impostazioni globali 4
Profili utente 5
Profili di gruppo 5
Sicurezza delle risorse 5
Limitazione dell'accesso a una funzione del programma 5
Controlli di sicurezza 7
Esempio: documento attributi sicurezza di sistema. . 8

Capitolo 2. Wizard di sicurezza iSeries e eServer Security Planner 11

Wizard di sicurezza. 11
eServer Security Planner 13

Capitolo 3. Controllo collegamento interattivo 15

Impostazione regole parola d'ordine 15
Livelli di una parola d'ordine 16
Pianificazione delle modifiche al livello di una parola d'ordine 17
Modifica parole d'ordine note 21
Impostazione dei valori di collegamento. 23
Modifica messaggi di errore del collegamento . . . 24
Pianificazione disponibilità di profili utente. . . . 24
Rimozione dei profili utente inattivi 25
Disabilitazione automatica dei profili utente . . 25
Rimozione automatica dei profili utente 26
Come evitare parole d'ordine predefinite 27
Monitoraggio dell'attività della parola d'ordine e del collegamento 27
Memorizzazione delle informazioni sulla parola d'ordine 28

Capitolo 4. Configurazione di iSeries per utilizzare Strumenti di sicurezza . . 29

Utilizzo di Strumenti di sicurezza in modo sicuro . 29
Come evitare i conflitti di file 29
Salvataggio di Strumenti di sicurezza. 30
Comandi e menu per i comandi di sicurezza . . . 30
Opzioni del menu Strumenti di sicurezza . . . 30
Utilizzo del menu batch di sicurezza 33
Comandi per personalizzare la sicurezza . . . 39
Valori impostati dal comando Configurazione riservatezza sistema 40
Funzioni del comando Revoca autorizzazione pubblica 42

Parte 2. Sicurezza iSeries avanzata 45

Capitolo 5. Protezione delle informazioni tramite autorizzazione oggetto 47

Applicazione dell'autorizzazione all'oggetto . . . 47
Sicurezza menu 48
Limitazioni del controllo accesso menu 48
Potenziamento del controllo accesso menu tramite la sicurezza dell'oggetto 49
Esempio: configurazione di un ambiente di transizione. 49
Utilizzo della sicurezza libreria come complemento alla sicurezza menu 51
Configurazione della proprietà dell'oggetto. . . . 52
Autorizzazione all'oggetto per comandi e programmi di sistema 52
Controllo funzioni di sicurezza 52
Analisi dei profili utente 53
Analisi delle autorizzazioni oggetto 55
Controllo oggetti modificati 55
Analisi dei programmi che adottano un'autorizzazione 56
Gestione del giornale di controllo e dei ricevitori di giornale. 56

Capitolo 6. Gestione autorizzazione . . 59

Monitoraggio dell'autorizzazione pubblica agli oggetti 59
Gestione dell'autorizzazione per nuovi oggetti. . . 60
Monitoraggio elenchi di autorizzazioni 60
Utilizzo degli elenchi di autorizzazioni 61
Accesso alle normative in iSeries Navigator . . 63
Monitoraggio dell'autorizzazione privata agli oggetti 63
Monitoraggio dell'accesso alle code di emissione e di lavori 64
Monitoraggio autorizzazioni speciali 64
Monitoraggio degli ambienti dell'utente 66
Gestione programmi di manutenzione 67

Capitolo 7. Utilizzo della sicurezza delle partizioni logiche (LPAR) 69

© Copyright IBM Corp. 1996, 2004

Gestione sicurezza per partizioni logiche 70

Capitolo 8. iSeries Operations Console 73
Panoramica sulla sicurezza di Operations Console 74
Autenticazione dell'unità console 74
Autenticazione utente 74
Riservatezza dei dati 74
Integrità dei dati. 75
Utilizzo di Operations Console con connettività LAN. 75
Protezione di Operations Console con connettività LAN. 75
Utilizzo del wizard di configurazione di Operations Console. 76

Capitolo 9. Rilevazione programmi sospetti 77
Protezione contro i virus del computer 77
Monitoraggio dell'utilizzo dell'autorizzazione adottata 79
Limitazione dell'utilizzo dell'autorizzazione adottata 80
Prevenzione dell'utilizzo dell'autorizzazione adottata da parte di nuovi programmi 81
Monitoraggio dell'utilizzo di programmi trigger . . 82
Controllo di programmi nascosti 83
Valutazione di programmi di uscita registrati . . . 85
Controllo programmi pianificati 86
Limitazione della funzione Salvataggio e ripristino 86
Controllo degli oggetti utente nelle librerie protette 87

Capitolo 10. Prevenzione e rilevazione di tentativi di violazione 89
Sicurezza fisica 89
Monitoraggio dell'attività del profilo utente . . . 89
Firma oggetto 90
Monitoraggio delle descrizioni del sottosistema . . 91
Voci di avvio automatico lavoro 92
Nomi e tipi di stazioni di lavoro 92
Voci di una coda lavori 92
Voci di instradamento 92
Voci di comunicazioni e nomi ubicazione remota . . 93
Voci lavoro di preavvio 93
Lavori e descrizioni lavoro 93
TPN (transaction program name) strutturati . . . 94
Richieste TPN strutturati 95
Metodi per monitorare gli eventi di sicurezza . . . 96

Parte 3. Comunicazioni di rete e applicazioni 99

Capitolo 11. Utilizzo di IFS (Integrated File System) per proteggere i file . . . 101
L'approccio dell'IFS (Integrated File System) alla sicurezza 101
File system principali (/), QOpenSys e definiti dall'utente 103
Funzionamento dell'autorizzazione 103
Comando Stampa autorizzazioni private (PRTPVTAUT) 106
Comando Stampa oggetti autorizzati pubblicamente (PRTPUBAUT) 107
Limitazione dell'accesso al file system QSYS.LIB 107
Protezione indirizzari. 109
Protezione per nuovi oggetti 109
Utilizzo del comando Creazione indirizzario . . 110
Creazione di un indirizzario con un'API . . . 110
Creazione di un file di flusso con l'API open() o creat() 110
Creazione di un oggetto utilizzando un'interfaccia del PC 110
File system QFileSvr.400 111
File system di rete 111

Capitolo 12. Comunicazioni APPC protette 113
Terminologia APPC 113
Elementi di base delle comunicazioni APPC . . . 114
Esempio: sessione APPC di base 114
Limitazione delle sessioni APPC 114
Accesso di un utente APPC al sistema di destinazione 115
Metodi del sistema per inviare le informazioni relative a un utente 115
Opzioni per distribuire la responsabilità della sicurezza di rete 117
Assegnazione a un sistema di destinazione di profili utente per lavori 117
Opzioni di pass-through di una stazione video . . 118
Come evitare assegnazioni unità impreviste . . . 120
Controllo di comandi remoti e lavori batch . . . 120
Valutazione della configurazione APPC. 121
Parametri rilevanti per le unità APPC 121
Parametri per le unità di controllo APPC . . . 124
Parametri per le descrizioni di linea 125

Capitolo 13. Comunicazioni TCP/IP protette 127
Come impedire l'elaborazione TCP/IP 127
Componenti di sicurezza TCP/IP. 127
Utilizzo delle regole del pacchetto per proteggere il traffico TCP/IP 128
Server proxy HTTP 128
VPN (Virtual Private Networking) 128
SSL (Secure Sockets Layer) 129
Protezione dell'ambiente TCP/IP 129
Controllo dei server TCP/IP con avvio automatico 130
Considerazioni di sicurezza per l'utilizzo di SLIP 132
Controllo dei collegamenti SLIP in entrata. . . 132
Controllo di sessioni di collegamento in uscita 134
Considerazioni sulla sicurezza per il protocollo point-to-point 136
Considerazioni sulla sicurezza per l'utilizzo del server Bootstrap Protocol 137
Prevenzione dell'accesso BOOTP 137
Protezione del server BOOTP 138
Considerazioni sulla sicurezza per l'utilizzo del server DHCP 139
Prevenzione accesso DHCP. 139

Protezione del server DHCP 140
Considerazioni sulla sicurezza per l'utilizzo del server TFTP 140
Prevenzione accesso TFTP 141
Protezione del server TFTP 141
Considerazioni sulla sicurezza per l'utilizzo del server REXEC 142
Prevenzione dell'accesso REXEC 142
Protezione del server REXEC 143
Considerazioni sulla sicurezza per l'utilizzo di RouteD 143
Considerazioni sulla sicurezza per l'utilizzo del server DNS 144
Prevenzione dell'accesso DNS 144
Protezione del server DNS 145
Considerazioni sulla sicurezza per l'utilizzo del server HTTP per iSeries 145
Prevenzione dell'accesso HTTP 146
Controllo dell'accesso al server HTTP 146
Considerazioni sulla sicurezza per l'utilizzo di SSL con IBM HTTP Server per iSeries 151
Considerazioni sulla sicurezza per LDAP 152
Considerazioni sulla sicurezza per LPD 153
Prevenzione dell'accesso LPD 153
Controllo accesso LPD 153
Considerazioni sulla sicurezza per SNMP 154
Prevenzione accesso SNMP 154
Controllo accesso SNMP 155
Considerazioni sulla sicurezza per il server INETD 155
Considerazioni sulla sicurezza per limitare il roaming TCP/IP 156

Capitolo 14. Accesso sicuro a una stazione di lavoro 159
Prevenzione dei virus di una stazione di lavoro 159
Accesso sicuro ai dati di una stazione di lavoro 159
Autorizzazione all'oggetto con accesso a una stazione di lavoro 160
Gestione applicazione 161
Utilizzo di SSL con iSeries Access per Windows 162
Sicurezza iSeries Navigator 162
Prevenzione accesso ODBC 163
Considerazioni sulla sicurezza per le parole d'ordine della sessione di una stazione di lavoro . 163
Protezione del server dalle procedure e dai comandi remoti 165
Protezione delle stazioni di lavoro dalle procedure e dai comandi remoti 165
Server gateway 166
Comunicazioni LAN wireless 167

Capitolo 15. Programmi di uscita sicurezza 169

Capitolo 16. Considerazioni sulla sicurezza per browser Internet 171
Rischio: danni alla stazione di lavoro 171
Rischio: accesso agli indirizzari iSeries tramite unità collegate 171
Rischio: applet firmate garantite 172

Capitolo 17. Informazioni correlate 173

Informazioni particolari 175
Marchi 177

Indice analitico. 179

Figure

1. Documento attributi sicurezza di sistema-Esempio 8
2. Pannello di pianificazione attivazione profilo–Esempio 25
3. Documento relativo agli utenti con autorizzazione privata per gli elenchi di autorizzazioni. 60
4. Visualizzazione oggetti elenco autorizzazioni 61
5. Documento di informazioni sull'utente: Esempio 1 65
6. Documento di informazioni sull'utente: Esempio 2 65
7. Stampa profilo utente-esempio di ambiente dell'utente 66
8. Gestione informazioni registrazione-Esempio 85
9. Descrizioni unità APPC-Documento di esempio 121
10. Documento elenco configurazioni-Esempio 122
11. Descrizioni unità di controllo APPC-Documento di esempio 124
12. Descrizioni linea APPC-Documento di esempio 125
13. Sistema iSeries con un server gateway 166

© Copyright IBM Corp. 1996, 2004

Tabelle

1. Valori di sistema per le parole d'ordine 15
2. Parole d'ordine per profili forniti da IBM 22
3. Parole d'ordine per DST (dedicated service tools). 22
4. Valori del sistema di collegamento 23
5. Messaggi di errore del collegamento 24
6. Comandi di strumento per i profili utente 31
7. Comandi di strumento per il controllo sicurezza 32
8. Comandi per documentazioni di sicurezza 34
9. Comandi per personalizzare il sistema . . . 39
10. Valori impostati dal comando CFGSYSSEC 40
11. Comandi la cui autorizzazione pubblica è impostata dal comando RVKPUBAUT. . . . 42
12. Programmi la cui autorizzazione pubblica è impostata dal comando RVKPUBAUT. . . . 42
13. Risultati della codifica 73
14. Esempio di Utilizzo autorizzazione adottata (USEADPAUT) 80
15. Programmi di uscita forniti dal sistema 84
16. Punti di uscita per l'attività del profilo utente 90
17. Programmi e utenti per richieste TPN. . . . 95
18. Valori di sicurezza nell'architettura APPC 116
19. Modalità di funzionamento congiunto del valore di sicurezza APPC e del valore SECURELOC. 117
20. Possibili valori per il parametro utente predefinito 118
21. Richieste di collegamento pass-through di esempio 119
22. Come i comandi TCP/IP stabiliscono quali server avviare 130
23. Valori di avvio automatico per i server TCP/IP 131
24. Origini di programmi di uscita di esempio 169

© Copyright IBM Corp. 1996, 2004

Informazioni su Suggerimenti e strumenti per la sicurezza di iSeries (SC13-3198-07)

Il ruolo dei computer nelle aziende è in rapido cambiamento. I dirigenti IT, i fornitori software, i responsabili della sicurezza e i revisori hanno bisogno di riconsiderare numerose aree che hanno dato per scontate in passato. La sicurezza di iSeries dovrebbe essere uno degli argomenti compresi in tale elenco.

I sistemi forniscono molte funzioni nuove notevolmente differenti dalle applicazioni di account tradizionali. Gli utenti accedono ai sistemi in nuovi modi: LAN, linee commutate (collegamento remoto), collegamenti wireless, reti di tutti i tipi. Spesso, gli utenti non visualizzano affatto un pannello di collegamento. Molte società sono in continua espansione per diventare "aziende estese", con reti di proprietà o con Internet.

Improvvisamente, sembra che i sistemi dispongano di tutta una nuova serie di porte e finestre. I gestori di sistemi e i responsabili della sicurezza sono giustamente preoccupati di come proteggere le informazioni in questo ambiente in continuo e rapido cambiamento.

Questo manuale fornisce una serie di suggerimenti pratici per utilizzare le funzioni di sicurezza di iSeries e per stabilire le procedure operative relative alla sicurezza. I consigli in queste informazioni si applicano a un'installazione con rischi e requisiti di sicurezza medi. Tali informazioni non forniscono una descrizione completa delle funzioni di sicurezza iSeries disponibili. Se si desiderano ulteriori informazioni sulle opzioni aggiuntive o informazioni di background, consultare le pubblicazioni descritte nel Capitolo 17, "Informazioni correlate", a pagina 173.

Tali informazioni descrivono inoltre come impostare e utilizzare gli strumenti di sicurezza che fanno parte di OS/400. Il Capitolo 4, "Configurazione di iSeries per utilizzare Strumenti di sicurezza", a pagina 29 e "Comandi e menu per i comandi di sicurezza" a pagina 30 forniscono informazioni di riferimento sugli strumenti di sicurezza. Esse forniscono esempi per l'utilizzo degli strumenti.

A chi è rivolto questo manuale

Un **responsabile della riservatezza** o un **responsabile della sicurezza** garantisce la sicurezza su un sistema. Tale responsabilità include normalmente le seguenti attività:

- Impostare e gestire i profili utente
- Impostare i valori su tutto il sistema che influenzano la sicurezza
- Gestire l'autorizzazione agli oggetti
- Applicare e controllare le normative di sicurezza

Se l'utente è responsabile della gestione della sicurezza per uno o più sistemi iSeries, è necessario che tenga bene a mente queste informazioni. Le istruzioni contenute in questo manuale presuppongono quanto segue:

- L'utente conosce bene le procedure operative di base di iSeries, come il collegamento e l'utilizzo dei comandi.

© Copyright IBM Corp. 1996, 2004

- L'utente conosce bene gli elementi di base della sicurezza iSeries: livelli di sicurezza , valori di sistema della sicurezza, profili utente e sicurezza degli oggetti.

  Nota: il Capitolo 1, "Elementi di base della sicurezza iSeries", a pagina 3 fornisce un'analisi di tali elementi. Se non si ha familiarità con tali elementi di base, si consiglia di consultare l'argomento *Pianificazione e sicurezza di base* nell'iSeries Information Center. Consultare "Requisiti necessari e informazioni correlate" per ulteriori dettagli.
- E' stata attivata la sicurezza sul sistema impostando il valore di sistema (QSECURITY) relativo al livello di sicurezza almeno su 30.

IBM migliora continuamente le funzioni di sicurezza di iSeries. Per sfruttare tali miglioramenti, sarebbe opportuno valutare regolarmente il pacchetto di correzioni cumulative correntemente disponibile per il release. Verificare se contiene correzioni di rilievo per la sicurezza.

Come utilizzare queste informazioni

Se non si è impostato il sistema per utilizzare gli strumenti di sicurezza o si è installato Security ToolKit for OS/400 per un release precedente, effettuare le seguenti operazioni:

1. Iniziare con il Capitolo 2, "Wizard di sicurezza iSeries e eServer Security Planner", a pagina 11. Tale argomento descrive come utilizzare queste funzioni per selezionare gli strumenti di sicurezza consigliati e come ottenere un'introduzione ad essi.
2. Per istruzioni ancor più basilari sulla sicurezza, è possibile esaminare le informazioni sui Riferimenti di sicurezza, che è possibile trovare in linea nell'iSeries Information Center.

Nota

Queste informazioni contengono *numerosi* suggerimenti per la protezione di iSeries. E' possibile che il sistema necessiti di protezione solo in alcune aree. Utilizzare tali informazioni per saperne di più sui possibili rischi di sicurezza e sui relativi rimedi. Quindi, concentrare la propria attenzione sulle aree maggiormente critiche per il proprio sistema.

Requisiti necessari e informazioni correlate

Utilizzare iSeries Information Center come punto di partenza per reperire informazioni tecniche relative iSeries.

E' possibile accedere all'Information Center in due modi:

- Dal seguente sito Web:

  `http://www.ibm.com/eserver/iseries/infocenter`
- Dal CD ROM *iSeries Information Center*, SK2T-8428-04. Tale CD-ROM viene fornito con il nuovo ordine di aggiornamento hardware iSeries o software IBM Operating System/400. E' inoltre possibile ordinare il CD-ROM dall'IBM Publications Center:

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

L'iSeries Information Center contiene informazioni iSeries nuove e aggiornate come l'installazione software e hardware, Linux, WebSphere, Java, alta disponibilità, database, partizioni logiche, comandi CL e API (application programming interface) del sistema. Inoltre, fornisce advisor e finder per assistenza nella pianificazione, risoluzione dei problemi e configurazione dell'hardware e del software iSeries.

Con ogni nuova ordinazione hardware, l'utente riceve il *CD-ROM Operazioni e impostazione iSeries*, SK2T-8429-02. Questo CD-ROM contiene IBM @server IBM e(logo)server iSeries Access per Windows e il wizard EZ-Setup. iSeries Access Family offre una vasta gamma di funzioni client e server per collegare i PC ai server iSeries. Il wizard EZ-Setup automatizza molte delle attività di installazione iSeries.

Come inviare i propri commenti

Le opinioni degli utenti sono importanti per fornire informazioni particolarmente accurate. Se vi sono commenti sul manuale o su qualsiasi altra documentazione iSeries, riempire il modulo commenti del lettore sul retro di questo manuale.

- Se si preferisce inviare commenti per posta, utilizzare il modulo commenti del lettore con l'indirizzo stampato sul retro. Se si sta inviando il modulo commenti da un paese diverso dagli Stati Uniti, è possibile consegnarlo ad una filiale locale IBM o ad un rappresentante IBM per una spedizione già affrancata.
- Se si preferisce inviare commenti via FAX, utilizzare uno dei seguenti numeri:
  - Stati Uniti, Canada e Porto Rico: 1-800-937-3430
  - Altri paesi: 1-507-253-5192
- Se si preferisce inviare commenti elettronicamente, utilizzare uno di questi indirizzi e-mail:
  - Commenti sui manuali:

    RCHCLERK@us.ibm.com
  - Commenti sull'iSeries Information Center:

    RCHINFOC@us.ibm.com

Assicurarsi di inserire i seguenti elementi:

- Il titolo del manuale o dell'argomento dell'iSeries Information Center.
- Il numero di pubblicazione di un manuale.
- Il numero di pagina o l'argomento del manuale a cui si riferisce il commento.

Parte 1. Sicurezza iSeries di base

© Copyright IBM Corp. 1996, 2004

Capitolo 1. Elementi di base della sicurezza iSeries

Questo argomento fornisce una breve analisi degli elementi di base che cooperano per garantire la sicurezza iSeries. In altre parti del presente manuale, vengono forniti ulteriori suggerimenti al d là di quelli basilari per l'utilizzo di tali elementi di sicurezza in modo che soddisfino le esigenze della propria azienda.

Livelli di sicurezza

E' possibile scegliere il livello di sicurezza che si desidera che il sistema applichi impostando il relativo valore di sistema (QSECURITY). Il sistema offre cinque livelli di sicurezza:

Livello 10:
Il sistema non applica alcuna sicurezza. Non è necessaria alcuna parola d'ordine. Se il profilo utente specificato non esiste sul sistema quando qualcuno si collega, il sistema ne crea uno.

ATTENZIONE:

Iniziando da V4R3 e nei release futuri, non è possibile impostare il valore di sistema QSECURITY su 10. Se il sistema è correntemente a un livello di sicurezza 10, rimarrà al livello 10 quando si installa la Versione 4 Release 3. Se si modifica il livello di sicurezza in un altro valore, non è possibile riportarlo al livello 10. Dal momento che il livello 10 non fornisce alcuna protezione di sicurezza, esso non è consigliato da IBM. **IBM non fornirà supporto per problemi che dovessero verificarsi a un livello di sicurezza 10 a meno che il problema non possa essere creato anche a un livello di sicurezza superiore.**

Livello 20:
Il sistema richiede un ID utente e una parola d'ordine per il collegamento. Si fa solitamente riferimento al livello 20 come **sicurezza di collegamento**. Per impostazione predefinita, tutti gli utenti hanno accesso a tutti gli oggetti poiché tutti gli utenti dispongono dell'autorizzazione speciale *ALLOBJ.

Livello 30:
Il sistema richiede un ID utente e una parola d'ordine per il collegamento. E' necessario che gli utenti abbiano l'autorizzazione ad utilizzare gli oggetti poiché non dispongono di alcuna autorizzazione per impostazione predefinita. Questo livello viene chiamato **sicurezza delle risorse**.

Livello 40:
Il sistema richiede un ID utente e una parola d'ordine per il collegamento. Oltre alla sicurezza delle risorse, il sistema fornisce funzioni di **protezione di integrità**. Le funzioni di protezione integrità, come la convalida di parametri per interfacce al sistema operativo, sono progettate per proteggere sia il sistema che gli oggetti sul sistema dalle manomissioni da parte di utenti del sistema con esperienza. Per la maggior parte delle

© Copyright IBM Corp. 1996, 2004

installazioni, il livello 40 è il livello di sicurezza consigliato. Quando si riceve un nuovo sistema iSeries con V4R5 o con un release successivo, il livello di sicurezza è impostato su 40.

Livello 50:
Il sistema richiede un ID utente e una parola d'ordine per il collegamento. Il sistema applica sia la sicurezza delle risorse che la protezione di integrità di livello 40, ma aggiunge **protezione integrità avanzata**, come la limitazione della gestione messaggio tra i programmi di stato del sistema e i programmi di stato dell'utente. Il livello di sicurezza 50 è ideato per sistemi iSeries con requisiti di sicurezza elevati.

Nota: Il livello 50 è il livello richiesto per la certificazione C2 (e per la certificazione FIPS-140).

Il capitolo 2 del manuale *Riferimenti alla sicurezza iSeries* fornisce ulteriori informazioni sui livelli di sicurezza e descrive in che modo passare da un livello di sicurezza a un altro.

Impostazioni globali

Il sistema dispone di impostazioni globali che influenzano il modo in cui le attività giungono sul sistema e il modo in cui il sistema appare agli utenti di un altro sistema. Tali impostazioni includono i seguenti elementi:

Valori di sistema della sicurezza:
I valori di sistema della sicurezza vengono utilizzati per controllare la sicurezza sul sistema. Tali valori sono suddivisi in quattro gruppi:
- Valori di sistema della sicurezza generali
- Altri valori di sistema correlati alla sicurezza
- Valori di sistema che controllano le parole d'ordine
- Valori di sistema che verificano il controllo

Numerosi argomenti in questo manuale discutono le implicazioni per la sicurezza di valori di sistema specifici. Il capitolo 3 nel manuale *Riferimenti alla sicurezza iSeries* descrive tutti i valori di sistema correlati alla sicurezza.

Attributi di rete:
Gli attributi di rete controllano in che modo il sistema prende parte a una rete (o sceglie di non farlo) con altri sistemi. Per ulteriori informazioni sugli attributi di rete, consultare il manuale *Work Management*.

Descrizioni del sottosistema e altri elementi di gestione lavoro:
Gli elementi di gestione lavoro stabiliscono in che modo il lavoro viene immesso sul sistema e in quale ambiente viene eseguito. Numerosi argomenti in queste informazioni discutono le implicazioni della sicurezza di alcuni valori di gestione lavoro. Il manuale *Work Management* fornisce informazioni complete.

Configurazione delle comunicazioni:
Anche la configurazione delle comunicazioni influenza il modo in cui il lavoro viene immesso sul sistema. Numerosi argomenti in queste informazioni forniscono suggerimenti per proteggere il sistema quando fa parte di una rete.

Profili utente

Ogni utente del sistema **deve** avere un profilo utente. E' necessario creare un profilo utente prima che un utente possa collegarsi. E' possibile utilizzare i profili utente anche per controllare l'accesso ai programmi di manutenzione come DASD e i dump della memoria principale. Consultare "Gestione programmi di manutenzione" a pagina 67 per ulteriori informazioni.

Il profilo utente è uno strumento flessibile e potente. Controlla le attività dell'utente e personalizza l'aspetto del sistema. Il manuale *Riferimenti alla sicurezza iSeries* descrive tutti i parametri nel profilo utente.

Profili di gruppo

Un profilo gruppo è un tipo speciale di profilo utente. E' possibile utilizzare un profilo di gruppo per definire l'autorizzazione per un gruppo di utenti, piuttosto che fornire autorizzazione a ciascun utente singolarmente. E' inoltre possibile utilizzare un profilo gruppo come modello quando si creano profili utente singoli utilizzando la funzione di copia profilo o, se si utilizza iSeries Navigator, è possibile utilizzare il menu delle normative di sicurezza per modificare le autorizzazioni utente.

Il capitolo 5 e il capitolo 7 nel manuale *Riferimenti alla sicurezza iSeries* forniscono ulteriori informazioni sulla pianificazione e l'utilizzo dei profili gruppo.

Sicurezza delle risorse

La sicurezza delle risorse sul sistema consente di definire chi può utilizzare gli oggetti e in che modo è possibile utilizzarli. La capacità di accedere ad un oggetto viene chiamata **autorizzazione**. Quando si imposta l'autorizzazione all'oggetto, può essere necessario usare cautela per concedere agli utenti sufficiente autorizzazione per svolgere il loro lavoro senza fornire loro l'autorizzazione di esaminare e modificare il sistema. L'autorizzazione all'oggetto fornisce permessi all'utente per un oggetto specifico e può definire le attività che l'utente può effettuare sull'oggetto. Una risorsa dell'oggetto può essere limitata tramite autorizzazioni utente dettagliate e specifiche, come ad esempio l'aggiunta o la modifica di record. E' possibile utilizzare le risorse del sistema per fornire all'utente l'accesso a sottoserie di autorizzazioni specifiche definite dal sistema: *ALL, *CHANGE, *USE e *EXCLUDE.

I file, i programmi, le librerie e gli indirizzari sono gli oggetti di sistema più comuni che richiedono la protezione di sicurezza della risorsa, ma è possibile specificare l'autorizzazione per qualsiasi singolo oggetto sul sistema.

Il Capitolo 5, "Protezione delle informazioni tramite autorizzazione oggetto" discute l'importanza di impostare l'autorizzazione all'oggetto sul sistema. Il capitolo 5 del manuale *Riferimenti alla sicurezza iSeries* descrive le opzioni per impostare la sicurezza delle risorse.

Limitazione dell'accesso a una funzione del programma

La limitazione accesso a una funzione del programma consente di fornire sicurezza per il programma quando non si dispone di un oggetto iSeries per proteggere il programma. Prima che il supporto di limitazione accesso a una funzione del programma fosse aggiunto in V4R3, si poteva realizzare ciò creando un elenco di autorizzazioni o un altro oggetto e controllando l'autorizzazione all'oggetto per

controllare l'accesso alla funzione del programma. Ora è possibile utilizzare la limitazione dell'accesso a una funzione del programma per controllare in modo più semplice l'accesso a un'applicazione, a parti di un'applicazione o a funzioni all'interno di un programma.

E' possibile utilizzare due metodi per gestire l'accesso di un utente alle funzioni dell'applicazione tramite iSeries Navigator. Il primo utilizza il supporto di Gestione applicazione:

1. Fare clic con il tasto destro del mouse sul sistema che contiene la funzione di cui si desidera modificare l'impostazione di accesso.
2. Selezionare **Gestione applicazione**.
3. Se ci si trova su un sistema di gestione, selezionare **Impostazioni locali**. In caso contrario, continuare con la fase successiva.
4. Selezionare una funzione gestibile.
5. Selezionare **Accesso predefinito**, se applicabile. Selezionando ciò, si consente a tutti gli utenti di accedere alla funzione per impostazione predefinita.
6. Selezionare **Accesso a tutti gli oggetti**, se applicabile. Selezionando ciò, si consente a tutti gli utenti con privilegio di sistema su tutti gli oggetti di accedere a tale funzione.
7. Selezionare **Personalizza**, se applicabile. Utilizzare i pulsante **Aggiungi** e **Rimuovi** sulla finestra di dialogo **Personalizza accesso** per aggiungere o rimuovere utenti o gruppi negli elenchi **Accesso consentito** e **Accesso negato**.
8. Selezionare **Rimuovi personalizzazione**, se applicabile. Selezionando ciò, si cancella qualsiasi accesso personalizzato per la funzione selezionata.
9. Fare clic su **OK** per chiudere la finestra di dialogo **Gestione applicazione**.

Il secondo metodo di gestione accesso utente coinvolge il supporto Utenti e gruppi di iSeries Navigator:

1. In iSeries Navigator, espandere **Utenti e gruppi**.
2. Selezionare **Tutti gli utenti**, **Gruppi** o **Utenti non in un gruppo** per visualizzare un elenco di utenti e gruppi.
3. Fare clic con il tastino destro del mouse su un utente o un gruppo e selezionare **Proprietà**.
4. Fare clic su **Capacità**.
5. Fare clic sul separatore **Applicazioni**.
6. Utilizzare questa pagina per modificare l'impostazione di accesso per un utente o un gruppo.
7. Fare doppio clic su **OK** per chiudere la finestra di dialogo **Proprietà**.

Consultare "Sicurezza iSeries Navigator" a pagina 162 per ulteriori informazioni sulla sicurezza di iSeries Navigator.

Se l'utente è un application writer, è possibile utilizzare le API di limitazione accesso a una funzione del programma per effettuare quanto segue:

- Registrare una funzione
- Richiamare informazioni sulla funzione
- Definire chi può o non può utilizzare la funzione
- Verificare se all'utente è consentito utilizzare la funzione

Nota: tale supporto **non** è una sostituzione per la sicurezza della risorsa. La limitazione dell'accesso a una funzione del programma non impedisce a un utente di accedere a una risorsa (come un file o un programma) da un'altra interfaccia.

Per utilizzare tale supporto all'interno di un'applicazione, è necessario che il fornitore dell'applicazione registri le funzioni quando l'applicazione viene installata. La funzione registrata corrisponde a un blocco di codice per specifiche funzioni nell'applicazione. Quando l'applicazione viene eseguita dall'utente, l'applicazione chiama l'API prima che l'applicazione chiami il blocco di codice. L'API chiama l'API di controllo utilizzo per visualizzare se all'utente è consentito utilizzare la funzione. Se all'utente è consentito utilizzare la funzione registrata, il blocco di codice viene eseguito. Se all'utente non è consentito utilizzare la funzione, non gli è neanche consentito di eseguire il blocco di codice.

Nota: le API comportano la registrazione di un ID funzione di 30 caratteri nel database di registrazione (WRKREGINF). Sebbene non esistano punti di uscita correlati agli ID funzione utilizzati dalle API di limitazione accesso a una funzione, è obbligatorio avere dei punti di uscita. Per registrare qualsiasi elemento nel registro, **è necessario** fornire un nome formato del punto di uscita. A questo proposito, l'API Registrazione funzione crea un nome formato fittizio e lo utilizza per tutte le funzioni registrate. Dal momento che tale nome formato è fittizio, nessun programma del punto di uscita verrà mai chiamato.

Il responsabile di sistema specifica a chi è consentito o negato l'accesso a una funzione. Tale responsabile può inoltre utilizzare l'API per gestire l'accesso a una funzione del programma o utilizzare la GUI di Gestione applicazione di iSeries Navigator. Il manuale *iSeries server API Reference* fornisce informazioni sulle API di limitazione accesso a una funzione del programma. Per ulteriori informazioni sul controllo dell'accesso alle funzioni, consultare "Sicurezza iSeries Navigator" a pagina 162.

Controlli di sicurezza

Gli utenti controllano la sicurezza del sistema per numerose ragioni:

- Per valutare se il piano di sicurezza è completo.
- Per accertarsi che i controlli di sicurezza pianificati siano adeguati e funzionanti. Tale tipo di controllo viene normalmente eseguito dal responsabile della riservatezza come parte della gestione giornaliera della sicurezza. Viene inoltre eseguito, a volte, in modo più dettagliato, come parte di un'analisi periodica della sicurezza tramite revisori interni o esterni.
- Per accertarsi che la sicurezza del sistema vada di pari passo con le modifiche all'ambiente del sistema. Di seguito vengono riportati alcuni esempi di modifiche che influenzano la sicurezza:
  - Creazione di nuovi oggetti da parte di utenti del sistema
  - Ammissione di nuovi utenti al sistema
  - Modifica della proprietà di un oggetto (autorizzazione non regolata)
  - Modifica di responsabilità (gruppo di utenti modificato)
  - Autorizzazione temporanea (revocata in ritardo)
  - Installazione di nuovi prodotti

- Per prepararsi a un evento futuro, come l'installazione di una nuova applicazione, il passaggio a un livello di sicurezza superiore o la configurazione di una rete di comunicazioni.

Le tecniche descritte nella presente sezione si adattano a tutte queste situazioni. Gli elementi che si controllano e la frequenza con cui si esegue tale controllo dipendono dalla dimensione e dalle esigenze di sicurezza dell'azienda.

Il controllo di sicurezza comporta l'utilizzo di comandi sul sistema e l'accesso alle informazioni del giornale e di registrazione. E' possibile creare un profilo speciale che può essere utilizzato da un utente che effettui un controllo di sicurezza del sistema. E' necessario che il profilo del revisore disponga dell'autorizzazione speciale *AUDIT per modificare le caratteristiche di controllo del sistema. Alcune delle attività di controllo suggerite in questo capitolo richiedono un profilo utente con autorizzazione speciale *ALLOBJ e *SECADM. Impostare la parola d'ordine per il profilo del revisore su *NONE una volta terminato il periodo di controllo.

Per ulteriori dettagli sul controllo sicurezza, consultare il Capitolo 9, del manuale *Riferimenti alla sicurezza*.

Esempio: documento attributi sicurezza di sistema

La Figura 1 mostra un esempio dell'emissione dal comando Stampa attributi riservatezza sistema (PRTSYSSECA). Il documento mostra le impostazioni relative ai valori di sistema e agli attributi di rete rilevanti per la sicurezza che sono consigliati per sistemi con normali requisiti di sicurezza. Mostra anche le impostazioni correnti nel sistema.

Nota: la colonna *Valore corrente* sul documento mostra l'impostazione corrente sul sistema. Confrontare questa con il valore consigliato per vedere dove potrebbero verificarsi rischi per la sicurezza.

```
Attributi sicurezza di sistema

Nome
valore di sist.  Valore corrente      Valore consigliato
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
```

Figura 1. Documento attributi sicurezza di sistema-Esempio (Parte 1 di 4)

```
QAUTOCFG        0                   0
QAUTORMT        1                   0
QAUTOVRT        9999                0
QCMNRCYLMT      0 0                 0 0
QCRTAUT         *CHANGE             Controllo a livello libreria.
QCRTOBJAUD      *NONE               Controllo a livello libreria.
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
```

Figura 1. Documento attributi sicurezza di sistema-Esempio (Parte 2 di 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
```

Figura 1. Documento attributi sicurezza di sistema-Esempio (Parte 3 di 4)

```
Attributi sicurezza di sistema

Nome
attributo rete  Valore corrente     Valore consigliato
DDMACC          *OBJAUT              *REJECT
JOBACN          *FILE                *REJECT
PCSACC          *OBJAUT              *REJECT
```

Figura 1. Documento attributi sicurezza di sistema-Esempio (Parte 4 di 4)

Capitolo 2. Wizard di sicurezza iSeries e eServer Security Planner

Gli strumenti Wizard di sicurezza del server iSeries e eServer Security Planner possono aiutare l'utente a decidere quali valori di sicurezza applicare sul server iSeries. Utilizzando il Wizard di sicurezza del server iSeries in iSeries Navigator si produrranno documenti che riportano le esigenze di sicurezza in base alle risposte selezionate. E' quindi possibile utilizzare queste informazioni per configurare la sicurezza del sistema.

Utilizzare il Wizard di sicurezza iSeries o eServer Security Planner come ausilio per pianificare e implementare una normativa della sicurezza di base per i server iSeries. Lo scopo di entrambi gli strumenti è di rendere più semplice l'implementazione e la gestione della sicurezza sui sistemi. Il wizard, disponibile come parte di OS/400, pone all'utente numerose domande di alto livello sull'ambiente server e, in base alle risposte, fornisce una serie di consigli che il wizard può applicare direttamente al sistema.

eServer Security Planner è la versione in linea del Wizard di sicurezza. Consente di selezionare le scelte in base alle esigenze di sicurezza e quindi fornisce una documentazione suggerendo quali funzioni sono necessarie per proteggere il sito.

eServer Security Planner è una versione, basata sul web, del wizard. Fornisce consigli per implementare la sicurezza sul sistema, esattamente come fa il wizard. Tuttavia, l'advisor non può applicare i consigli. Piuttosto, emette un elenco di valori di sicurezza del sistema e altri attributi che sarebbe opportuno applicare sul sistema, in base alla risposte dell'utente alle domande dell'advisor stesso.

Wizard di sicurezza

Decidere quale valore del sistema di sicurezza iSeries sarebbe opportuno utilizzare per la propria azienda potrebbe essere complicato. Se non si ha familiarità con l'implementazione della sicurezza sui server iSeries o l'ambiente in cui si esegue il server iSeries è stato recentemente modificato, il Wizard di sicurezza può essere utile all'utente per prendere una decisione.

Cos'è un wizard?

- Un wizard è uno strumento progettato per essere eseguito da un utente inesperto per installare o configurare degli elementi su un sistema.
- Il wizard richiede all'utente le informazioni tramite domande. La risposta a ciascuna domanda determina la domanda successiva.
- Quando il wizard ha chiesto tutte le domande, all'utente viene presentata una finestra di dialogo finale. L'utente fa clic sul pulsante **Fine** per installare e configurare la voce.

Obiettivi del wizard di sicurezza

L'obiettivo del wizard di sicurezza è la configurazione di quanto segue, in base alle risposte dell'utente.

- Valori di sistema e attributi di rete correlati alla sicurezza.
- Documenti correlati alla sicurezza per il monitoraggio del sistema.

© Copyright IBM Corp. 1996, 2004

- Per creare un Documento di informazioni responsabile e un Documento di informazioni utente:
  - Il Documento di informazioni responsabile contiene impostazioni di sicurezza consigliate e le procedure da seguire prima di rendere effettivi i consigli.
  - Il Documento di informazioni utente contiene informazioni che è possibile utilizzare per la normativa di sicurezza aziendale. Ad esempio, le regole di composizione delle parole d'ordine sono incluse in questa documentazione.
- Per fornire le impostazioni consigliate per varie voci correlate alla sicurezza sul sistema.

Obiettivi del wizard di sicurezza

- Gli obiettivi del wizard di sicurezza sono:
  - Stabilire le impostazioni di sicurezza del sistema, in base alle risposte degli utenti alle domande del wizard, quindi implementare le impostazioni quando sono appropriate.
  - Il wizard produce una documentazione di informazioni dettagliate che includono quanto segue:
    - Documentazione che spiega i consigli del wizard.
    - Documentazione che descrive nei dettagli le procedure da seguire prima dell'implementazione.
    - Documentazione che elenca le informazioni di rilievo da distribuire agli utenti del sistema.
- Tali voci rendono operativa la normativa di sicurezza sul sistema.
- Il wizard consiglia la documentazione del giornale di controllo che dovrebbe essere pianificata per un'esecuzione periodica. Una volta pianificata, tale documentazione aiuta a:
  - Accertarsi che vengano seguite le normative di sicurezza.
  - Accertarsi che le normative di sicurezza vengano modificate soltanto con l'approvazione dell'utente.
  - Pianificare la documentazione per monitorare eventi correlati alla sicurezza, sul sistema.
- Il wizard consente di salvare i consigli o di applicare alcuni o tutti i suggerimenti al sistema.

Nota: il wizard di sicurezza può essere utilizzato più di una volta sullo stesso sistema per consentire agli utenti che potrebbero possedere un'installazione obsoleta di esaminare la sicurezza corrente. E' possibile utilizzare il wizard di sicurezza a partire da un sistema V3R7 (quando iSeries Navigator è stato presentato) in poi.

Per utilizzare iSeries Navigator, è necessario disporre di IBM iSeries Access per Windows installato su un PC con Windows 95/NT e disporre di un collegamento server iSeries da tale PC. E' necessario che l'utente del Wizard sia collegato a un server iSeries. E' necessario che l'utente abbia un ID utente con autorizzazione speciale *ALLOBJ, *SECADM, *AUDIT e *IOSYSCFG. Per assistenza nel collegamento di un PC Windows 95/NT PC al sistema iSeries, consultare l'argomento IBM iSeries Access per Windows nell'Information Center (consultare "Requisiti necessari e informazioni correlate" a pagina xii per dettagli).

Per accedere al wizard di sicurezza , effettuare quanto segue:

1. In iSeries Navigator, espandere il server.
2. Fare clic con il tastino destro del mouse su **Sicurezza** e selezionare **Configura**.
   - Quando un utente avvia l'opzione **Sicurezza** di iSeries Navigator, viene inviata una richiesta al server iSeries per controllare l'autorizzazione speciale dell'utente.

- Se l'utente non dovesse avere tutte le autorizzazioni speciali richieste (*ALLOBJ, *AUDIT, *IOSYSCFG, *SECADM) l'opzione **Configura** non verrà visualizzata e non sarà in grado di accedere al wizard di sicurezza.

3. Supponendo che l'utente disponga dell'autorizzazione richiesta:
   - Le precedenti risposte del wizard vengono richiamate.
   - Le impostazioni di sicurezza correnti vengono richiamate.

Il wizard di sicurezza presenterà uno dei tre seguenti pannelli di benvenuto. A seconda di quale delle seguenti condizioni si verifica, verrà visualizzato uno dei tre pannelli:

- Il wizard non è mai stato eseguito per il server iSeries di destinazione.
- Il wizard è stato eseguito prima e le modifiche di sicurezza sono state rimandate.
- Il wizard è stato eseguito prima e le modifiche di sicurezza sono state eseguite.

Se non si sta utilizzando iSeries Navigator, è comunque possibile ottenere un aiuto per la pianificazione delle proprie esigenze di sicurezza. eServer Security Planner è una versione in linea del wizard di sicurezza, con una differenza. L'advisor non configurerà automaticamente il sistema. Tuttavia, creerà una documentazione di opzioni di sicurezza consigliate basate sulle risposte dell'utente. Per accedere a eServer Security Planner, andare all'eServer Information Center:

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

eServer Security Planner

eServer Security Planner è una versione in linea del Wizard di sicurezza. Pone le stesse domande del wizard di sicurezza e, in base alle risposte dell'utente, crea gli stessi consigli. Le differenze principali tra i due strumenti sono:

- eServer Security Planner **non**—
  - Produce documentazione.
  - Confronta le impostazioni correnti con le impostazioni consigliate.
  - Imposta i valori di sistema automaticamente.
- Non è possibile applicare i consigli da eServer Security Planner.

eServer Security Planner crea un programma CL che è possibile tagliare, incollare e modificare pa proprio uso per rendere automatica la configurazione della sicurezza. E' inoltre possibile collegarsi direttamente alla documentazione del server iSeries da eServer Security Planner. Ciò fornisce informazioni sui valori di sistema o sulla documentazione che possono aiutare l'utente a stabilire se questa impostazione è adatta al proprio ambiente.

Per accedere a eServer Security Planner, puntare il browser Internet sull'URL seguente:

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

Capitolo 3. Controllo collegamento interattivo

Quando si pensa alla limitazione dell'accesso al sistema, partire dal punto più ovvio, il pannello di collegamento. Di seguito vengono riportate le opzioni che è possibile utilizzare per rendere difficile il collegamento al sistema utilizzando il relativo pannello di collegamento.

Impostazione regole parola d'ordine

Per proteggere il collegamento al sistema, effettuare quanto segue:
- Impostare una normativa che attesta che le parole d'ordine non devono essere banali e non devono essere condivise.
- Impostare i valori di sistema come aiuto per l'applicazione della sicurezza. La Tabella 1 visualizza le impostazioni consigliate dei valori di sistema.

La combinazione di valori nella Tabella 1 è piuttosto limitativa ed è pensata per ridurre in modo significativo la probabilità di parole d'ordine banali. Tuttavia, è possibile che gli utenti trovino difficoltoso e frustrante selezionare una parola d'ordine che corrisponda a tali limitazioni.

Considerare di fornire agli utenti quanto segue:
1. Un elenco di criteri per le parole d'ordine.
2. Esempi di parole d'ordine valide e non.
3. Suggerimenti per inventare una buona parola d'ordine.

Eseguire il comando Configurazione riservatezza sistema (CFGSYSSEC) per impostare questi valori. Utilizzare il comando Stampa attributi riservatezza di sistema (PRTSYSSECA) stampare le impostazioni correnti per questi valori di sistema.

Il capitolo 3 del manuale *Riferimenti alla sicurezza iSeries*, "Valori impostati dal comando Configurazione riservatezza sistema" a pagina 40 fornisce ulteriori informazioni sul comando CFGSYSSEC.

Tabella 1. Valori di sistema per le parole d'ordine

Nome valore di sistema	Descrizione	Valore consigliato
QPWDEXPITV	Frequenza con cui gli utenti del sistema devono modificare le parole d'ordine. E' possibile specificare un valore differente per singoli utenti nel profilo utente.	60 (giorni)
QPWDLMTAJC	Se il sistema impedisce i caratteri adiacenti uguali.	1 (sì)
QPWDLMTCHR	Quali caratteri non è possibile utilizzare nelle parole d'ordine.[2]	AEIOU#$@
QPWDLMTREP	Se il sistema impedisce la presenza dello stesso carattere più volte nella parola d'ordine.	2 (non consentito consecutivamente)
QPWDLVL	Se le parole d'ordine del profilo utente sono limitate a 10 caratteri o a un massimo di 128.	0[3]
QPWDMAXLEN	Il numero massimo di caratteri in una parola d'ordine.	8
QPWDMINLEN	Il numero minimo di caratteri in una parola d'ordine.	6
QPWDPOSDIF	Se è necessario che ogni carattere in una parola d'ordine sia differente dal carattere nella stessa posizione della parola d'ordine precedente.	1 (sì)

© Copyright IBM Corp. 1996, 2004

Tabella 1. Valori di sistema per le parole d'ordine (Continua)

Nome valore di sistema	Descrizione	Valore consigliato
QPWDRQDDGT	Se è necessario che la parola d'ordine contenga almeno un carattere numerico.	1 (sì)
QPWDRQDDIF	Tempo di attesa dell'utente prima di utilizzare nuovamente la stessa parola d'ordine.[2]	5 o meno (intervalli di scadenza)[1]
QPWDVLDPGM	Quale programma di uscita è chiamato per convalidare una parola d'ordine assegnata recentemente.	*NONE

Note:

1. Il valore di sistema QPWDEXPITV specifica la frequenza con cui è necessario modificare la parola d'ordine, come ad esempio ogni 60 giorni. Questo è l'**intervallo di scadenza**. Il valore di sistema QPWDRQDDIF specifica quanti intervalli di scadenza devono passare prima di potere utilizzare nuovamente la stessa parola d'ordine. Il capitolo 3 del manuale *Riferimenti alla sicurezza iSeries* fornisce ulteriori informazioni sul funzionamento congiunto di tali valori di sistema.
2. QPWDLMTCHR non è applicato ai livelli 2 o 3 della parola d'ordine. Consultare "Livelli di una parola d'ordine" per dettagli.
3. Fare riferimento a "Pianificazione delle modifiche al livello di una parola d'ordine" a pagina 17 per determinare il livello delle parole d'ordine adatto alla proprie esigenze.

Livelli di una parola d'ordine

Apartire da V5R1 del sistema operativo, il valore di sistema QPWDLVL offre una sicurezza della parola d'ordine maggiore. Nei precedenti release, gli utenti erano limitati a parole d'ordine con lunghezza non superiore a 10 caratteri, da un intervallo limitato di caratteri. Ora, gli utenti possono selezionare una frase o una parola d'ordine con un numero massimo di 128 caratteri, a seconda del livello della parola d'ordine a cui è impostato il sistema. I livelli della parola d'ordine sono:

- **Livello 0:** i sistemi vengono forniti a questo livello. Al livello 0, le parole d'ordine hanno una lunghezza massima di 10 caratteri, contenenti soltanto A-Z, 0–9, #, @, $ e i caratteri _. Le parole d'ordine a livello 0 sono meno sicure di quelle a livelli superiori.
- **Livello 1:** stesse regole del livello parola d'ordine 0, ma le parole d'ordine per iSeries Support per Windows Network Neighborhood (d'ora in avanti chiamato iSeries NetServer) non vengono salvate.
- **Livello 2:** le parole d'ordine sono sicure a questo livello. E' possibile utilizzare tale livello per scopi di verifica. Le parole d'ordine vengono salvate per gli utenti al livello 0 o 1 se hanno una lunghezza pari o inferiore a 10 caratteri e utilizzano la serie di caratteri per le parole d'ordine di livello 0 o 1. Le frasi o parole d'ordine a questo livello presentano le seguenti caratteristiche:
  - fino a 128 caratteri in lunghezza.
  - comprensivi di tutti i caratteri disponibili sulla tastiera.
  - non possono essere composte interamente da spazi; questi vengono rimossi dalla fine della parola d'ordine.
  - sensibili al maiuscolo e al minuscolo.
- **Livello 3:** le parole d'ordine a questo livello sono le più sicure e utilizzano gli algoritmi di codifica più avanzati disponibili. Le parole d'ordine a questo livello hanno le stesse caratteristiche del livello 2. Le parole d'ordine per iSeries NetServer non vengono salvate a questo livello.

Sarebbe opportuno utilizzare solo i livelli 2 e 3 delle parole d'ordine se ogni sistema nella rete corrisponde a questi criteri.

- Il sistema operativo è V5R1 o successivi
- Il livello della parola d'ordine è impostato su 2 o 3

In modo simile, è necessario che gli utenti si colleghino utilizzando lo stesso livello di parola d'ordine. I livelli delle parole d'ordine sono globali; gli utenti non possono scegliere il livello a cui desiderano proteggere le parole d'ordine.

Pianificazione delle modifiche al livello di una parola d'ordine

E' necessario pianificare con attenzione la modifica dei livelli delle parole d'ordine. E' possibile che le operazioni con altri sistemi abbiano esito negativo o che gli utenti non possano collegarsi al sistema se non è stata pianificata in modo adeguato la modifica al livello delle parole d'ordine. Prima di modificare il valore di sistema QPWDLVL, accertarsi di avere salvato i dati di sicurezza utilizzando il comando SAVSECDTA o SAVSYS. Se si dispone di una copia di riserva corrente, sarà possibile reimpostare le parole d'ordine per tutti i profili utente se è necessario tornare a un livello di parole d'ordine inferiore.

I prodotti che si utilizzano sul sistema e sui client con cui il sistema si interfaccia, potrebbero avere problemi quando il valore di sistema (QPWDLVL) del livello della parola d'ordine è impostato su 2 o 3. Qualsiasi prodotto o client che invia le parole d'ordine al sistema in un formato codificato, piuttosto che nel testo in chiaro che un utente immette su un pannello di collegamento, deve essere aggiornato per gestire le nuove regole di codifica della parola d'ordine per QPWDLVL di livello 2 o 3. L'invio della parola d'ordine codificata è noto come **sostituzione della parola d'ordine**.

La sostituzione della parola d'ordine è utilizzata per impedire la cattura di una parola d'ordine durante la trasmissione su una rete. I sostituti della parola d'ordine generati da client meno recenti che non supportano il nuovo algoritmo per il livello 2 o 3 di QPWDLVL, anche se i caratteri specifici sono corretti, non verranno accettati. Ciò si applica inoltre a qualsiasi accesso peer da iSeries a iSeries che utilizza i valori codificati per eseguire l'autenticazione da un sistema a un altro.

Il problema deriva dal fatto che alcuni prodotti interessati (come Java Toolbox) sono forniti come middleware. Un prodotto di terzi che incorpora una versione precedente di uno di tali prodotti non funzionerà correttamente finché non verrà ricreato utilizzando una versione aggiornata di middleware.

Considerati questo e altri scenari, è semplice comprendere perché una pianificazione attenta è necessaria prima di modificare il valore di sistema QPWDLVL.

Considerazioni per modificare QPWDLVL da 0 a 1

Il livello 1 della parola d'ordine consente a un sistema, che non ha necessità di comunicare con il prodotto Windows 95/98/ME AS/400 Client Support for Windows Network Neighborhood (iSeries NetServer), di eliminare le parole d'ordine iSeries NetServer dal sistema. L'eliminazione delle parole d'ordine codificate non necessarie dal sistema aumenta la sicurezza generale del sistema stesso.

Al livello QPWDLVL 1, tutti i meccanismi di autenticazione parola d'ordine e sostituzione parola d'ordine precedenti a V5R1 continueranno ad essere operativi. La possibilità di violazione è veramente minima ad eccezione delle funzioni e dei servizi che richiedono la parola d'ordine iSeries NetServer.

Considerazioni per modificare QPWDLVL da 0 o 1 a 2

Il livello 2 della parola d'ordine introduce l'utilizzo di parole d'ordine sensibili al maiuscolo e al minuscolo con una lunghezza massima di 128 caratteri (denominate anche frasi d'ordine) e fornisce la capacità massima di tornare nuovamente a QPWDLVL 0 o 1.

Indipendentemente dal livello di parola d'ordine del sistema, parole d'ordine di livello 2 e 3 vengono create ogni qualvolta si modifichi una parola d'ordine o un utente si colleghi al sistema. La creazione di una parola d'ordine di livello 2 e 3 mentre il sistema è ancora al livello 0 o 1 prepara alla modifica nel livello 2 o 3 della parola d'ordine.

Prima di modificare QPWDLVL in 2, sarebbe opportuno utilizzare i comandi DSPAUTUSR o PRTUSRPRF TYPE(*PWDINFO) per individuare tutti i profili utente che non dispongono di una parola d'ordine utilizzabile al livello 2 della parola d'ordine. A seconda dei profili individuati da tali comandi, è possibile che si desideri utilizzare uno dei seguenti meccanismi per aggiungere una parola d'ordine di livello 2 e 3 ai profili.

- Modificare la parola d'ordine per il profilo utente utilizzando il comando CL CHGUSRPRF o CHGPWD o l'API QSYCHGPW. Ciò provocherà la modifica, da parte del sistema, della parola d'ordine utilizzabile ai livelli 0 e 1 e il sistema creerà anche due parole d'ordine sensibili al minuscolo e al maiuscolo equivalenti utilizzabili ai livelli 2 e 3 della parola d'ordine. Una versione tutta maiuscola e tutta minuscola della parola d'ordine viene creata per essere utilizzata ai livelli 2 o 3 della parola d'ordine.

  Ad esempio, la modifica della parola d'ordine in C4D2RB4Y dà come risultato la creazione, da parte del sistema, di parole d'ordine di livello 2 C4D2RB4Y e c4d2rb4y.
- Collegarsi al sistema tramite un meccanismo che presenta la parola d'ordine nel testo in chiaro (non utilizzare la sostituzione della parola d'ordine). Se la parola d'ordine è valida e il profilo utente non dispone di una parola d'ordine utilizzabile ai livelli 2 e 3, il sistema crea due parole d'ordine equivalenti sensibili al maiuscolo e al minuscolo utilizzabili ai livelli 2 e 3. Una versione tutta maiuscola e tutta minuscola della parola d'ordine viene creata per essere utilizzata ai livelli 2 o 3 della parola d'ordine.

L'assenza di una parola d'ordine utilizzabile al livello 2 o 3 può rappresentare un problema ogni qualvolta neanche il profilo utente disponga di una parola d'ordine utilizzabile ai livelli 0 e 1 o quando l'utente tenta di collegarsi tramite un prodotto che utilizza la sostituzione delle parole d'ordine. In tali casi, l'utente non potrà collegarsi quando il livello della parola d'ordine viene modificato in 2.

Se un profilo utente non ha una parola d'ordine utilizzabile ai livelli 2 e 3, il profilo utente non ha una parola d'ordine utilizzabile ai livelli 0 e 1 e l'utente si collega tramite un prodotto che invia parole d'ordine con testo in chiaro, il sistema convalida l'utente rispetto ad una parola d'ordine di livello 0 e crea due parole d'ordine di livello 2 (come descritto in precedenza) per il profilo utente. I collegamenti successivi verranno convalidati rispetto alle parole d'ordine di livello 2.

Qualsiasi client/servizio che utilizza la sostituzione della parola d'ordine non funzionerà correttamente al livello QPWDLVL 2 se il client/servizio non è stato aggiornato per utilizzare il nuovo schema di sostituzione parola d'ordine (frase d'ordine). L'amministratore dovrebbe verificare se è necessario un client/servizio che non è stato aggiornato nel nuovo schema di sostituzione parola d'ordine.

I client/servizi che utilizzano la sostituzione della parola d'ordine includono:

- TELNET
- iSeries Access
- server host iSeries
- QFileSrv.400
- Supporto di stampa iSeries NetServer
- DDM
- DRDA
- SNA LU6.2

Si consiglia vivamente di salvare i dati di sicurezza prima di modificarli in QPWDLVL 2. Ciò può essere utile per rendere la transizione nuovamente a QPWDLVL 0 o 1 più semplice se diventa necessario.

Si consiglia di non modificare gli altri valori di sistema della parola d'ordine, come ad esempio QPWDMINLEN e QPWDMAXLEN, finché non venga effettuata una verifica a QPWDLVL 2. Ciò renderà più semplice la transizione verso QPWDLVL 1 o 0 se necessario. Tuttavia, è necessario che il valore di sistema QPWDVLDPGM specifichi *REGFAC o *NONE prima che il sistema consenta la modifica di QPWDLVL su 2. Quindi, se viene utilizzato un programma di convalida parola d'ordine, è possibile che si desideri scriverne uno nuovo che sia possibile registrare per il punto di uscita QIBM_QSY_VLD_PASSWRD utilizzando il comando ADDEXITPGM.

Le parole d'ordine iSeries NetServer sono ancora supportate al livello QPWDLVL 2, quindi qualsiasi funzione/servizio che richieda una parola d'ordine iSeries NetServer dovrebbe funzionare comunque correttamente.

Una volta che l'amministratore ha acquisito familiarità con l'esecuzione del sistema al livello QPWDLVL 2, è possibile iniziare a modificare i valori di sistema della parola d'ordine per usufruire di parole d'ordine più lunghe. Tuttavia, è necessario che l'amministratore sia consapevole che le parole d'ordine più lunghe provocheranno i seguenti effetti:

- Se si specificano delle parole d'ordine maggiori di 10 caratteri, la parola d'ordine del livello 0 e 1 viene eliminata. Tale profilo utente non si potrebbe collegare se il sistema viene riportato al livello 0 o 1 della parola d'ordine.
- Se le parole d'ordine contengono caratteri speciali o non seguono le regole di composizione per nomi oggetto semplici (esclusa la sensibilità al maiuscolo e al minuscolo), la parola d'ordine di livello 0 e 1 viene eliminata.
- Se si specificano parole d'ordine superiori a 14 caratteri, la parola d'ordine iSeries NetServer per il profilo utente viene eliminata.
- I valori di sistema della parola d'ordine si applicano soltanto al nuovo valore del livello 2 della parola d'ordine e non si applicano alla parola d'ordine di livello 0 e 1 generata dal sistema o ai valori della parola d'ordine iSeries NetServer (se sono stati creati).

Considerazioni per modificare QPWDLVL da 2 a 3

Dopo avere eseguito il sistema a QPWDLVL 2 per un determinato periodo di tempo, è possibile che l'amministratore prenda in considerazione il passaggio a QPWDLVL 3 per aumentare al massimo la protezione di sicurezza della parola d'ordine.

A QPWDLVL 3, tutte le parole d'ordine iSeries NetServer vengono eliminate, quindi sarebbe opportuno non spostare un sistema a QPWDLVL 3 fino a quando non sia più necessario utilizzare le parole d'ordine iSeries NetServer.

A QPWDLVL 3, vengono eliminate tutte le parole d'ordine di livello 0 e 1. L'amministratore può utilizzare i comandi DSPAUTUSR o PRTUSRPRF per individuare i profili utente che non presentano parole d'ordine di livello 2 o 3 associate ad essi.

Modifica in un livello di parola d'ordine inferiore

Tornare a un valore QPWDLVL inferiore, se possibile, non è un'operazione del tutto semplice. In generale è possibile immaginarla come un viaggio di sola andata da valori QPWDLVL inferiori a valori QPWDLVL superiori. Tuttavia, potrebbero verificarsi dei casi in cui è necessario riconfigurare un valore inferiore di QPWDLVL.

Ciascuna delle seguenti sezioni discute il lavoro richiesto per tornare a un livello della parola d'ordine inferiore.

Considerazioni per passare da QPWDLVL 3 a 2: Tale modifica è relativamente semplice. Una volta che QPWDLVL è impostato su 2, l'amministratore deve stabilire se è necessario che qualche profilo utente contenga delle parole d'ordine iSeries NetServer o delle parole d'ordine di livello 0 o 1 e, in questo caso, modificare la parola d'ordine del profilo utente in un valore consentito.

Inoltre, è possibile che i valori di sistema della parola d'ordine debbano essere modificati nuovamente in valori compatibili con iSeries NetServer e nelle parole d'ordine di livello 0 e 1, se tali parole d'ordine sono necessarie.

Considerazioni per passare da QPWDLVL 3 a 1 o 0: Dal momento che le probabilità che si verifichino dei problemi con tali parole d'ordine sul sistema sono molto elevate (come ad esempio l'impossibilità di effettuare un collegamento poiché tutte le parole d'ordine di livello 0 e 1 sono state eliminate), tale modifica non è supportata direttamente. Per passare da QPWDLVL 3 a QPWDLVL 1 o 0, è necessario che il sistema effettui la modifica intermedia in QPWDLVL 2.

Considerazioni per passare da QPWDLVL 2 a 1: Prima di modificare QPWDLVL in 1, sarebbe opportuno che l'amministratore utilizzasse i comandi DSPAUTUSR o PRTUSRPRF TYPE(*PWDINFO) per individuare qualsiasi profilo utente che non dispone di una parola d'ordine di livello 0 o 1. Se il profilo utente richiederà una parola d'ordine una volta modificato QPWDLVL, sarebbe opportuno che l'amministratore si accertasse della creazione di una parola d'ordine di livello 0 e 1 utilizzando uno dei seguenti meccanismi:

- Modificare la parola d'ordine per il profilo utente utilizzando il comando CL CHGUSRPRF o CHGPWD o l'API QSYCHGPW. Ciò provocherà la modifica, da parte del sistema, della parola d'ordine utilizzabile ai livelli 2 e 3 e inoltre il sistema creerà una parola d'ordine maiuscola equivalente utilizzabile ai livelli 0 e 1 della parola d'ordine. Il sistema può creare soltanto una parola d'ordine di livello 0 e 1 se si verificano le seguenti condizioni.
  - La parola d'ordine ha una lunghezza pari o inferiore a 10 caratteri.
  - E' possibile convertire la parola d'ordine nei caratteri EBCDIC maiuscoli A-Z, 0-9, @, #, $ e sottolineatura.
  - La parola d'ordine non inizia con un carattere numerico o di sottolineatura.

Ad esempio, la modifica della parola d'ordine in un valore RainyDay dà come risultato la creazione, da parte del sistema, di una parola d'ordine RAINYDAY di livello 0 e 1. Ma, la modifica del valore della parola d'ordine in Rainy Days In April provocherà che l'eliminazione, da parte del sistema, della parola d'ordine di livello 0 e 1 (poiché la parola d'ordine è troppo lunga e contiene degli spazi).

Non viene emesso alcun messaggio o indicazione se non è stato possibile creare una parola d'ordine di livello 0 o 1.

- Collegarsi al sistema tramite un meccanismo che presenta la parola d'ordine con testo in chiaro (non utilizza la sostituzione della parola d'ordine). Se la parola d'ordine è valida e il profilo utente non dispone di una parola d'ordine utilizzabile ai livelli 0 e 1, il sistema crea una parola d'ordine maiuscola equivalente utilizzabile ai livelli 0 e 1 della parola d'ordine. Il sistema può creare una parola d'ordine di livello 0 e 1 soltanto se si verificano le condizioni elencate precedentemente.

L'amministratore può quindi modificare QPWDLVL in 1. Tutte le parole d'ordine iSeries NetServer vengono eliminate quando la modifica in QPWDLVL 1 diventa operativa (IPL successivo).

Considerazioni per passare da QPWDLVL 2 a 0: Le considerazioni sono le stesse di quelle relative alla modifica da QPWDLVL 2 a 1 ad eccezione del fatto che le parole d'ordine iSeries NetServer vengono conservate quando le modifiche diventano operative.

Considerazioni per passare da QPWDLVL 1 a 0: Dopo avere modificato QPWDLVL in 0, sarebbe opportuno che l'amministratore utilizzasse i comandi DSPAUTUSR o PRTUSRPRF per individuare qualsiasi profilo utente che non dispone di una una parola d'ordine iSeries Netserver. Se il profilo utente richiede una parola d'ordine iSeries NetServer, è possibile crearla modificando la parola d'ordine dell'utente o collegandosi tramite un meccanismo che presenta la parola d'ordine con testo in chiaro.

L'amministratore può quindi modificare QPWDLVL in 0.

Modifica parole d'ordine note

Effettuare quanto segue per chiudere alcune possibilità ben note di entrare nel server iSeries che potrebbero esistere sul sistema.

__ Passo 1. Accertarsi che nessun profilo utente abbia ancora parole d'ordine predefinite (uguali al nome profilo utente). E' possibile utilizzare il comando Analisi parole d'ordine predefinite (ANZDFTPWD). (Consultare "Come evitare parole d'ordine predefinite" a pagina 27.)

__ Passo 2. Tentare di collegarsi al sistema con le combinazioni di profili utente e parole d'ordine visualizzate nella Tabella 2 a pagina 22. Tali parole d'ordine sono pubblicate e costituiscono la prima di scelta di chiunque tenti di irrompere nel sistema. Se è possibile effettuare il collegamento, utilizzare il comando Modifica profilo utente (CHGUSRPRF) per modificare la parola d'ordine nel valore consigliato.

__ Passo 3. Avviare DST (Dedicated Service Tools) e tentare di collegarsi con le parole d'ordine visualizzate nella Tabella 2 a pagina 22. Fare riferimento a iSeries Information Center—>Sicurezza—>Programmi di

manutenzione. Consultare “Requisiti necessari e informazioni correlate” a pagina xii per informazioni sull’accesso all’iSeries Information Center.

__ Passo 4. Se è possibile collegarsi a DST con una qualsiasi di tali parole d’ordine, sarebbe opportuno modificare le parole d’ordine. L’iSeries Information Center—>Sicurezza—>Programmi di manutenzione fornisce istruzioni dettagliate su come modificare le parole d’ordine e gli ID utente di tali programmi. Consultare “Requisiti necessari e informazioni correlate” a pagina xii per informazioni sull’accesso all’iSeries Information Center.

__ Passo 5. Infine, accertarsi che non sia possibile effettuare il collegamento semplicemente premendo il tasto Invio sul pannello di collegamento senza immettere parola d’ordine e ID utente. Tentare numerosi pannelli differenti. Se è possibile collegarsi senza immettere informazioni sul pannello di collegamento, effettuare una delle seguenti operazioni:

- Passare al livello di sicurezza 40 o 50 (valore di sistema QSECURITY).

  Nota: è possibile che le applicazioni vengano eseguite in modo differente quando si aumenta il livello di sicurezza a 40 o 50.
- Modificare tutte le voci della stazione di lavoro per sottosistemi interattivi in modo che puntino a descrizioni lavoro che specificano USER(*RQD).

Tabella 2. Parole d’ordine per profili forniti da IBM

ID utente	Parola d’ordine	Valore consigliato
QSECOFR	QSECOFR[1]	Un valore non banale noto solo al responsabile di sistema. **Annotare la parola d’ordine selezionata e conservarla al sicuro.**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2, 3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

Note:

1. Il sistema viene fornito con il valore *Impostare la parola d’ordine su scaduta* per QSECOFR impostato su *YES. La prima volta che si effettua il collegamento a questo nuovo sistema, è necessario modificare la parola d’ordine QSECOFR.
2. Il sistema ha bisogno di tali profili utente per le funzioni del sistema, ma sarebbe opportuno non consentire agli utenti di collegarsi con tali profili. Per i nuovi sistemi installati con V3R1 o release successivi, tale parola d’ordine viene fornita come *NONE.

   Quando si esegue il comando CFGSYSSEC, il sistema imposta le parole d’ordine su *NONE.
3. Per eseguire iSeries Access per Windows utilizzando TCP/IP, è necessario abilitare il profilo utente QUSER.

Tabella 3. Parole d’ordine per DST (dedicated service tools)

Livello DST	ID utente[1]	Parola d’ordine	Valore consigliato
Funzione di base	11111111	11111111	Un valore non banale noto solo al responsabile della sicurezza.[2]

Tabella 3. Parole d'ordine per DST (dedicated service tools) (Continua)

Livello DST	ID utente[1]	Parola d'ordine	Valore consigliato
Funzione completa	22222222	22222222[3]	Un valore non banale noto solo al responsabile della sicurezza.[2]
Funzione di sicurezza	QSECOFR	QSECOFR[3]	Un valore non banale noto solo al responsabile della sicurezza.[2]
Funzione di servizio	QSRV	QSRV[3]	Un valore non banale noto solo al responsabile della sicurezza.[2]

Note:

1. Un ID utente è richiesto soltanto per release PowerPC AS (RISC) del sistema operativo.
2. Se il tecnico di manutenzione hardware ha necessità di collegarsi con tale parola d'ordine e ID utente, modificare la parola d'ordine in un nuovo valore una volta che il tecnico è andato via.
3. Il profilo utente dei programmi di manutenzione scadrà al primo utilizzo.

Nota: le parole d'ordine DST possono essere modificate soltanto da un'unità autenticata. Ciò vale anche per tutte le parole d'ordine e gli ID utente corrispondenti identici. Per ulteriori informazioni sulle unità autenticate, consultare le informazioni di installazione di Operations Console nell'iSeries Information Center.

Impostazione dei valori di collegamento

La Tabella 4 visualizza numerosi valori che è possibile impostare per rendere più difficile il collegamento al sistema per una persona non autorizzata. Se si esegue il comando CFGSYSSEC, i valori di sistema vengono configurati sulle impostazioni consigliate. Per ulteriori informazioni su tali valori di sistema, consultare il Capitolo 3 del manuale *Riferimenti alla sicurezza iSeries*.

Tabella 4. Valori del sistema di collegamento

Nome valore di sistema	Descrizione	Impostazione consigliata
QAUTOCFG	Se il sistema configura automaticamente nuove unità.	0 (No)
QAUTOVRT	Il numero di descrizioni unità virtuali che il sistema creerà automaticamente se non è presente alcuna unità disponibile per l'utilizzo.	0
QDEVRCYACN	Operazioni del sistema quando un'unità si ricollega in seguito a un errore.[1]	*DSCMSG
QDSCJOBITV	Tempo di attesa del sistema prima di terminare un lavoro scollegato.	120
QDSPSGNINF	Se il sistema visualizza informazioni sulla precedente attività di collegamento quando un utente si collega.	1 (Sì)
QINACTITV	Tempo di attesa del sistema prima di eseguire un'azione in caso di lavoro interattivo inattivo.	60
QINACTMSGQ	Azioni del sistema una volta raggiunto il periodo QINACTITV.	*ENDJOB
QLMTDEVSSN	Se il sistema impedisce il collegamento di un utente su più di una stazione di lavoro alla volta.	1 (Sì)

Tabella 4. Valori del sistema di collegamento (Continua)

Nome valore di sistema	Descrizione	Impostazione consigliata
QLMTSECOFR	Se gli utenti con autorizzazione speciale *ALLOBJ o *SERVICE possono collegarsi soltanto su stazioni di lavoro specifiche.	1 (Sì)[2]
QMAXSIGN	Numero massimo di tentativi di collegamento non corretti, consecutivi (il profilo utente o la parola d'ordine non sono corretti).	3
QMAXSGNACN	Azioni del sistema una volta raggiunto il limite QMAXSIGN.	3 (Disabilitare sia il profilo utente che l'unità)

Note:

1. E' possibile che il sistema scolleghi e ricolleghi le sessioni TELNET quando la descrizione unità per la sessione è assegnata in modo esplicito.
2. Se si imposta il valore di sistema su 1 (Sì), sarà necessario autorizzare in modo esplicito gli utenti con l'autorizzazione speciale *ALLOBJ o *SERVICE alle unità. Il modo più semplice per eseguire tale operazione è fornire al profilo utente QSECOFR l'autorizzazione *CHANGE a unità specifiche.

Modifica messaggi di errore del collegamento

Gli hacker desiderano essere al corrente dei loro progressi quando irrompono in un sistema. Quando un messaggio di errore sul pannello di collegamento comunica `Parola d'ordine non corretta`, è possibile che l'hacker supponga che l'ID utente sia corretto. E' possibile indurre l'hacker in errore utilizzando il comando modifica descrizione messaggio (CHGMSGD) per modificare il testo di due messaggi di errore del collegamento. La Tabella 5 visualizza il testo consigliato.

Tabella 5. Messaggi di errore del collegamento

ID messaggio	Testo fornito	Testo consigliato
CPF1107	CPF1107 – Parola d'ordine non corretta per profilo utente.	Le informazioni sul collegamento non sono corrette **Nota:** Non includere l'ID messaggio nel testo del messaggio.
CPF1120	CPF1120 – L'utente `XXXXX` non esiste.	Le informazioni sul collegamento non sono corrette. **Nota:** Non includere l'ID messaggio nel testo del messaggio.

Pianificazione disponibilità di profili utente

E' possibile che si desideri che alcuni profili utente siano disponibili per il collegamento soltanto a determinate ore del giorno o in alcuni giorni della settimana. Ad esempio, se si dispone di un'impostazione profilo per un revisore della sicurezza, è possibile che si desideri abilitare tale profilo utente soltanto durante le ore in cui è pianificata l'attività del revisore. E' inoltre possibile che si desideri disabilitare i profili utente con autorizzazione speciale *ALLOBJ (incluso il profilo utente QSECOFR) durante le ore non di picco.

E' possibile utilizzare il comando Modifica voce Scd di attivazione (CHGACTSCDE) per impostare i profili utente da abilitare e disabilitare

automaticamente. Per ciascun profilo utente che si desidera pianificare, viene creata una voce che definisce la pianificazione del profilo utente.

Ad esempio, se si desidera che il profilo QSECOFR sia disponibile soltanto tra le 7 di mattina e le 10 di sera, sarà necessario immettere quanto segue sul pannello CHGACTSCDE:

```
             Modifica voce Scd di attivazione (CHGACTSCDE)

Immettere le scelte e premere Invio.

Profilo utente . . . . . > QSECOFR       Nome
Abilitazione ora . . . . . > '7:00'      Ora, *NONE
Disabilitazione ora  . . . . . > '22:00'  Ora, *NONE
Giorni . . . . . > *MON          *ALL, *MON, *TUE, *WED...
                                 > *TUE
                                 > *WED
                                 > *THU
             + per altri valori > *FRI
```

Figura 2. Pannello di pianificazione attivazione profilo–Esempio

In effetti, è possibile che si desideri avere il profilo QSECOFR disponibile soltanto per un numero molto limitato di ore ogni giorno. E' possibile utilizzare un altro profilo utente con la classe *SECOFR per eseguire la maggior parte delle funzioni del sistema. In questo modo si evita di esporre un profilo utente noto ai tentativi di violazione.

E' possibile utilizzare il comando Visualizzazione voci giornale di controllo (DSPAUDJRNE) periodicamente per stampare le voci del giornale di controllo CP (Modifica profilo). Utilizzare tali voci per verificare che il sistema abiliti e disabiliti i profili utente secondo la pianificazione stabilita.

Un altro metodo per accertarsi che i profili utente vengano disabilitati sulla pianificazione stabilita è utilizzare il comando Stampa profilo utente (PRTUSRPRF). Quando si specifica *PWDINFO per il tipo di documentazione, questa include lo stato di ciascun profilo utente selezionato. Se, ad esempio, si disabilitano regolarmente tutti i profili utente con autorizzazione speciale *ALLOBJ, è possibile pianificare l'esecuzione del seguente comando una volta disabilitati i profili:

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

Rimozione dei profili utente inattivi

Sarebbe opportuno che il sistema contenesse soltanto profili utente necessari. Se un profilo utente non è più necessario poiché l'utente se n'è andato o ha intrapreso un incarico differente all'interno della società, rimuoverlo. Se un utente ha lasciato la società per un periodo prolungato, disabilitare (disattivare) tale profilo utente. Un profilo utente non necessario può fornire un accesso non autorizzato al sistema.

Disabilitazione automatica dei profili utente

E' possibile utilizzare il comando Analisi attività profilo (ANZPRFACT) per disabilitare regolarmente i profili utente rimasti inattivi per un numero di giorni specificato. Quando si utilizza il comando ANZPRFACT, si specifica il numero di giorni inattivi che il sistema ricerca. Il sistema prende in considerazione la data dell'ultimo utilizzo, la data di ripristino e la data di creazione del profilo utente.

Una volta specificato un valore per il comando ANZPRFACT, il sistema pianifica l'esecuzione settimanale di un lavoro all'1 a.m. (a partire dal giorno successivo alla prima specifica del valore). Il lavoro esamina tutti i profili e disabilita i profili inattivi. Non è necessario utilizzare nuovamente il comando ANZPRFACT a meno che non si desideri modificare il numero di giorni inattivi.

E' possibile utilizzare il comando Modifica elenco profili attivi (CHGACTPRFL) per esentare alcuni profili dall'elaborazione ANZPRFACT. Il comando CHGACTPRFL crea un elenco di profili utente che il comando ANZPRFACT non disabiliterà, indipendentemente dal relativo tempo di inattività.

Quando il sistema esegue il comando ANZPRFACT, scrive una voce CP nel giornale di controllo per ciascun profilo utente disabilitato. E' possibile utilizzare il comando DSPAUDJRNE per elencare i profili utente che sono stati appena disabilitati.

Nota: il sistema scrive le voci di controllo soltanto se il valore QAUDCTL specifica *AUDLVL e il valore di sistema QAUDLVL specifica *SECURITY.

Un altro metodo per accertarsi che i profili utente vengano disabilitati al momento stabilito dalla pianificazione è utilizzare il comando Stampa profilo utente (PRTUSRPRF). Quando si specifica *PWDINFO per il tipo di documentazione, questa include lo stato di ciascun profilo utente selezionato.

Rimozione automatica dei profili utente

E' possibile utilizzare il comando Modifica voce SCD di scadenza (CHGEXPSCDE) per gestire le rimozione o la disabilitazione dei profili utente. Se si è certi che un utente si assenterà per un periodo prolungato, è possibile pianificare la rimozione o la disabilitazione del profilo utente.

La prima volta che si utilizza il comando CHGEXPSCDE, viene creata una voce di pianificazione lavoro che verrà eseguita 1 minuto dopo mezzanotte tutti i giorni. Il lavoro esamina il file QASECEXP per stabilire se è pianificata la rimozione di qualche profilo utente per quel giorno.

Con il comando CHGEXPSCDE, si disabilita o si cancella un profilo utente. Se si sceglie di cancellare un profilo utente, è necessario specificare l'attività del sistema relativamente agli oggetti di proprietà dell'utente. Prima di pianificare un profilo utente per la cancellazione, è necessario ricercare gli oggetti di proprietà dell'utente. Ad esempio, se l'utente possiede i programmi che adottano l'autorizzazione, si desidera che tali programmi adottino la proprietà del nuovo proprietario? O il nuovo proprietario dispone di maggiore autorizzazione di quanta ne è necessaria (come ad esempio un'autorizzazione speciale)? Forse, è necessario creare un nuovo profilo utente con autorizzazioni specifiche per possedere i programmi che devono adottare l'autorizzazione.

E' inoltre necessario verificare se si verificheranno problemi di applicazione, se si cancella il profilo utente. Ad esempio, qualsiasi descrizione lavoro specifica il profilo utente come profilo predefinito?

E' possibile utilizzare il comando Visualizzazione pianificazione di scadenza (DSPEXPSCD) per visualizza l'elenco di profili di cui è pianificata la disabilitazione o la rimozione.

E' possibile utilizzare il comando Visualizzazione utenti autorizzati (DSPAUTUSR) per elencare tutti i profili utente sul sistema. Utilizzare il comando Cancellazione profilo utente (DLTUSRPRF) per cancellare i profili non aggiornati.

Nota di sicurezza: si disabilita un profilo utente impostando il relativo stato su *DISABLED. Quando si disabilita un profilo utente, lo si rende non disponibile per un utilizzo interattivo. Non è possibile collegarsi tramite o modificare un lavoro relativo a un profilo utente disabilitato. I lavori batch possono essere eseguiti tramite un profilo utente disabilitato.

Come evitare parole d'ordine predefinite

Quando si crea un nuovo profilo utente, l'impostazione predefinita è specificare una parola d'ordine uguale al nome profilo utente. Ciò consente di accedere al sistema, se un utente conosce la normativa per assegnare nomi profilo e sa che una nuova persona entrerà a far parte della società.

Quando si creano nuovi profili utente, considerare di assegnare una parola d'ordine univoca, non banale invece di utilizzare la parola d'ordine predefinita. Comunicare al nuovo utente la parola d'ordine in modo riservato, come ad esempio in una lettera "Benvenuti nel sistema" che evidenzia le normative di sicurezza. Indicare all'utente di modificare la parola d'ordine la prima volta che si collega, impostando il profilo utente su PWDEXP(*YES).

E' possibile utilizzare il comando Analisi parole d'ordine predefinite (ANZDFTPWD) per controllare le parole d'ordine predefinite di tutti i profili utente sul sistema . Quando si stampa la documentazione, è possibile scegliere di impostare un'azione del sistema (come ad esempio la disabilitazione del profilo utente) se la parola d'ordine corrisponde al nome profilo utente. Il comando ANZDFTPWD stampa un elenco dei profili trovati e l'azione intrapresa dal sistema.

Nota: le parole d'ordine vengono memorizzate sul sistema in formato codificato a senso unico. Non è possibile decodificarle. Il sistema codifica la parola d'ordine specificata e la confronta con la parola d'ordine memorizzata come succederebbe se ci si collegasse al sistema. Se è in corso il controllo relativo ai problemi di autorizzazione (*AUTFAIL), il sistema scriverà una voce del giornale di controllo PW per ciascun profilo utente che *non* dispone di una parola d'ordine predefinita (per i sistemi che eseguono V4R1 o release precedenti). A partire da V4R2, il sistema non scrive le voci del giornale di controllo PW quando si esegue il comando ANZDFTPWD.

Monitoraggio dell'attività della parola d'ordine e del collegamento

Se l'utente è preoccupato di tentativi non autorizzati per accedere al sistema, è possibile utilizzare il comando PRTUSRPRF come aiuto per controllare l'attività della parola d'ordine e del collegamento.

Di seguito vengono riportati diversi suggerimenti per l'utilizzo di tale documentazione:

- Stabilire se l'intervallo di scadenza della parola d'ordine per alcuni profili utente è maggiore del valore di sistema e se tale intervallo di scadenza più lungo è giustificato. Ad esempio, nella documentazione, USERY ha un intervallo di scadenza della parola d'ordine di 120 giorni.

- Utilizzare tale documentazione regolarmente per controllare i tentativi di collegamento non riusciti. E' possibile che l'eventuale intruso che tenti di accedere al sistema sia consapevole che il sistema prende dei provvedimenti dopo un numero di tentativi non riusciti. Ogni notte, l'ipotetico intruso potrebbe compiere un numero di tentativi inferiore rispetto al valore QMAXSIGN per evitare che l'utente si accorga di tali tentativi. Tuttavia, se si utilizza tale documentazione ogni mattina e si nota che alcuni profili utente presentano tentativi di collegamento non riusciti, è possibile sospettare la presenza di un problema.
- Identificare i profili utente che non vengono utilizzati da lungo tempo o le cui parole d'ordine non vengono modificate da lungo tempo.

Memorizzazione delle informazioni sulla parola d'ordine

Per supportare alcune funzioni di rete e requisiti di comunicazione, i server iSeries forniscono un metodo sicuro di memorizzazione delle parole d'ordine che possono essere decodificate. Il sistema utilizza queste parole d'ordine, ad esempio, per stabilire un collegamento SLIP ad un altro sistema. ("Sicurezza e sessioni di collegamento in uscita" a pagina 135 descrive questo utilizzo delle parole d'ordine memorizzate.)

I server iSeries memorizzano queste parole d'ordine speciali in un'area protetta che non è accessibile a programmi o interfacce utente. Solo funzioni di sistema esplicitamente autorizzate possono impostare queste parole d'ordine e richiamarle.

Ad esempio, quando si utilizza una parola d'ordine memorizzata per collegamenti SLIP in uscita, si imposta la parola d'ordine con il comando di sistema che crea il profilo di configurazione (WRKTCPPTP). E' necessario disporre *IOSYSCFG per utilizzare il comando. Uno script di collegamento con codifica speciale richiama la parola d'ordine e la decodifica durante la procedura di collegamento in uscita. La parola d'ordine decodificata non è visualizzabile per l'utente o in qualsiasi registrazione lavoro.

Come responsabile della sicurezza, è necessario stabilire se sarà consentita la memorizzazione di parole d'ordine che è possibile decodificare nel sistema. Si utilizza il valore di sistema Conservazione dati sicurezza server (QRETSVRSEC) per specificare questa opzione. Il valore predefinito è 0 (No). Quindi, il sistema non memorizzerà parole d'ordine che possono essere decodificare a meno che non si imposti esplicitamente questo valore di sistema.

Se si dispone di requisiti di comunicazione o di rete per le parole d'ordine memorizzate, si dovrebbero impostare normative appropriate e conoscere le normative e le pratiche dei propri partner di comunicazioni. Ad esempio, quando si utilizza SLIP per comunicare con un altro server iSeries, entrambi i sistemi dovrebbero prendere in considerazione l'impostazione di profili utente speciali per stabilire le sessioni. I profili speciali dovrebbero avere limitata autorizzazione nel sistema. Questo limita l'impatto sul proprio sistema se una parola d'ordine memorizzata viene compromessa sul sistema del partner.

Capitolo 4. Configurazione di iSeries per utilizzare Strumenti di sicurezza

Queste informazioni descrivono come configurare il sistema per utilizzare gli strumenti di sicurezza che fanno parte di OS/400. Quando si installa OS/400, gli strumenti di sicurezza sono pronti per essere utilizzati. Gli argomenti riportati di seguito forniscono dei suggerimenti per le procedure operative con gli strumenti di sicurezza.

Utilizzo di Strumenti di sicurezza in modo sicuro

Quando si installa OS/400, gli oggetti associati con gli strumenti di sicurezza sono protetti. Per utilizzare gli strumenti di sicurezza in modo sicuro, evitare di apportare modifiche all'autorizzazione per qualsiasi oggetto strumento di sicurezza.

Di seguito vengono riportate le impostazioni di sicurezza per gli oggetti strumento di sicurezza:

- I comandi e i programmi strumento di sicurezza si trovano nella libreria del prodotto QSYS. I comandi e i programmi vengono forniti con l'autorizzazione pubblica di *EXCLUDE. Molti dei comandi strumento di sicurezza creano i file nella libreria QUSRSYS. Quando il sistema crea tali file, l'autorizzazione pubblica per i file è *EXCLUDE.

  I file che contengono informazioni per produrre una documentazione modificata hanno nomi che iniziano con QSEC. I file che contengono informazioni per la gestione di profili utenti hanno nomi che iniziano con QASEC. Tali file contengono informazioni riservate sul sistema. Quindi, sarebbe opportuno non modificare l'autorizzazione pubblica ai file.
- Gli strumenti di sicurezza utilizzano l'impostazione del sistema normale per indirizzare un'emissione di stampa. Tali prospetti contengono informazioni riservate relative al sistema. Per indirizzare l'emissione in modo da proteggere la coda di emissione, apportare le modifiche necessarie al profilo utente o alla descrizione lavoro per utenti che eseguiranno gli strumenti di sicurezza.
- A causa delle funzioni di sicurezza e dal momento che accedono a molti oggetti sul sistema, i comandi strumento di sicurezza richiedono l'autorizzazione speciale *ALLOBJ. Alcuni comandi richiedono inoltre l'autorizzazione speciale *SECADM, *AUDIT o *IOSYSCFG. Per accertarsi che i comandi vengano eseguiti correttamente, sarebbe opportuno collegarsi come responsabile della riservatezza quando si utilizzano gli strumenti di sicurezza. Quindi, non dovrebbe essere necessario concedere l'autorizzazione privata a qualsiasi comando strumento di sicurezza.

Come evitare i conflitti di file

Molti dei comandi di documentazione strumento di sicurezza creano un file di database che è possibile utilizzare per stampare una versione modificata della documentazione. "Comandi e menu per i comandi di sicurezza" a pagina 30 indica il nome file per ciascun comando. E' possibile eseguire un comando soltanto da un lavoro alla volta. La maggior parte dei comandi dispone ora di controlli per

© Copyright IBM Corp. 1996, 2004

l'applicazione di questa regola. Se si esegue un comando quando non è ancora terminata l'esecuzione da parte di un altro lavoro, si riceverà un messaggio di errore.

Molti lavori di stampa sono lavori di lunga esecuzione. Sarà necessario evitare con cura i conflitti di file quando si inoltrano le documentazioni in batch o le si aggiungono al programma di pianificazione lavoro. Ad esempio, è possibile che si desideri stampare due versioni della documentazione PRTUSRPRF con criteri di selezione differenti. Se si inoltrano delle documentazioni in batch, sarebbe opportuno utilizzare una coda lavori che esegua soltanto un lavoro alla volta per assicurare che i lavori di documentazione vengano eseguiti in modo sequenziale.

Se si utilizza il programma di pianificazione lavoro, è necessario pianificare i due lavori in un periodo sufficientemente distanziato in modo che la prima versione venga completata prima dell'avvio del secondo lavoro.

Salvataggio di Strumenti di sicurezza

Si salvano i programmi strumento di sicurezza ogni qualvolta si esegue il comando Salvataggio sistema (SAVSYS) o un'opzione dal menu Salvataggio che esegue il comando SAVSYS.

I file strumento di sicurezza si trovano nella libreria QUSRSYS. L'utente avrebbe dovuto salvare tale libreria come parte delle normali procedure operative. La libreria QUSRSYS contiene i dati per molti programmi su licenza sul sistema. Consultare l'Information Center per ulteriori informazioni sui comandi e le opzioni per salvare la libreria QUSRSYS.

Comandi e menu per i comandi di sicurezza

Questa sezione descrive i comandi e i menu per gli strumenti di sicurezza. Esempi di come utilizzare i comandi sono inclusi nelle presenti informazioni.

Sono disponibili due menu per gli strumenti di sicurezza:

- Il menu SECTOOLS (Strumenti di sicurezza) per eseguire i comandi in modo interattivo.
- Il menu SECBATCH (Inoltro o Pianificazione documentazioni di sicurezza in batch) per eseguire i comandi di documentazione in batch. Il menu SECBATCH è composto da due parti. La prima parte del menu utilizza il comando Inoltro lavoro (SBMJOB) per inoltrare le documentazioni per un'elaborazione immediata in batch.

  La seconda parte del menu utilizza il comando Aggiunta specifica schedulazione lavori (ADDJOBSCDE). Si utilizza tale comando per pianificare l'esecuzione regolare delle documentazioni di sicurezza a un'ora e un giorno specificati.

Opzioni del menu Strumenti di sicurezza

La Tabella 6 a pagina 31 descrive tali opzioni di menu e i comandi associati:

Tabella 6. Comandi di strumento per i profili utente

Opzione di menu[1]	Nome comando	Descrizione	File di database utilizzato
1	ANZDFTPWD	Utilizzare il comando Analisi parole d'ordine predefinite per notificare e effettuare azioni sui profili utente che dispongono di una parola d'ordine uguale al nome profilo utente.	QASECPWD[2]
2	DSPACTPRFL	Utilizzare il comando Visualizzazione elenco profili attivi per visualizzare o stampare l'elenco di profili utente esenti dall'elaborazione ANZPRFACT.	QASECIDL[2]
3	CHGACTPRFL	Utilizzare il comando Modifica elenco profili attivi per aggiungere e rimuovere i profili utente dall'elenco di utenti esenti per il comando ANZPRFACT. Un profilo utente che si trova nell'elenco profili attivi è sempre attivo (finché non si rimuove il profilo dall'elenco). Il comando ANZPRFACT non disabilita un profilo che si trovi nell'elenco profili attivi, indipendentemente dal tempo in cui il profilo è rimasto inattivo.	QASECIDL[2]
4	ANZPRFACT	Utilizzare il comando Analisi attività profilo per disabilitare i profili utente che non sono stati utilizzati per un numero specificato di giorni. Dopo avere utilizzato il comando ANZPRFACT per specificare il numero di giorni, il sistema esegue il lavoro ANZPRFACT durante la notte. E' possibile utilizzare il comando CHGACTPRFL per esentare i profili utente dalla disabilitazione.	QASECIDL[2]
5	DSPACTSCD	Utilizzare il comando Visualizzazione pianificazione attivazione per visualizzare o stampare le informazioni sulla pianificazione per abilitare o disabilitare profili utenti specifici. Si crea la pianificazione con il comando CHGACTSCDE.	QASECACT[2]
6	CHGACTSCDE	Utilizzare il comando Modifica voce Scd di attivazione per rendere un profilo utente disponibile per il collegamento soltanto in alcune ore del giorno o della settimana. Per ciascun profilo utente che si pianifica, il sistema crea delle voci di pianificazione lavoro per le ore di abilitazione e di disabilitazione.	QASECACT[2]
7	DSPEXPSCD	Utilizzare il comando Visualizzazione pianificazione di scadenza per visualizzare o stampare l'elenco di profili utente pianificati da disabilitare o da eliminare dal sistema in futuro. Si utilizza il comando CHGEXPSCDE per impostare i profili utenti da mettere in scadenza.	QASECEXP[2]

Tabella 6. Comandi di strumento per i profili utente (Continua)

Opzione di menu[1]	Nome comando	Descrizione	File di database utilizzato
8	CHGEXPSCDE	Utilizzare il comando Modifica voce Scd di scadenza per pianificare la rimozione di un profilo utente. E' possibile rimuoverlo temporaneamente (disabilitandolo) o è possibile cancellarlo dal sistema. Tale comando utilizza una voce di pianificazione lavoro da eseguire ogni giorno alle 00:01 (1 minuto dopo mezzanotte). Il lavoro esamina il file QASECEXP per stabilire se è impostato un profilo utente che scadrà in tale giorno. Utilizzare il comando DSPEXPSCD per visualizzare i profili utente di cui è pianificata la scadenza.	QASECEXP[2]
9	PRTPRFINT	Utilizzare il comando Stampa valori interni profilo per stampare una documentazione contenente informazioni sul numero di voci contenute in un profilo utente. Il numero di voci stabilisce la dimensione del profilo utente.	

Note:

1. Le opzioni derivano dal menu SECTOOLS.
2. Questo file si trova nella libreria QUSRSYS.

E' possibile utilizzare il tasto pagina giù sul menu per visualizzare opzioni aggiuntive. La Tabella 7 descrive le opzioni di menu e i comandi associati per il controllo sicurezza:

Tabella 7. Comandi di strumento per il controllo sicurezza

Opzione di menu[1]	Nome comando	Descrizione	File di database utilizzato
10	CHGSECAUD	Utilizzare il comando Modifica controllo riservatezza per impostare il controllo sicurezza e per modificare i valori di sistema che lo controllano. Quando si esegue il comando CHGSECAUD, il sistema crea il giornale di controllo sicurezza (QAUDJRN), se non esiste già. Il comando CHGSECAUD fornisce opzioni che rendono più semplice impostare il valore di sistema QAUDLVL (livello di controllo). E' possibile specificare *ALL per attivare tutte le possibili impostazioni del livello di controllo. Oppure è possibile specificare *DFTSET per attivare le impostazioni utilizzate più (comunemente *AUTFAIL, *CREATE, *DELETE, *SECURITY e *SAVRST). **Nota:** se si utilizzano gli strumenti di sicurezza per impostare il controllo, accertarsi di pianificare la gestione dei ricevitori del giornale di controllo. In caso contrario, potrebbero verificarsi dei problemi con l'utilizzo del disco.	

Tabella 7. Comandi di strumento per il controllo sicurezza (Continua)

Opzione di menu[1]	Nome comando	Descrizione	File di database utilizzato
11	DSPSECAUD	Utilizzare il comando Visualizzazione controllo riservatezza per visualizzare informazioni relative al giornale di controllo sicurezza e i valori di sistema che controllano tale controllo.	

Note:
1. Le opzioni derivano dal menu SECTOOLS.

Utilizzo del menu batch di sicurezza

Di seguito è riportata la prima parte del menu SECBATCH:

```
SECBATCH         Inoltro o pianificazione prospetti di sicurezza in batch
                                                                  Sistema:
 Scegliere una delle seguenti opzioni:

  Inoltrare prospetti in batch
     1. Oggetti di adozione
     2. Voci giornale di controllo
     3. Autorità elenco autorizzazioni
     4. Autorità comandi
     5. Autorità private comandi
     6. Sicurezza delle comunicazioni
     7. Autorità indirizzario
     8. Autorità privata indirizzario
     9. Autorità documento
    10. Autorità privata documento
    11. Autorità file
    12. Autorità privata file
    13. Autorità cartella
```

Quando si seleziona un'opzione da tale menu, viene visualizzato il pannello Inoltro lavoro (SBMJOB). Se si desidera modificare le opzioni predefinite per il comando, è possibile premere F4 (Richiesta) sulla riga *Comando da eseguire*.

Per visualizzare la pianificazione documentazioni batch, scorrere giù la pagina del menu SECBATCH. Utilizzando tale opzione su questa parte del menu è possibile, ad esempio, impostare il sistema in modo che esegua regolarmente le versioni modificate delle documentazioni. E' possibile scorrere giù la pagina per opzioni di menu aggiuntive. Quando si seleziona un'opzione da tale parte del menu, viene visualizzato il pannello Aggiunta specifica schedulazione lavori (ADDJOBSCDE).

E' possibile posizionare il cursore sulla riga *Comando da eseguire* e premere F4 (Richiesta) per scegliere differenti impostazioni per la documentazione. Sarebbe opportuno assegnare un nome lavoro significativo in modo che sia possibile riconoscere la voce quando si visualizzano le voci di pianificazione lavoro.

Opzioni del menu Batch di sicurezza

La Tabella 8 a pagina 34 descrive le opzioni di menu e i comandi associati per le documentazioni di sicurezza.

Quando si utilizzano le documentazioni di sicurezza, il sistema stampa soltanto le informazioni che corrispondono sia ai criteri di selezione specificati che i criteri di selezione per lo strumento. Ad esempio, le descrizioni lavoro specificate che utilizzano un nome profilo utente sono di rilievo per la sicurezza. Quindi, la documentazione (PRTJOBDAUT) della descrizione lavoro stampa le descrizioni

lavoro nella libreria specificata soltanto se l'autorizzazione pubblica per la descrizione lavoro non è *EXCLUDE *e* se la descrizione lavoro specifica un nome profilo utente nel parametro USER.

In modo simile, quando si stampano le informazioni del sottosistema (comando PRTSBSDAUT), il sistema stampa le informazioni su un sottosistema soltanto quando la descrizione del sottosistema ha una voce di comunicazioni che specifica un profilo utente.

Se una documentazione particolare stampa meno informazioni del previsto, consultare le informazioni dell'aiuto in linea per individuare i criteri di selezione per la documentazione.

Tabella 8. Comandi per documentazioni di sicurezza

Opzione di menu[1]	**Nome comando**	**Descrizione**	**File di database utilizzato**
1, 40	PRTADPOBJ	Utilizzare il comando Stampa oggetti di adozione per stampare un elenco di oggetti che adottano l'autorizzazione del profilo utente specificato. E' possibile specificare un singolo profilo, un nome profilo generico (come ad esempio tutti i profili che iniziano con Q) o tutti i profili utente sul sistema. Tale documentazione ha due versioni. La documentazione completa elenca tutti gli oggetti adottati che corrispondono ai criteri di selezione. La documentazione modificata elenca le differenze tra gli oggetti adottati che sono correntemente sul sistema e gli oggetti adottati che si trovavano sul sistema durante l'ultimo utilizzo della documentazione.	QSECADPOLD[2]
2, 41	DSPAUDJRNE	Utilizzare il comando Visualizzazione voci giornale di controllo per visualizzare o stampare informazioni relative alle voci nel giornale di controllo sicurezza. E' possibile selezionare tipi di voci specifici, utenti specifici e un periodo di tempo.	QASYxxJ4[3]

Tabella 8. Comandi per documentazioni di sicurezza (Continua)

Opzione di menu[1]	Nome comando	Descrizione	File di database utilizzato
3, 42	PRTPVTAUT *AUTL	Quando si utilizza il comando Stampa autorizzazioni private per gli oggetti *AUTL, si riceve un elenco di tutti gli elenchi di autorizzazioni sul sistema. La documentazione include gli utenti autorizzati a ciascun elenco e l'autorizzazione di cui dispongono gli utenti per l'elenco. Utilizzare queste informazioni come aiuto per analizzare le origini dell'autorizzazione all'oggetto sul sistema. Tale documentazione ha tre versioni. La documentazione completa elenca tutti gli elenchi di autorizzazioni sul sistema. La documentazione modificata elenca aggiunte e modifiche all'autorizzazione dall'ultimo utilizzo della documentazione. La documentazione cancellata elenca gli utenti la cui autorizzazione all'elenco di autorizzazioni è stata cancellata dall'ultimo utilizzo della documentazione. Quando si stampa la documentazione completa, è disponibile l'opzione per stampare un elenco di oggetti protetti da ciascun elenco di autorizzazioni. Il sistema creerà una documentazione separata per ciascun elenco di autorizzazioni.	QSECATLOLD[2]
6, 45	PRTCMNSEC	Utilizzare il comando Stampa riservatezza di comunicazioni per stampare le impostazioni rilevanti per la sicurezza per gli oggetti che influenzano le comunicazioni sul sistema. Tali impostazioni influenzano il modo in cui gli utenti e i lavori possono accedere al sistema. Questo comando produce due tipi di documentazioni: uno che visualizza gli elenchi di configurazioni sul sistema e un altro che elenca i parametri rilevanti per la sicurezza delle descrizioni linea riga, programmi di controllo e descrizioni unità. Ciascuna di tali documentazioni ha una versione completa e una versione modificata.	QSECCMNOLD[2]

Tabella 8. Comandi per documentazioni di sicurezza (Continua)

Opzione di menu[1]	Nome comando	Descrizione	File di database utilizzato
15, 54	PRTJOBDAUT	Utilizzare il comando Stampa autorizzazione descrizione lavoro per stampare un elenco di descrizioni lavoro che specificano un profilo utente e dispongono di autorizzazione pubblica diversa da *EXCLUDE. La documentazione visualizza le autorizzazioni speciali per il profilo utente specificato nella descrizione lavoro. Tale documentazione ha due versioni. La documentazione completa elenca tutti gli oggetti descrizione lavoro che corrispondono ai criteri di selezione. La documentazione modificata elenca le differenze tra gli oggetti descrizione lavoro correntemente sul sistema e gli oggetti descrizione lavoro che si trovavano sul sistema durante l'ultimo utilizzo della documentazione.	QSECJBDOLD[2]
Consultare nota 4	PRTPUBAUT	Utilizzare il comando Stampa oggetti autorizzati pubblicamente per stampare un elenco di oggetti la cui autorizzazione pubblica non è *EXCLUDE. Quando si esegue il comando, si specifica il tipo di oggetto e la libreria o le librerie per la documentazione. Utilizzare il comando PRTPUBAUT per stampare le informazioni relative agli oggetti a cui ogni utente sul sistema può accedere. Tale documentazione ha due versioni. La documentazione completa elenca tutti gli oggetti che corrispondono ai criteri di selezione. La documentazione modificata elenca le differenze tra gli oggetti specificati correntemente sul sistema e gli oggetti (dello stesso tipo nella stessa libreria) che si trovavano sul sistema durante l'ultimo utilizzo della documentazione.	QPBxxxxxx[5]
Consultare nota 5.	PRTPVTAUT	Utilizzare il comando Stampa autorizzazioni private per stampare un elenco di autorizzazioni private agli oggetti del tipo specificato nella libreria specificata. Utilizzare tale documentazione come aiuto per stabilire le origini dell'autorizzazione agli oggetti. Tale documentazione ha tre versioni. La documentazione completa elenca tutti gli oggetti che corrispondono ai criteri di selezione. La documentazione modificata elenca le differenze tra gli oggetti specificati correntemente sul sistema e gli oggetti (dello stesso tipo nella stessa libreria) che si trovavano sul sistema durante l'ultimo utilizzo della documentazione. La documentazione cancellata elenca gli utenti la cui autorizzazione a un oggetto è stata cancellata dall'ultimo utilizzo della documentazione.	QPVxxxxxx[5]

Tabella 8. Comandi per documentazioni di sicurezza (Continua)

Opzione di menu[1]	Nome comando	Descrizione	File di database utilizzato
24, 63	PRTQAUT	Utilizzare il comando Stampa autorizzazione coda per stampare le impostazioni di sicurezza per le code di emissione e le code lavoro sul sistema. Tali impostazioni controllano chi può visualizzare e modificare le voci nella coda di emissione o nella coda lavori. Tale documentazione ha due versioni. La documentazione completa elenca tutti gli oggetti della coda lavori e della coda di emissione che corrispondono ai criteri di selezione. La documentazione modificata elenca le differenze tra gli oggetti della coda di emissione e della coda lavori correntemente sul sistema e gli oggetti della della coda di emissione e della coda lavori che si trovavano sul sistema durante l'ultimo utilizzo della documentazione.	QSECQOLD[2]
25, 64	PRTSBSDAUT	Utilizzare il comando Stampa descrizione sottosistema per stampare le voci di comunicazione rilevanti per la sicurezza per le descrizioni sottosistema sul sistema. Tali impostazioni controllano in che modo il lavoro viene immesso sul sistema e la modalità di esecuzione dei lavori. La documentazione stampa una descrizione sottosistema soltanto se dispone di voci di comunicazione che specificano un nome profilo utente. Tale documentazione ha due versioni. La documentazione completa elenca tutti gli oggetti descrizione sottosistema che corrispondono ai criteri di selezione. La documentazione modificata elenca le differenze tra gli oggetti descrizione sottosistema correntemente sul sistema e gli oggetti descrizione sottosistema che si trovavano sul sistema durante l'ultimo utilizzo della documentazione.	QSECSBDOLD[2]
26, 65	PRTSYSSECA	Utilizzare il comando Stampa attributi riservatezza sistema per stampare un elenco di attributi di rete e di valori di sistema rilevanti per la sicurezza. La documentazione visualizza il valore corrente e il valore consigliato.	
27, 66	PRTTRGPGM	Utilizzare il comando Stampa programmi trigger per stampare un elenco di programmi trigger associati ai file di database sul sistema. Tale documentazione ha due versioni. La documentazione completa elenca ciascun programma trigger assegnato e che corrisponde ai criteri di selezione. La documentazione modificata elenca i programmi trigger che sono stati assegnati dall'ultimo utilizzo della documentazione.	QSECTRGOLD[2]

Tabella 8. Comandi per documentazioni di sicurezza (Continua)

Opzione di menu[1]	Nome comando	Descrizione	File di database utilizzato
28, 67	PRTUSROBJ	Utilizzare il comando Stampa oggetti utente per stampare un elenco di oggetti utente (oggetti non forniti da IBM) che si trovano nella libreria. E' possibile utilizzare tale documentazione per stampare un elenco di oggetti utente che si trovano in una libreria (come ad esempio QSYS) contenuta nella parte di sistema dell'elenco librerie. Tale documentazione ha due versioni. La documentazione completa elenca tutti gli oggetti utente che corrispondono ai criteri di selezione. La documentazione modificata elenca le differenze tra gli oggetti utente che sono correntemente sul sistema e gli oggetti utente che si trovavano sul sistema durante l'ultimo utilizzo della documentazione.	QSECPUOLD[2]
29, 68	PRTUSRPRF	Utilizzare il comando Stampa profilo utente per analizzare i profili utente che corrispondono ai criteri specificati. E' possibile selezionare i profili utente sulla base di autorizzazioni speciali, classe utente o mancata corrispondenza tra autorizzazioni speciali e classe utente. E' possibile stampare le informazioni sull'autorizzazione, sull'ambiente o sul livello della parola d'ordine.	
30, 69	PRTPRFINT	Utilizzare il comando Stampa valori interni profilo per stampare una documentazione contenente informazioni interne sul numero di voci.	
31, 70	CHKOBJITG	Utilizzare il comando Controllo integrità oggetto per stabilire se gli oggetti eseguibili (come ad esempio i programmi) sono stati modificati senza l'utilizzo di un programma di compilazione. Tale comando può aiutare a individuare i tentativi di introduzione di un programma virus sul sistema o di modifica di un programma per eseguire istruzioni non autorizzate. Il manuale *Riferimenti alla sicurezza iSeries* fornisce ulteriori informazioni sul comando CHKOBJITG.	

Tabella 8. Comandi per documentazioni di sicurezza (Continua)

Opzione di menu[1]	Nome comando	Descrizione	File di database utilizzato

Note:

1. Le opzioni derivano dal menu SECBATCH.
2. Questo file si trova nella libreria QUSRSYS.
3. xx è il tipo di voce di giornale di due caratteri. Ad esempio, il file di emissione modello per le voci di giornale AE è QSYS/QASYAEJ4. I file di emissione modello sono descritti nell'Appendice F del manuale *Riferimenti alla sicurezza iSeries*.
4. Il menu SECBATCH contiene opzioni per i tipi di oggetto che sono normalmente di interesse dei responsabili della sicurezza. Ad esempio, utilizzare le opzioni 11 o 50 per eseguire il comando PRTPUBAUT rispetto agli oggetti *FILE. Utilizzare le opzioni generali (18 e 57) per specificare il tipo di oggetto.
5. Il menu SECBATCH contiene opzioni per i tipi di oggetto che sono normalmente di interesse dei responsabili della sicurezza. Ad esempio, le opzioni 12 o 51 eseguono il comando PRTPVTAUT rispetto agli oggetti *FILE. Utilizzare le opzioni generali (19 e 58) per specificare il tipo di oggetto.
6. xxxxxx nel nome del file corrisponde al tipo di oggetto. Ad esempio, il file per gli oggetti programma è chiamato QPBPGM per le autorizzazioni pubbliche e QPVPGM per le autorizzazioni private. I file si trovano nella libreria QUSRSYS.

   Il file contiene un membro per ciascuna libreria per cui è stata stampata la documentazione. Il nome membro è uguale al nome libreria.

Comandi per personalizzare la sicurezza

La Tabella 9 descrive i comandi che è possibile utilizzare per personalizzare la sicurezza sul sistema. Tali comandi si trovano nel menu SECTOOLS.

Tabella 9. Comandi per personalizzare il sistema

Opzione di menu[1]	Nome comando	Descrizione	File di database utilizzato
60	CFGSYSSEC	Utilizzare il comando Configurazione riservatezza sistema per impostare i valori di sistema rilevanti per la sicurezza sulle impostazioni consigliate. Il comando imposta inoltre il controllo sicurezza sul sistema. "Valori impostati dal comando Configurazione riservatezza sistema" a pagina 40 descrive le attività del comando. **Nota:** per ottenere consigli sulla sicurezza adeguati alla situazione dell'utente, eseguire il wizard di sicurezza iSeries o iSeries Security Advisor invece di eseguire tale comando. Consultare il Capitolo 2, "Wizard di sicurezza iSeries e eServer Security Planner", a pagina 11 per informazioni su tali strumenti.	
61	RVKPUBAUT	Utilizzare il comando Revoca autorizzazione pubblica per impostare l'autorizzazione pubblica su *EXCLUDE per una serie di comandi sensibili alla sicurezza sul proprio sistema. "Funzioni del comando Revoca autorizzazione pubblica" a pagina 42 elenca le azioni eseguite dal comando RVKPUBAUT.	

Note:

1. Le opzioni derivano dal menu SECTOOLS.

Valori impostati dal comando Configurazione riservatezza sistema

La Tabella 10 elenca i valori di sistema impostati quando si esegue il comando CFGSYSSEC. Il comando CFGSYSSEC esegue un programma denominato QSYS/QSECCFGS.

Tabella 10. Valori impostati dal comando CFGSYSSEC

Nome valore di sistema	Impostazione	Descrizione valore di sistema
QALWOBJRST	*NONE	Se è possibile il ripristino di programmi di stato del sistema e di programmi che adottano l'autorizzazione
QAUTOCFG	0 (No)	Configurazione automatica di nuove unità
QAUTOVRT	0	Il numero di descrizioni di unità virtuali che il sistema creerà automaticamente se non vi è alcuna unità disponibile per l'uso.
QDEVRCYACN	*DSCMSG (Scollegare con messaggio)	Operazione di sistema quando viene ristabilita la comunicazione
QDSCJOBITV	120	Periodo di tempo prima che il sistema esegua un'operazione su un lavoro scollegato
QDSPSGNINF	1 (Sì)	Se gli utenti visualizzano il pannello delle informazioni di collegamento
QINACTITV	60	Periodo di tempo prima che il sistema esegua un'operazione su un lavoro interattivo inattivo
QINACTMSGQ	*ENDJOB	Operazione che il sistema esegue per un lavoro inattivo
QLMTDEVSSN	1 (Sì)	Se gli utenti devono limitarsi al collegamento ad un'unità alla volta
QLMTSECOFR	1 (Sì)	Se gli utenti *ALLOBJ e *SERVICE sono limitati a specifiche unità
QMAXSIGN	3	Quanti tentativi di collegamento ad esito negativo consecutivi sono consentiti
QMAXSGNACN	3 (Entrambi)	Se il sistema disabilita la stazione di lavoro o il profilo utente quando si raggiunge il limite QMAXSIGN.
QRMTSIGN	*FRCSIGNON	Come gestisce il sistema un tentativo di collegamento remoto (pass-through o TELNET).
QRMTSVRATR	0 (Disattivato)	Consente al sistema di essere analizzato in remoto.
QSECURITY [1 a pagina 41]	50	Il livello di sicurezza applicato
QVFYOBJRST	3 (Verificare le firme al ripristino)	Verificare l'oggetto al ripristino
QPWDEXPITV	60	Con quale frequenza gli utenti devono modificare le parole d'ordine
QPWDMINLEN	6	Lunghezza minima per le parole d'ordine
QPWDMAXLEN	8	Lunghezza massima per le parole d'ordine
QPWDPOSDIF	1 (Sì)	Se ogni posizione in una nuova parola d'ordine deve essere differente dalla stessa posizione nell'ultima parola d'ordine
QPWDLMTCHR	Consultare nota 2 a pagina 41	Caratteri non consentiti nelle parole d'ordine
QPWDLMTAJC	1 (Sì)	Se numeri adiacenti sono proibiti nelle parole d'ordine
QPWDLMTREP	2 (Non possono essere ripetuti consecutivamente)	Se caratteri che si ripetono sono proibiti nelle parole d'ordine

Tabella 10. Valori impostati dal comando CFGSYSSEC (Continua)

Nome valore di sistema	Impostazione	Descrizione valore di sistema
QPWDRQDDGT	1 (Sì)	Se le parole d'ordine devono contenere almeno un numero
QPWDRQDDIF	1 (32 parole d'ordine univoche)	Quante parole d'ordine univoche sono richieste prima che una parola d'ordine possa essere ripetuta
QPWDVLDPGM	*NONE	Il programma di uscita utente che il sistema richiama per convalidare le parole d'ordine

Note:

1. Se l'esecuzione attualmente avviene con un valore QSECURITY di 40 o inferiore, accertarsi di esaminare le informazioni nel Capitolo 2 del manuale *Riferimenti alla sicurezza iSeries* prima di passare ad un livello di sicurezza superiore.
2. I caratteri limitati sono memorizzati nel messaggio con ID CPXB302 contenuto nel file di messaggi QSYS/QCPFMSG. Sono inviati come AEIOU@$#. E' possibile utilizzare il comando Modifica descrizione messaggio (CHGMSGD) per modificare i caratteri limitati. Il valore di sistema QPWDLMTCHR non è applicato ai livelli di parola d'ordine 2 o 3.

Il comando CFGSYSSEC inoltre imposta la parola d'ordine su *NONE per i seguenti profili utente forniti da IBM:

QSYSOPR
QPGMR
QUSER
QSRV
QSRVBAS

Infine, il comando CFGSYSSEC imposta il controllo di sicurezza utilizzando il comando Modifica controllo riservatezza (CHGSECAUD). Il comando CFGSYSSEC attiva il controllo delle operazioni e degli oggetti ed inoltre, specifica la serie di operazioni predefinita da controllare nel comando CHGSECAUD.

Personalizzazione del programma

Se alcune di queste impostazioni non sono appropriate per la propria installazione, è possibile creare la propria versione del programma che elabora il comando. Effettuare le seguenti operazioni.

__ Passo 1. Utilizzare il comando Reperimento origine CL (RTVCLSRC) per copiare l'origine per il programma che si esegue quando si utilizza il comando CFGSYSSEC. Il programma da reperire è QSYS/QSECCFGS. Una volta reperito, assegnargli un *nome differente*.

__ Passo 2. Editare il programma per apportare le modifiche. Quindi compilarlo. Quando lo si compila, accertarsi di *non* sostituire il programma QSYS/QSECCFGS fornito da IBM. Il proprio programma dovrebbe avere un nome differente.

__ Passo 3. Utilizzare il comando Modifica comando (CHGCMD) per modificare il programma in modo che elabori il parametro (PGM) del comando per il comando CFGSYSSEC. Impostare il valore PGM sul nome del proprio programma. Ad esempio, se si crea un programma nella libreria QGPL denominata MYSECCFG, si dovrebbe immettere quanto segue:

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

Nota: se si modifica il programma QSYS/QSECCFGS, IBM non può fornire garanzie esplicite o implicite di affidabilità, stato di efficienza, prestazioni o funzionalità del programma. Viene espressamente declinata ogni responsabilità per le garanzie implicite di commerciabilità e adeguatezza ad un particolare scopo.

Funzioni del comando Revoca autorizzazione pubblica

E' possibile utilizzare il comando Revoca autorizzazione pubblica (RVKPUBAUT) per impostare l'autorizzazione pubblica su *EXCLUDE per una serie di comandi e programmi. Il comando RVKPUBAUT esegue un programma denominato QSYS/QSECRVKP. Quando viene consegnato, QSECRVKP revoca l'autorizzazione pubblica (impostandola su *EXCLUDE) per i comandi elencati nella Tabella 11 e le API (application programming interface) elencate nella Tabella 12. All'arrivo del sistema, questi comandi ed API hanno l'autorizzazione pubblica impostata su *USE.

I comandi elencati nella Tabella 11 e le API elencate nella Tabella 12 eseguono tutti delle funzioni nel sistema tali da fornire l'opportunità di un uso illecito. Come responsabile della sicurezza, si dovrebbero autorizzare esplicitamente gli utenti ad eseguire questi comandi e programmi piuttosto che renderli disponibili a tutti gli utenti di sistema.

Quando si esegue il comando RVKPUBAUT, si specifica la libreria che contiene i comandi. Il valore predefinito è la libreria QSYS. Se si dispone di più di una lingua nazionale sul sistema, è necessario eseguire il comando per ogni libreria QSYSxxx.

Tabella 11. Comandi la cui autorizzazione pubblica è impostata dal comando RVKPUBAUT

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIBRSTOBJRSTS36F
ADDWSE	CRTCFGL	RSTS36FLR
CHGAJE	CRTCTLAPPC	RSTS36LIBM
CHGCFGL	CRTDEVAPPC	STRRMTSPT
CHGCFGLE	CRTSBSD	STRSBS
CHGCMNE	ENDRMTSPT	WRKCFGL
CHGCTLAPPC	RMVAJE	
CHGDEVAPPC	RMVCFGLE	

Le API nella Tabella 12 si trovano tutte nella libreria QSYS:

Tabella 12. Programmi la cui autorizzazione pubblica è impostata dal comando RVKPUBAUT

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

Quando si esegue il comando RVKPUBAUT, il sistema imposta l'autorizzazione pubblica per l'indirizzario pricipale su *USE (a meno che non sia già impostata su *USE o su un livello inferiore).

Personalizzazione del programma

Se alcune di queste impostazioni non sono appropriate per la propria installazione, è possibile creare la propria versione del programma che elabora il comando. Effettuare le seguenti operazioni.

__ Passo 1. Utilizzare il comando Reperimento origine CL (RTVCLSRC) per copiare l'origine per il programma che si esegue quando si utilizza il comando RVKPUBAUT. Il programma da reperire è QSYS/QSECRVKP. Una volta reperito, assegnargli un *nome differente*.

__ Passo 2. Editare il programma per apportare le modifiche. Quindi compilarlo. Quando lo si compila, accertarsi di *non* sostituire il programma QSYS/QSECRVKP fornito da IBM. Il proprio programma dovrebbe avere un nome differente.

__ Passo 3. Utilizzare il comando Modifica comando (CHGCMD) per modificare il programma in modo che elabori il parametro (PGM) del comando per il comando RVKPUBAUT. Impostare il valore PGM sul nome del proprio programma. Ad esempio, se si crea un programma nella libreria QGPL denominata MYRVKPGM, si dovrebbe immettere quanto segue:

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

Nota: se si modifica il programma QSYS/QSECRVKP, IBM non può fornire garanzie esplicite o implicite di affidabilità, stato di efficienza, prestazioni o funzionalità del programma. Viene espressamente declinata ogni responsabilità per le garanzie implicite di commerciabilità e adeguatezza ad un particolare scopo.

Parte 2. Sicurezza iSeries avanzata

© Copyright IBM Corp. 1996, 2004

Capitolo 5. Protezione delle informazioni tramite autorizzazione oggetto

L'impegno come responsabile della sicurezza è quello di proteggere le informazioni dell'organizzazione senza limitare eccessivamente gli utenti che operano sul sistema. E' necessario assicurarsi che gli utenti dispongano dell'autorizzazione sufficiente ad eseguire i propri lavori senza fornirgli però l'autorizzazione di esaminare tutto il sistema ed effettuare modifiche non autorizzate.

Suggerimento sulla sicurezza

Un'autorizzazione troppo ristretta può essere controproducente. Gli utenti talvolta reagiscono alle limitazione dell'autorizzazione che risultano troppo restrittive condividendo reciprocamente le parole d'ordine.

Il sistema operativo OS/400 fornisce sicurezza integrata dell'oggetto. Gli utenti devono utilizzare le interfacce che il sistema fornisce per accedere agli oggetti. Ad esempio, se si vuole accedere ad un file di database, è necessario utilizzare comandi o programmi progettati per l'accesso ai file di database. Non è possibile utilizzare un comando progettato per l'accesso ad una coda messaggi o ad una registrazione lavori.

Quando si usa un'interfaccia di sistema per accedere ad un oggetto, il sistema verifica che l'utente abbia l'autorizzazione all'oggetto richiesta da quell'interfaccia. L'autorizzazione all'oggetto è uno strumento potente e flessibile per proteggere le risorse sul sistema. L'impegno come responsabile della sicurezza è quello di impostare uno schema efficace di sicurezza dell'oggetto di cui è possibile la gestione e la manutenzione.

Applicazione dell'autorizzazione all'oggetto

Quando si tenta l'accesso ad un oggetto, il sistema operativo controlla l'autorizzazione a tale oggetto. Tuttavia, se il livello di sicurezza sul proprio sistema (valore di sistema QSECURITY) è impostato su 10 o 20, ogni utente automaticamente ha l'autorizzazione ad accedere ad ogni oggetto poiché ogni profilo utente dispone dell'autorizzazione speciale *ALLOBJ.

Suggerimento sull'autorizzazione all'oggetto: se non si è certi di utilizzare la sicurezza dell'oggetto, verificare il valore di sistema QSECURITY (livello di sicurezza). Se QSECURITY è 10 o 20, non si sta utilizzando la sicurezza dell'oggetto.

Sono necessarie pianificazione e preparazione prima di passare al livello di sicurezza 30 o superiore. Altrimenti, i propri utenti potrebbero non essere in grado di accedere alle informazioni necessarie.

L'argomento **Sicurezza e pianificazione di base del sistema** nell'Information Center fornisce un metodo per analizzare le applicazioni e decidere come si dovrebbe configurare la sicurezza dell'oggetto. Se non si sta ancora utilizzando la sicurezza dell'oggetto o il proprio schema di sicurezza dell'oggetto è obsoleto o non lineare, leggere questo argomento come guida di introduzione.

© Copyright IBM Corp. 1996, 2004

Sicurezza menu

Il server iSeries era originariamente progettato come un prodotto conseguente a S/36 e S/38. Molte istallazioni di server iSeries erano, contemporaneamente, installazioni di S/36 o S/38. Per controllare ciò che gli utenti potevano fare, i responsabili della sicurezza su quei sistemi precedenti spesso utilizzavano una tecnica a cui si fa riferimento come **sicurezza menu** o **controllo accesso menu**.

Controllo accesso menu significa che quando un utente si collega, visualizza un menu. L'utente può eseguire solo le funzioni che sono elencate nel menu. L'utente non può richiamare una riga comandi sul sistema per eseguire le funzioni non inserite nel menu. In teoria, il responsabile della sicurezza non dovrebbe preoccuparsi dell'autorizzazione agli oggetti poiché menu e programmi controllano le possibili azioni degli utenti.

Il server iSeries fornisce diverse opzioni profilo utente per assistenza con il controllo accesso menu, è possibile utilizzare il:

- Parametro **Menu iniziale** (INLMNU) per controllare quale menu l'utente visualizza per primo dopo il collegamento.
- Parametro **Programma iniziale** (INLPGM) per eseguire un programma di configurazione prima che l'utente visualizzi un menu. Oppure, si può utilizzare il parametro INLPGM per limitare un utente all'esecuzione di un singolo programma.
- Parametro **Possibilità limitate** (LMTCPB) per consentire all'utente solo una serie limitata di comandi. Impedisce inoltre all'utente di specificare un programma o menu iniziale differente sul pannello Collegamento. (Il parametro LMTCPB limita solo i comandi immessi dalla riga comandi.)

Limitazioni del controllo accesso menu

I computer e gli utenti dei computer hanno subito moltissimi cambiamenti da qualche anno a questa parte. Sono disponibili molti strumenti, quali ad esempio i programmi query ed i fogli elettronici, in modo che gli utenti possano eseguire per proprio conto un un pò di programmazione per alleggerire i reparti IS. Alcuni strumenti, come ad esempio SQL o ODBC, forniscono la capacità di visualizzare e modificare informazioni. Abilitare questi strumenti all'interno di una struttura di menu è estremamente complicato.

Le stazioni di lavoro a funzione fissa ("schermo verde") stanno rapidamente venendo sostituite da personal computer e reti da computer a computer. Se il proprio sistema fa parte di una rete, gli utenti possono entrare nel sistema senza neanche visualizzare un pannello o un menu di collegamento.

Come responsabile della sicurezza nel tentativo di applicare il controllo accesso menu, si incontrano due problemi basilari:

- Se si riescono a limitare gli utenti all'utilizzo dei soli menu, essi saranno probabilmente insoddisfatti poiché la loro capacità di servirsi di strumenti moderni è ridotta.
- Se non si riesce ad ottenere ciò, si potrebbero rendere vulnerabili informazioni critiche e confidenziali che si suppone il controllo accesso menu dovrebbe proteggere. Quando il proprio sistema fa parte di una rete, la capacità di applicare il controllo accesso menu si riduce. Ad esempio, il parametro LMTCPB si applica solo ai comandi immessi da una riga comandi in una sessione interattiva. Il parametro LMTCPB non ha effetto sulle richieste provenienti dalle sessioni di comunicazione, come ad esempio trasferimento file PC, FTP o comandi remoti.

Potenziamento del controllo accesso menu tramite la sicurezza dell'oggetto

Con le molte nuove opzioni disponibili per il collegamento ai sistemi, uno schema di sicurezza proficuo per il server iSeries per il futuro non può basarsi unicamente sul controllo accesso menu. Questo argomento fornisce suggerimenti per passare ad un ambiente di sicurezza oggetto complementare al controllo accesso menu.

L'argomento *Sicurezza e pianificazione di base del sistema* nell'Information Center descrive una tecnica per analizzare l'autorizzazione che gli utenti devono avere relativamente agli oggetti per eseguire le applicazioni correnti. Si assegnano quindi gli utenti ai gruppi e si concede ai gruppi l'autorizzazione appropriata. Questo è un approccio logico e ragionevole. Tuttavia, se il proprio sistema è stato operativo per molti anni e dispone di molte applicazioni, l'attività di analisi delle applicazioni e configurazione dell'autorizzazione all'oggetto può probabilmente sembrare un compito gravoso.

Suggerimento sull'autorizzazione all'oggetto: i menu correnti combinati con i programmi che adottano l'autorizzazione dei proprietari del programma possono fornire una transizione che supera il controllo accesso menu. Assicurarsi di proteggere sia i programmi che adottano l'autorizzazione che i profili utente che la possiedono.

L'utente può essere in grado di utilizzare i menu correnti per assistenza nella configurazione di un ambiente di transizione mentre si analizzano gradualmente le applicazioni e gli oggetti. Il seguente è un esempio che utilizza il menu Immissione ordine (OEMENU) ed i file e programmi associati.

Esempio: configurazione di un ambiente di transizione

Questo esempio inizia con i seguenti presupposti e requisiti:

- Tutti i file si trovano nella libreria ORDERLIB.
- L'utente non conosce i nomi di tutti i file. Non conosce nemmeno quale autorizzazione richiedono le opzioni menu per file differenti.
- Il menu e tutti i programmi da esso richiamati si trovano in una libreria denominata ORDERPGM.
- Si desidera che chiunque si colleghi al sistema sia in grado di visualizzare informazioni in tutti i file di ordine, file cliente e file di voci (con query o fogli elettronici, ad esempio).
- Solo utenti il cui menu di collegamento corrente è OEMENU dovrebbero essere in grado di modificare i file. E, devono utilizzare i programmi nel menu per farlo.
- Utenti di sistema che non sono responsabili della sicurezza non dispongono dell'autorizzazione speciale *ALLOBJ o *SECADM.

Effettuare i seguenti passi per modificare questo ambiente controllo accesso menu in modo che soddisfi la necessità di query:

__ Passo 1. Creare un elenco di utenti il cui menu iniziale è l'OEMENU.

E' possibile utilizzare il comando Stampa profilo utente (PRTUSRPRF *ENVINFO) per elencare l'ambiente per ogni profilo utente sul sistema. Il documento include il menu iniziale, il programma iniziale e la libreria corrente. La Figura 7 a pagina 66 mostra un esempio di documento.

__ Passo 2. Accertarsi che l'oggetto OEMENU (può essere un oggetto *PGM o un oggetto *MENU) sia di proprietà di un profilo utente non utilizzato per il collegamento. Il profilo utente dovrebbe essere disabilitato o avere una parola d'ordine *NONE. Per questo esempio, presupponiamo che OEOWNER sia il proprietario dell'oggetto programma OEMENU.

__ Passo 3. Assicurarsi che il profilo utente proprietario dell'oggetto programma OEMENU non sia un profilo di gruppo. E' possibile utilizzare il seguente comando:

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

__ Passo 4. Modificare il programma OEMENU in modo che adotti l'autorizzazione del profilo utente OEOWNER. (Utilizzare il comando CHGPGM per modificare il parametro USRPRF in *OWNER.)

Nota: gli oggetti *MENU non possono adottare l'autorizzazione. Se OEMENU è un oggetto *MENU, è possibile adattare questo esempio tramite una delle seguenti azioni:

- Creare un programma per visualizzare il menu.
- Utilizzare l'autorizzazione adottata per i programmi in esecuzione quando l'utente seleziona opzioni dal menu OEMENU.

__ Passo 5. Impostare l'autorizzazione pubblica per tutti i file in ORDERLIB su *USE immettendo i seguenti due comandi:

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

Tenere a mente che se si seleziona l'autorizzazione *USE, gli utenti possono copiare il file utilizzando il Trasferimento file PC o l'FTP.

__ Passo 6. Assegnare al profilo che possiede il programma menu l'autorizzazione *ALL ai file immettendo quanto segue:

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

Per la maggior parte delle applicazioni, l'autorizzazione *CHANGE ai file è sufficiente. Tuttavia, le applicazioni possono eseguire funzioni, come ad esempio l'eliminazione dei membri file fisico, che richiedono un'autorizzazione superiore a *CHANGE. Alla fine, l'utente dovrebbe analizzare le applicazioni e fornire solo il livello di autorizzazione minimo necessario all'applicazione. Tuttavia, durante il periodo di transizione, adottando l'autorizzazione *ALL , si evitano malfunzionamenti delle applicazioni causati da un'insufficiente autorizzazione.

__ Passo 7. Limitare l'autorizzazione ai programmi nella libreria immettendo quanto segue:

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

__ Passo 8. Assegnare al profilo OEOWNER l'autorizzazione per i programmi nella libreria ordini immettendo quanto segue:

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

__ Passo 9. Assegnare agli utenti identificati nel passo 1 l'autorizzazione al programma menu immettendo quanto segue per ogni utente:

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
    USER(nome-profilo-utente) AUT(*USE)
```

Una volta completati questi passi, tutti gli utenti non esplicitamente esclusi saranno in grado di accedere (ma non di modificare) i file nella libreria ORDERLIB. Utenti che hanno l'autorizzazione al programma OEMENU saranno in grado di utilizzare i programmi che si trovano sul menu per aggiornare i file nella libreria ORDERLIB. Solo utenti con l'autorizzazione al programma OEMENU saranno ora in grado di modificare i file in questa libreria. Una combinazione di sicurezza oggetto e controllo accesso menu protegge i file.

Quando si completano passi analoghi per tutte le librerie che contengono dati utente, si è creato uno schema semplice per il controllo degli aggiornamenti al database. Questo metodo impedisce agli utenti di sistema di aggiornare i file di database tranne quando utilizzano i menu ed i programmi approvati. Nello stesso tempo, si sono resi disponibili i file di database per la visualizzazione, l'analisi e la copia da parte di utenti con strumenti di supporto alla decisione o con collegamenti da un altro sistema o da un PC.

Suggerimento sull'autorizzazione all'oggetto: quando il proprio sistema fa parte di una rete, l'autorizzazione *USE può fornire un livello di autorizzazione superiore al previsto. Ad esempio, con FTP, è possibile effettuare una copia di un file in un altro sistema (incluso un PC) se si dispone dell'autorizzazione *USE al file.

Utilizzo della sicurezza libreria come complemento alla sicurezza menu

Per accedere ad un oggetto in una libreria, è necessario disporre dell'autorizzazione sia all'oggetto che alla libreria. La maggior parte delle operazioni richiede l'autorizzazione *EXECUTE o l'autorizzazione *USE alla libreria.

In base alla situazione, è possibile essere in grado di utilizzare l'autorizzazione alla libreria come semplice mezzo per la protezione degli oggetti. Ad esempio, supponiamo che per l'esempio del menu Immissione ordine, chiunque disponga dell'autorizzazione al menu Immissione ordine possa utilizzare tutti i programmi nella libreria ORDERPGM. Piuttosto che proteggere singoli programmi, è possibile impostare l'autorizzazione pubblica alla libreria ORDERPGM su *EXCLUDE. E' possibile quindi garantire a profili utente specifici l'autorizzazione *USE alla libreria, che consentirà loro di utilizzare i programmi nella libreria. (Questo presuppone che l'autorizzazione pubblica ai programmi sia impostata su *USE o su un livello maggiore.)

L'autorizzazione alla libreria può rappresentare un modo semplice, efficiente di gestire l'autorizzazione all'oggetto. Tuttavia, è necessario accertarsi di avere una buona conoscenza del contenuto delle librerie che si stanno proteggendo in modo da non fornire accesso indesiderato agli oggetti.

Configurazione della proprietà dell'oggetto

La proprietà degli oggetti sul sistema è una parte importante del proprio schema di autorizzazione all'oggetto. Per impostazione predefinita, il proprietario di un oggetto dispone dell'autorizzazione *ALL all'oggetto. Il Capitolo 5 nel manuale *Riferimenti alla sicurezza iSeries* fornisce suggerimenti ed esempi per la pianificazione della proprietà dell'oggetto. Di seguito sono riportati alcuni suggerimenti:

- In generale, i profili di gruppo non dovrebbero possedere oggetti. Se un profilo di gruppo possiede un oggetto, tutti i membri del gruppo dispongono dell'autorizzazione *ALL all'oggetto a meno che il membro del gruppo non sia esplicitamente escluso.
- Se si utilizza l'autorizzazione adottata, considerare se i profili utente che possiedono i programmi dovrebbero possedere anche gli oggetti applicazione, come ad esempio i file. Si potrebbe non volere che gli utenti che eseguono i programmi che adottano l'autorizzazione abbiano l'autorizzazione *ALL ai file.

Se si sta utilizzando iSeries Navigator, questo può essere realizzato completando le modifiche tramite la funzione **normative** di sicurezza. Per ulteriori informazioni, fare riferimento all'iSeries Information Center (consultare "Requisiti necessari e informazioni correlate" a pagina xii per i dettagli).

Autorizzazione all'oggetto per comandi e programmi di sistema

I seguenti sono alcuni suggerimenti da applicare quando si limita l'autorizzazione ad oggetti forniti da IBM:

- Quando si ha più di una lingua nazionale impostata sul sistema, il sistema a sua volta ha più di una libreria di sistema (QSYS). Il sistema ha una libreria QSYSxxxx per ogni lingua nazionale presente sul sistema. Se si sta utilizzando l'autorizzazione all'oggetto per controllare l'accesso ai comandi di sistema, ricordarsi di proteggere il comando nella libreria QSYS ed in ogni libreria QSYSxxx nel sistema.
- La libreria System/38 a volte fornisce un comando con funzione equivalente ai comandi che si desidera limitare. Assicurarsi di limitare il comando equivalente nella libreria QSYS38.
- Se si dispone dell'ambiente System/36, è possibile che sia necessario limitare ulteriori programmi. Ad esempio, il programma QY2FTML fornisce il trasferimento file System/36.

Controllo funzioni di sicurezza

Questo capitolo descrive le tecniche per il controllo dell'efficacia della sicurezza sul proprio sistema. Gli utenti controllano la sicurezza del proprio sistema per diverse ragioni:

- Per valutare l'eventuale completezza del piano di sicurezza.
- Per accertarsi che i controlli di sicurezza pianificati siano nell'ubicazione desiderata e funzionino. Questo tipo di controllo viene di solito eseguito dal responsabile della riservatezza come parte della gestione quotidiana della riservatezza. Viene anche eseguito, talvolta in modo più approfondito, come parte di una revisione periodica della sicurezza da parte di revisori interni o esterni.
- Per accertarsi che la sicurezza del sistema si mantenga al passo con le modifiche all'ambiente di sistema. Alcuni esempi di modifiche che interessano la sicurezza sono:

  - Nuovi oggetti creati dagli utenti del sistema
  - Nuovi utenti ammessi nel sistema
  - Modifica della proprietà dell'oggetto (autorizzazione non adattata)
  - Modifica delle responsabilità (gruppo utenti modificato)
  - Autorizzazione temporanea (non revocata in tempo)
  - Nuovi prodotti installati
- Per prepararsi ad un futuro evento, come ad esempio l'installazione di una nuova applicazione, passando ad un livello di sicurezza superiore o configurando una rete di comunicazioni.

Le tecniche descritte in questo capitolo sono appropriate per tutte queste situazioni. Quali elementi sottoporre a controllo e con quale frequenza dipende dalla dimensione e dalle esigenze di sicurezza della propria organizzazione. Lo scopo di questo capitolo è quello di illustrare quali informazioni sono disponibili, come ottenerle e perché sono necessarie, piuttosto che fornire direttive per la frequenza dei controlli.

Queste informazioni sono suddivise in tre parti:

- Un elenco di controllo delle voci di sicurezza che è possibile pianificare e controllare.
- Informazioni sulla impostazione e l'utilizzo del giornale di controllo fornito dal sistema.
- Altre tecniche disponibili per raccogliere informazioni relative alla sicurezza nel sistema.

Il controllo della sicurezza coinvolge l'utilizzo di comandi sul sistema iSeries e l'accesso alle informazioni della registrazione e del giornale nel sistema. E' possibile che si voglia creare un profilo speciale ad uso di chi esegue un controllo della sicurezza del proprio sistema. Il profilo di revisore avrà bisogno dell'autorizzazione speciale *AUDIT per essere in grado di modificare le caratteristiche del controllo del sistema. Alcune delle attività di controllo suggerite in questo capitolo richiedono un profilo utente con l'autorizzazione speciale *ALLOBJ e *SECADM. Assicurarsi di impostare la parola d'ordine per il profilo di revisore su *NONE una volta terminato il periodo di controllo.

Per ulteriori dettagli sul controllo della sicurezza consultare il Capitolo 9, del manuale *Riferimenti alla sicurezza*.

Analisi dei profili utente

E' possibile visualizzare o stampare un elenco completo di tutti gli utenti sul sistema con il comando Visualizzazione utenti autorizzati (DSPAUTUSR). E' possibile ordinare in sequenza l'elenco per nome profilo o nome profilo gruppo. Di seguito è riportato un esempio della sequenza del profilo gruppo.

```
                        Visualizzazione utenti autorizzati

Profilo    Profilo   Ultima modifica   Nessuna parola
gruppo      utente    parola d'ordine     d'ordine     Testo
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      Vendite e MKTG
            DPTWH       08/13/0x            X        Magazzino
            RICHARDS    09/05/0x                     Janet Richards
            SMITHJ      09/18/0x                     John Smith
```

Stampa dei profili utente selezionati

E' possibile utilizzare il comando Visualizzazione profilo utente (DSPUSRPRF) per creare un file di emissione che è possibile elaborare utilizzando uno strumento di query.

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

E' possibile utilizzare uno strumento di query per creare numerosi prospetti di analisi del file di emissione, come ad esempio:

- Un elenco di tutti gli utenti che dispongono di entrambe le autorizzazioni speciali *ALLOBJ e *SPLCTL.
- Un elenco di tutti gli utenti ordinati in sequenza per campo profilo utente, come ad esempio un programma iniziale o una classe utente.

E' possibile creare dei programmi di query per produrre differenti prospetti dal file di emissione. Ad esempio:

- Elencare tutti i profili utente che dispongono di autorizzazioni speciali selezionando i record in cui il campo UPSPAU non è uguale a *NONE.
- Elencare tutti gli utenti a cui è consentito immettere i comandi selezionando i record dove il campo *Possibilità limitate* (denominato UPLTCP nel file di emissione database del modello) è uguale a *NO o *PARTIAL.
- Elencare tutti gli utenti che dispongono di un menu iniziale o di un programma iniziale particolari.
- Elencare gli utenti inattivi basandosi sulla data del campo ultimo collegamento.

Esame di profili utente di ampie dimensioni

I profili utente con numerose autorizzazioni, che sembrano distribuiti casualmente sulla maggior parte del sistema, possono riflettere una mancanza di pianificazione della sicurezza. Di seguito è riportato un metodo per individuare i profili utente di ampie dimensioni e per valutarli:

1. Utilizzare il comando Visualizzazione descrizione oggetto (DSPOBJD) per creare un file di emissione contenente informazioni su tutti i profili utente sul sistema:

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

2. Creare un programma di query per elencare il nome e la dimensione di ciascun profilo utente, in sequenza discendente per dimensione.
3. Stampare informazioni dettagliate sui profili utente di maggiori dimensioni e valutare l'adeguatezza delle autorizzazioni e degli oggetti di proprietà se sono appropriati:

   ```
   DSPUSRPRF USRPRF(nome-profilo-utente) +
             TYPE(*OBJAUT) OUTPUT(*PRINT)
   DSPUSRPRF USRPRF(nome-profilo-utente) +
             TYPE(*OBJOWN) OUTPUT(*PRINT)
   ```

   Alcuni profili utente forniti da IBM sono di dimensioni molto ampie a causa del numero di oggetti che possiedono. Normalmente non è necessario elencarli e analizzarli. Tuttavia, sarebbe opportuno verificare i programmi che adottano l'autorizzazione dei profili utente forniti da IBM che dispongono dell'autorizzazione speciale *ALLOBJ, come QSECOFR e QSYS.

Per ulteriori dettagli sul controllo sicurezza, consultare il Capitolo 9, del manuale *Riferimenti alla sicurezza*.

Analisi delle autorizzazioni oggetto

E' possibile utilizzare il seguente metodo per stabilire chi dispone dell'autorizzazione alle librerie sul sistema:

1. Utilizzare il comando DSPOBJD per elencare tutte le librerie sul sistema:

   ```
   DSPOBJD OBJ(QSYS/*ALL) OBJTYPE(*LIB) ASPDEV(*ALLAVL) OUTPUT(*PRINT)
   ```

   Nota: le librerie negli ASP indipendenti che non si trovano nello stato AVAILABLE non verranno visualizzate da tale comando.
2. Utilizzare il comando Visualizzazione autorizzazione oggetto (DSPOBJAUT) per elencare le autorizzazioni a una libreria specifica:

   ```
   DSPOBJAUT OBJ(QSYS/nome-libreria) OBJTYPE(*LIB) +
             ASPDEV(nome-unità-asp) OUTPUT(*PRINT)
   ```
3. Utilizzare il comando Visualizzazione libreria (DSPLIB) per elencare gli oggetti nella libreria:

   ```
   DSPLIB LIB(QSYS/nome-libreria) ASPDEV(nome-unità-asp) OUTPUT(*PRINT)
   ```

Utilizzando questi prospetti, è possibile stabilire gli elementi contenuti in una libreria e chi ha accesso alla libreria. Se necessario, è possibile utilizzare il comando DSPOBJAUT per visualizzare l'autorizzazione per gli oggetti selezionati anche nella libreria.

Controllo oggetti modificati

E' possibile utilizzare il comando Controllo integrità oggetto (CHKOBJITG) per ricercare gli oggetti che sono stati modificati. Un oggetto modificato è normalmente un'indicazione che qualcuno sta tentando di manomettere con il sistema. E' possibile che si desideri eseguire questo comando dopo che qualcuno ha:

- ripristinato i programmi sul sistema
- utilizzato DST (dedicated service tools)

Quando si esegue il comando, il sistema crea un file di database contenente le informazioni su qualsiasi potenziale problema di integrità. E' possibile controllare gli oggetti di proprietà di un profilo, di numerosi profili differenti o di tutti i profili. E' possibile ricercare gli oggetti il cui dominio è stato modificato. E' inoltre possibile calcolare nuovamente i valori di convalida programma per ricercare gli oggetti di tipo *PGM, *SRVPGM, *MODULE e *SQLPKG che sono stati modificati.

L'esecuzione del programma CHKOBJITG richiede l'autorizzazione speciale *AUDIT. E' possibile che occorra molto tempo per l'esecuzione del comando a causa delle scansioni e dei calcoli che esegue. Sarebbe opportuno eseguirlo quando il sistema non è occupato.

Nota: i profili che possiedono molti oggetti con molte autorizzazioni private possono assumere dimensioni molto ampie. La dimensione di un profilo proprietario influenza le prestazioni durante la visualizzazione e la gestione dell'autorizzazione agli oggetti di proprietà e durante il salvataggio o il ripristino dei profili. E' possibile inoltre che vengano influenzate anche le operazioni del sistema. Per impedire impatti sulle prestazioni o sulle operazioni del sistema, distribuire la proprietà degli oggetti a più profili. **Non assegnare tutti (o quasi tutti) gli oggetti a un solo profilo proprietario.**

Analisi dei programmi che adottano un'autorizzazione

I programmi che adottano l'autorizzazione di un utente con autorizzazione speciale *ALLOBJ rappresentano un rischio per la sicurezza. E' possibile utilizzare il seguente metodo per trovare ed esaminare tali programmi:

1. Per ciascun utente con autorizzazione speciale *ALLOBJ, utilizzare il comando Visualizzazione adozione programma (DSPPGMADP) per elencare i programmi che adottano tale autorizzazione utente:

   ```
   DSPPGMADP USRPRF(nome-profilo-utente) +
   OUTPUT(*PRINT)
   ```

   Nota: l'argomento "Stampa dei profili utente selezionati" a pagina 54 visualizza in che modo elencare gli utenti con autorizzazione *ALLOBJ.
2. Utilizzare il comando DSPOBJAUT per stabilire chi è autorizzato a utilizzare ciascun programma di adozione e qual è l'autorizzazione pubblica per il programma:

   ```
   DSPOBJAUT OBJ(nome-libreria/nome-programma) +
             OBJTYPE(*PGM) ASPDEV(nome-libreria/nome-programma) +
   OUTPUT(*PRINT)
   ```
3. Esaminare il codice di origine e la descrizione programma per valutare:
   - Se all'utente del programma è impedito lo sfruttamento eccessivo di una funzione, come l'utilizzo di una riga comandi durante l'esecuzione nel profilo adottato.
   - Se il programma adotta il livello di autorizzazione minimo necessario per la funzione desiderata. Le applicazioni che utilizzano un errore del programma possono essere progettate utilizzando lo stesso profilo utente per oggetti e programmi. Quando viene adottata l'autorizzazione del proprietario di un programma, l'utente dispone dell'autorizzazione *ALL agli oggetti dell'applicazione. In molti casi, il profilo del proprietario non richiede alcuna autorizzazione speciale.
4. Verificare quando il programma è stato modificato l'ultima volta, utilizzando il comando DSPOBJD:

   ```
   DSPOBJD OBJ(nome-libreria/nome-programma) +
           OBJTYPE(*PGM) ASPDEV(nome-libreria/nome-programma) +
           DETAIL(*FULL)
   ```

Gestione del giornale di controllo e dei ricevitori di giornale

Il giornale di controllo, QSYS/QAUDJRN, è pensato esclusivamente per il controllo della sicurezza. Sarebbe opportuno non inserire gli oggetti nel giornale di controllo. Sarebbe opportuno che il controllo sincronizzazione non utilizzasse il giornale di

controllo. Sarebbe opportuno non inviare le voci utente a tale giornale utilizzando il comando Invio voce di giornale (SNDJRNE) o l'API Invio voce di giornale (QJOSJRNE).

Viene utilizzata una speciale protezione vincoli per assicurare che il sistema possa scrivere voci di controllo nel giornale di controllo. Quando il controllo è attivo (il valore di sistema QAUDCTL non è *NONE), il lavoro arbitro sistema (QSYSARB) pone un vincolo sul giornale QSYS/QAUDJRN. Non è possibile eseguire alcune operazioni sul giornale di controllo quando il controllo è attivo, come ad esempio:

- comando DLTJRN
- comando ENDJRNxxx
- comando APYJRNCHG
- comando RMVJRNCHG
- comando DMPOBJ o DMPSYSOBJ
- Spostamento del giornale
- Ripristino del giornale
- Operazioni che gestiscono l'autorizzazione, come ad esempio il comando GRTOBJAUT
- comando WRKJRN

Le informazioni registrate nelle voci del giornale di sicurezza sono descritte nel manuale *Riferimenti alla sicurezza*. Tutte le voci di sicurezza nel giornale di controllo hanno un codice giornale T. Oltre alle voci di sicurezza, il giornale QAUDJRN contiene anche le voci del sistema. Tali voci hanno un codice giornale J, correlato all'IPL (initial program load) e alle operazioni generali eseguite sui ricevitori del giornale (ad esempio, il salvataggio del ricevitore).

Se il giornale o il relativo ricevitore corrente viene danneggiato in modo che non sia possibile inserirvi le voci di controllo, il valore di sistema QAUDENDACN stabilisce quale azione è necessario che il sistema intraprenda. Il ripristino da un ricevitore di giornale o da un giornale danneggiato è lo stesso per altri giornali.

E' possibile che si desideri che il sistema gestisca la modifica dei ricevitori di giornale. Specificare MNGRCV(*SYSTEM) quando si crea il giornale QAUDJRN o modificare il giornale su tale valore. Se si specifica MNGRCV(*SYSTEM), il sistema scollega automaticamente il ricevitore quando raggiunge la relativa dimensione soglia e crea e collega un nuovo ricevitore di giornale. Ciò viene denominato **Modifica di sistema-Gestione del giornale**. Consultare iSeries Information Center—>Gestione sistemi–> Gestione giornale–>Gestione giornale locale–>Gestione giornali per ulteriori informazioni. Consultare "Requisiti necessari e informazioni correlate" a pagina xii per informazioni sull'accesso all'iSeries Information Center.

Capitolo 6. Gestione autorizzazione

E' disponibile una serie di documenti sulla sicurezza per aiutare l'utente a tenere traccia della modalità di configurazione della sicurezza sul sistema. Inizialmente, quando si utilizza questa documentazione, è possibile stampare l'intero contenuto (autorizzazione per tutti i file o per tutti i programmi, ad esempio).

Una volta creata la propria base di informazioni, è possibile utilizzare le versioni modificate della documentazione regolarmente. Le versioni modificate consentono di individuare modifiche rilevanti alla sicurezza nel sistema che richiedono attenzione. Ad esempio, è possibile utilizzare il documento che contiene l'autorizzazione pubblica per i file ogni settimana. Si può richiedere solo la versione modificata del documento. Questa conterrà sia i nuovi file sul sistema disponibili per chiunque che i file esistenti la cui autorizzazione pubblica è stata modificata rispetto all'ultimo documento.

Sono disponibili due menu per eseguire gli strumenti di sicurezza:

- Utilizzare il menu SECTOOLS per l'esecuzione interattiva dei programmi.
- Utilizzare il menu SECBATCH per l'esecuzione dei programmi in batch. Il menu SECBATCH è composto da due parti: una per l'inoltro immediato di lavori alla coda lavori e l'altra per il collocamento dei lavori nel programma di pianificazione lavoro.

Se si sta utilizzando iSeries Navigator, seguire questi passi per l'esecuzione degli strumenti di sicurezza:

1. In iSeries Navigator, espandere Server—>**Sicurezza**.
2. Fare clic con il tastino destro del mouse su **Normative** e selezionare **Esplora** per visualizzare un elenco di normative che è possibile creare e gestire.

Monitoraggio dell'autorizzazione pubblica agli oggetti

Per ragioni sia di semplicità che di prestazioni, la maggior parte dei sistemi sono configurati in modo che la maggior parte degli oggetti sia disponibile per la maggior parte degli utenti. Agli utenti viene esplicitamente vietato l'accesso a certi oggetti confidenziali e sensibili alla sicurezza piuttosto che dover essere esplicitamente autorizzati ad utilizzare ogni oggetto. Pochi sistemi con elevati requisiti di sicurezza seguono l'approccio opposto ed autorizzano gli oggetti sulla base di una necessità di conoscerli. In quei sistemi, la maggior parte degli oggetti vengono creati con l'autorizzazione pubblica impostata su *EXCLUDE.

iSeries è un sistema basato sugli oggetti con molti tipi differenti di oggetti. La maggior parte dei tipi di oggetti non contiene informazioni delicate né esegue funzioni rilevanti per la sicurezza. Come responsabile della sicurezza su un sistema iSeries con esigenze di sicurezza ordinarie, si desidera probabilmente concentrare l'attenzione su oggetti che richiedono protezione, come ad esempio file di database e programmi. Per altri tipi di oggetto, è possibile semplicemente impostare l'autorizzazione pubblica sufficiente per le applicazioni, che per la maggior parte dei tipi di oggetto è l'autorizzazione *USE.

E' possibile utilizzare il comando Stampa oggetti autorizzazione pubblica (PRTPUBAUT) per stampare informazioni sugli oggetti a cui gli utenti pubblici possono accedere. (Un **utente pubblico** è chiunque dotato di autorizzazione per il

© Copyright IBM Corp. 1996, 2004

collegamento non sia esplicitamente autorizzato ad un oggetto.) Quando si utilizza il comando PRTPUBAUT, è possibile specificare i tipi di oggetto e le librerie o indirizzari, che si desidera esaminare. Sono disponibili opzioni nei menu SECBATCH e SECTOOLS per stampare il Documento degli oggetti con autorizzazione pubblica per i tipi di oggetto che più comunemente hanno implicazioni di sicurezza. E' possibile stampare la versione modificata di questo documento regolarmente per visualizzare gli oggetti che potrebbero richiedere attenzione.

Gestione dell'autorizzazione per nuovi oggetti

OS/400 fornisce funzioni che guidano l'utente nella gestione dell'autorizzazione e della proprietà di nuovi oggetti nel sistema. Quando un utente crea un nuovo oggetto, il sistema stabilisce quanto segue:

- Chi sarà il proprietario dell'oggetto
- Qual'è l'autorizzazione pubblica per l'oggetto
- Se l'oggetto dispone di qualche autorizzazione privata
- Dove inserire l'oggetto (quale libreria o indirizzario)
- Se l'accesso all'oggetto sarà controllato

Il sistema utilizza valori di sistema, parametri libreria e parametri profilo utente per decidere su questi punti. La sezione "Assegnazione autorizzazione e proprietà a nuovi oggetti" nel capitolo 5 del manuale *Riferimenti alla sicurezza iSeries* fornisce diversi esempi delle opzioni disponibili.

E' possibile utilizzare il comando PRTUSRPRF per stampare i parametri profilo utente che interessano la proprietà e l'autorizzazione per i nuovi oggetti. La Figura 5 a pagina 65 illustra un esempio di questo documento.

Monitoraggio elenchi di autorizzazioni

E' possibile raggruppare oggetti con requisiti di sicurezza simili utilizzando un elenco di autorizzazioni. Concettualmente, un elenco di autorizzazioni contiene un elenco di utenti e le autorizzazioni di cui dispongono per gli oggetti protetti dall'elenco. Gli elenchi di autorizzazioni forniscono un modo efficiente di gestire l'autorizzazione ad oggetti simili nel sistema. Tuttavia, in alcuni casi, rendono difficile tenere traccia delle autorizzazioni agli oggetti.

E' possibile utilizzare il comando Stampa autorizzazioni private (PRTPVTAUT) per stampare informazioni circa gli utenti con autorizzazioni contenute nell'elenco autorizzazioni. La Figura 3 illustra un esempio del documento.

```
                          Autorizzazioni private (Documento completo)
Elenco
Autorizzazioni           Gruppo                          Elenco  ----------Oggetto----------  ------------Dati------------
SYSTEM4       Propriet.  primario     Utente     Autorizz.  Gst.  Oper. Gst. Esist. Modif. Rif.   Lett. Agg. Aggior. Canc. Esec.
LIST1         QSECOFR    *NONE       *PUBLIC    *EXCLUDE
LIST2         BUDNIKR    *NONE       BUDNIKR    *ALL        X     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      X
                                     GROUP1     *ALL              X    X     X      X     X    X     X    X    X      X
*PUBLIC                  *EXCLUDE
```

Figura 3. Documento relativo agli utenti con autorizzazione privata per gli elenchi di autorizzazioni

Questo documento riporta le stesse informazioni che si visualizzano nel pannello Modifica elenco autorizzazioni (EDTAUTL). Il vantaggio del documento è che fornisce informazioni sugli elenchi di autorizzazioni in un'unica ubicazione. Se si

sta configurando la sicurezza per un nuovo gruppo di oggetti, ad esempio, è possibile effettuare una veloce scansione del documento per visualizzare se un elenco di autorizzazioni esistente soddisfa le proprie esigenze per quegli oggetti.

E' possibile stampare una versione modificata del documento per visualizzare i nuovi elenchi di autorizzazioni con gli utenti che ne dispongono modificati rispetto all'ultimo documento stampato. L'utente dispone anche dell'opzione per stampare un elenco degli oggetti che sono protetti da ciascun elenco di autorizzazioni. La Figura 4 illustra un esempio del documento per un elenco autorizzazioni:

```
                    Visualizzazione oggetti elenco autorizzazioni
Elenco autorizzazioni . . . . . :   CUSTAUTL
Libreria  . . . . . :       QSYS
Proprietario . . . . . :  AROWNER
Gruppo primario . . . . . :      *NONE

                                                        Gruppo
Oggetto        Libreria        Tipo        Proprietario   primario          Testo
CUSTMAS        CUSTLIB        *FILE        AROWNER        *NONE
CUSTORD        CUSTORD        *FILE        OEOWNER        *NONE
```

Figura 4. Visualizzazione oggetti elenco autorizzazioni

E' possibile utilizzare questo documento, ad esempio, per cogliere l'effetto dell'aggiunta di un nuovo utente ad un elenco autorizzazioni (quali autorizzazioni riceverà tale utente).

Utilizzo degli elenchi di autorizzazioni

iSeries Navigator fornisce funzioni di sicurezza progettate per assistere l'utente nello sviluppo di un piano e di una normativa di sicurezza e configura il sistema per soddisfare i bisogni della propria società. Una delle funzioni disponibili è rappresentata dall'uso dell'elenco di autorizzazioni.

Gli elenchi di autorizzazioni hanno le seguenti funzioni.
- Un elenco di autorizzazioni raggruppa oggetti con requisiti di sicurezza simili.
- Un elenco di autorizzazioni concettualmente contiene un elenco di utenti e gruppi e le autorizzazioni di cui ognuno dispone per gli oggetti protetti dall'elenco.
- Ogni utente e gruppo può avere un'autorizzazione differente alla serie di oggetti che l'elenco protegge.
- L'autorizzazione può essere fornita per mezzo dell'elenco, piuttosto che a singoli utenti e gruppi.

Attività che possono essere eseguite tramite gli elenchi di autorizzazioni includono le seguenti.
- Creare un elenco di autorizzazioni
- Modificare un elenco di autorizzazioni.
- Aggiungere utenti e gruppi.
- Modificare i permessi utente.
- Visualizzare oggetti protetti.

Per utilizzare questa funzione, attenersi alle seguenti istruzioni:
1. Da iSeries Navigator, espandere Server—>Sicurezza. Si visualizzerà **Elenchi autorizzazioni** e **Normative**.

2. Fare clic con il tastino destro del mouse su **Elenchi autorizzazioni** e selezionare **Nuovo elenco autorizzazioni**. Il **Nuovo elenco autorizzazioni** consente di effettuare le seguenti operazioni
   - **Utilizzo:** consente l'accesso agli attributi dell'oggetto e all'utilizzo dell'oggetto. Gli utenti pubblici possono visualizzare, ma non modificare gli oggetti.
   - **Modifica:** consente la modifica del contenuto dell'oggetto (con alcune eccezioni).
   - **Tutto:** consente tutte le operazioni sull'oggetto, tranne quelle riservate al proprietario. L'utente o il gruppo può controllare l'esistenza dell'oggetto, specificare la sicurezza per l'oggetto, modificare l'oggetto ed eseguire funzioni di base sull'oggetto. L'utente o il gruppo possono anche modificare la proprietà dell'oggetto.
   - **Esclusione:** tutte le operazioni sull'oggetto sono proibite. Non è consentito l'accesso né le operazioni per quanto riguarda l'oggetto agli utenti e gruppi che dispongono di questo permesso. Specifica che agli utenti pubblici non è consentito l'utilizzo dell'oggetto.

Quando si gestiscono elenchi di autorizzazioni sembrerà opportuno concedere permessi sia per gli oggetti che per i dati. I permessi relativi agli oggetti che è possibile selezionare sono elencati di seguito:
- **Operativo:** fornisce il permesso di esaminare la descrizione di un oggetto e di utilizzare l'oggetto come stabilito dal permesso relativo ai dati di cui l'utente o il gruppo dispone per l'oggetto.
- **Gestione:** fornisce il permesso di specificare la sicurezza per l'oggetto, spostare o ridenominare l'oggetto e aggiungere membri ai file di database.
- **Esistenza:** fornisce il permesso di controllare l'esistenza e la proprietà dell'oggetto. L'utente o il gruppo possono cancellare l'oggetto, liberare la memoria dell'oggetto, eseguire operazioni di salvataggio e ripristino per l'oggetto, e trasferire la proprietà dell'oggetto. Se un utente o un gruppo ha uno speciale permesso per il salvataggio, non ha bisogno del permesso per l'esistenza dell'oggetto.
- **Modifica** (utilizzato solo per file di database e pacchetti SQL): fornisce il permesso necessario per modificare gli attributi di un oggetto. Se l'utente o il gruppo dispone di questo permesso su un file di database, l'utente o il gruppo può aggiungere e rimuovere trigger, aggiungere e rimuovere limiti univoci e di riferimento e modificare gli attributi del file di database. Se l'utente o il gruppo ha questo permesso su un pacchetto SQL, può modificare gli attributi del pacchetto in questione. Questo permesso viene attualmente utilizzato solo per i file di database ed i pacchetti SQL.
- **Riferimento** (utilizzato solo per file di database e pacchetti SQL): fornisce il permesso necessario perché sia possibile il riferimento ad un oggetto da parte di un altro oggetto, operazioni simili su tale oggetto potrebbero essere limitate dall'altro oggetto. Se l'utente o il gruppo dispone di questo permesso su un file fisico, può aggiungere limiti di riferimento in cui il file fisico è il principale. Questo permesso attualmente è utilizzato solo per i file di database.

I permessi relativi ai dati che è possibile selezionare sono elencati di seguito:
- **Lettura:** fornisce il permesso necessario a richiamare e visualizzare il contenuto dell'oggetto, come ad esempio la visualizzazione dei record in un file.
- **Aggiunta:** fornisce il permesso di aggiungere voci ad un oggetto, come ad esempio l'aggiunta di messaggi ad una coda messaggi o l'aggiunta di record ad un file.
- **Aggiornamento:** fornisce il permesso di modificare le voci in un oggetto, come ad esempio modificare i record in un file.

- **Cancellazione:** fornisce il permesso di eliminare voci da un oggetto, come ad esempio l'eliminazione di messaggi da una coda messaggi o la cancellazione di record da un file.
- **Esecuzione:** fornisce il permesso necessario ad eseguire un programma, un programma di servizio o un pacchetto SQL. L'utente può anche ubicare un oggetto in una libreria o in un indirizzario.

Per ulteriori informazioni su ogni processo in fase di creazione o di modifica dei propri elenchi di autorizzazioni, utilizzare l'aiuto in linea disponibile in iSeries Navigator.

Accesso alle normative in iSeries Navigator

E' possibile utilizzare iSeries Navigator per visualizzare e gestire normative per il proprio server iSeries. iSeries Navigator ha cinque aree relative alla normativa:

- **Normativa di controllo**
  Questa consente all'utente di impostare il monitoraggio per specifiche azioni ed accedere a specifiche risorse nel sistema.
- **Normativa di sicurezza**
  Questa consente all'utente di specificare il livello di sicurezza ed ulteriori opzioni relative alla sicurezza del sistema.
- **Normativa della parola d'ordine**
  Questa consente all'utente di specificare il livello della parola d'ordine per il sistema.
- **Normativa di ripristino**
  Questa consente di specificare come certi oggetti vengono ripristinati nel sistema.
- **Normativa di collegamento**
  Questa consente di specificare come un utente può collegarsi al sistema.

Per visualizzare o modificare le normative con iSeries Navigator, seguire questi passi:

1. Da iSeries Navigator, espandere Server—>**Sicurezza**.
2. Fare clic con il tastino destro del mouse su **Normative** e selezionare **Esplora** per visualizzare un elenco di normative che è possibile creare e gestire. Consultare l'aiuto iSeries Navigator per informazioni specifiche su queste normative.

Monitoraggio dell'autorizzazione privata agli oggetti

Opzioni menu SECBATCH:
12 *per l'inoltro immediato* **41** *per utilizzare il programma di pianificazione lavoro*

E' possibile utilizzare il comando Stampa autorizzazioni private (PRTPVTAUT) per stampare un elenco di tutte le autorizzazioni private per gli oggetti di un tipo specificato in una data libreria.

E' possibile utilizzare questo documento per facilitare l'individuazione di nuove autorizzazioni agli oggetti. Può anche essere di aiuto per impedire che lo schema di autorizzazioni private divenga contorto e ingestibile.

Monitoraggio dell'accesso alle code di emissione e di lavori

Qualche volta un responsabile della sicurezza compie un grande sforzo per proteggere l'accesso ai file e poi non si preoccupa di quello che accade quando il contenuto di un file viene stampato. I server iSeries forniscono funzioni perché l'utente possa proteggere code di emissione e code lavori particolarmente significative. Si protegge una coda di emissione in modo che utenti non autorizzati non possano, ad esempio, visualizzare o copiare file di spool riservati che sono in attesa di stampa. Si proteggono le code lavori in modo che un utente non autorizzato non possa reindirizzare un lavoro riservato ad una coda di emissione non riservata o annullare interamente il lavoro.

Opzioni menu SECBATCH:
24 per l'inoltro immediato 63 *per utilizzare il programma di pianificazione lavoro*

Sicurezza e pianificazione di base del sistema nell'Information Center ed il manuale *Riferimenti alla sicurezza iSeries* descrivono come proteggere le code di emissione e le code lavori.

E' possibile utilizzare il comando Stampa autorizzazione coda (PRTQAUT) per stampare le impostazioni di sicurezza per le code lavori e le code di emissione nel sistema. E' possibile quindi valutare lavori di stampa che stampano informazioni riservate ed assicurarsi che vadano alle code di emissione e di lavori protette.

Per code di emissione e code lavori che si ritengono sensibili alla sicurezza, è possibile confrontare le proprie impostazioni di sicurezza rispetto alle informazioni nell'Appendice D del manuale *Riferimenti alla sicurezza iSeries*. Le tabelle nell'Appendice D indicano quali impostazioni sono necessarie per eseguire differenti funzioni della coda di emissione e della coda lavori.

Monitoraggio autorizzazioni speciali

Quando utenti sul proprio sistema dispongono di autorizzazioni speciali non necessarie, gli sforzi per sviluppare un valido schema di autorizzazioni all'oggetto potrebbero essere vani. L'autorizzazione all'oggetto è priva di senso quando un profilo utente dispone dell'autorizzazione speciale *ALLOBJ. Un utente con l'autorizzazione speciale *SPLCTL può visualizzare qualsiasi file di spool presente sul sistema, indipendentemente dagli sforzi compiuti per proteggere le code di emissione. Un utente con l'autorizzazione speciale *JOBCTL può influenzare le operazioni di sistema e reindirizzare i lavori. Un utente con l'autorizzazione speciale *SERVICE può essere in grado di utilizzare i programmi di manutenzione per accedere ai dati senza passare attraverso il sistema operativo.

Opzioni menu SECBATCH:
29 per l'inoltro immediato 68 *per utilizzare il programma di pianificazione lavoro*

E' possibile utilizzare il comando Stampa profilo utente (PRTUSRPRF) per stampare informazioni sulle autorizzazioni speciali e sulle classi utente per i profili utente nel sistema. Quando si utilizza il documento, si hanno diverse opzioni:
- Tutti i profili utente
- Profili utente con specifiche autorizzazioni speciali
- Profili utente con specifiche classi utente
- Profili utente con mancata corrispondenza tra classe utente ed autorizzazioni speciali.

La Figura 5 mostra un esempio di documento che contiene le autorizzazioni speciali per tutti i profili utente:

```
                                    Informazioni profilo utente
  Tipo documento  . . . . . . . . . :   *AUTINFO
  Selezione per   . . . . . . . . . :   *SPCAUT
  Autorizzazioni speciali   . . . . :   *ALL
                   -------------Autorizzazioni speciali-------------
                                *IO                                                    Gruppo
Profilo   Profili   *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Classe             Autorizz.   Tipo       Possibilità
utente    gruppo     OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  utente     Propriet.  gruppo     autorizz.  limitate
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
```

Figura 5. Documento di informazioni sull'utente: Esempio 1

Oltre alle autorizzazioni speciali, il documento indica quanto segue:
- Se il profilo utente ha capacità limitata.
- Se l'utente o il gruppo dell'utente possiede nuovi oggetti che l'utente crea.
- Quale autorizzazione riceve automaticamente il gruppo dell'utente per i nuovi oggetti che l'utente crea.

La Figura 6 mostra un esempio del documento relativo alla mancata corrispondenza tra autorizzazioni speciali e classi utente:

```
Informazioni profilo utente
Tipo documento . . . . . . . . . :   *AUTINFO
Selezione per  . . . . . . . . . :   *MISMATCH
--------------------------------Autorizzazioni speciali-------------
                                *IO                                                    Gruppo
Profilo   Profili   *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Classe             Autorizz.   Tipo       Possibilità
utente    gruppo     OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  utente     Propriet.  gruppo     autorizz.  limitate
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
```

Figura 6. Documento di informazioni sull'utente: Esempio 2

Nella Figura 6, si noti quanto segue:
- USERX ha una classe utente di operatore di sistema (*SYSOPR) ma ha le autorizzazioni speciali *ALLOBJ e *SPLCTL.
- USERY ha una classe utente di utente (*USER) ma ha l'autorizzazione speciale *SECADM.

- Anche USERZ ha una classe utente (*USER) ed un'autorizzazione speciale *SECADM. E' possibile anche notare che USERZ è un membro di QPGMR, che ha le autorizzazioni speciali *JOBCTL e *SAVSYS.

E' possibile utilizzare questi documenti regolarmente per facilitare il monitoraggio della gestione dei profili utente.

Monitoraggio degli ambienti dell'utente

Un ruolo del profilo utente è quello di definire l'ambiente dell'utente, inclusi le code di emissione, il menu iniziale e la descrizione lavoro. L'ambiente dell'utente influenza il modo in cui l'utente visualizza il sistema e, in qualche misura, ciò che all'utente è consentito fare. L'utente deve avere l'autorizzazione agli oggetti specificati nel profilo utente. Tuttavia, se il proprio schema di autorizzazione è ancora in divenire o non è molto restrittivo, l'ambiente dell'utente che è definito in un profilo utente può produrre risultati indesiderati. I seguenti sono alcuni esempi:

Opzioni menu SECBATCH:
29 *per l'inoltro immediato* **68** *per utilizzare il programma di pianificazione lavoro*

- La descrizione del lavoro dell'utente può specificare un profilo utente con un'autorizzazione superiore all'utente.
- L'utente può avere un menu iniziale senza riga comandi. Tuttavia, il programma di gestione del tasto attenzione dell'utente può fornire una riga comandi.
- L'utente può essere autorizzato ad utilizzare documenti riservati. Tuttavia, l'emissione dell'utente può essere indirizzata ad una coda di emissione a disposizione di utenti che non dovrebbero visualizzare la documentazione.

E' possibile utilizzare l'opzione *ENVINFO del comando Stampa profilo utente (PRTUSRPRF) per facilitare il monitoraggio degli ambienti definiti per gli utenti di sistema. La Figura 7 visualizza un esempio del documento:

```
                                    Informazioni profilo utente
  Tipo documento . . . . . :   *ENVINFO
  Selezione per  . . . . . :   *USRCLS
                          Menu          Programma      Descrizione      Coda          Coda          Programma
Profilo       Libreria    Iniziale/     Iniziale/        lavoro/        messaggi/     emissione/    attenzione/
utente        corrente    Libreria      Libreria         Libreria       Libreria      Libreria       Libreria
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
```

Figura 7. Stampa profilo utente-esempio di ambiente dell'utente

Gestione programmi di manutenzione

I programmi di manutenzione vengono utilizzati per configurare, gestire ed effettuare la manutenzione del server. Ai programmi di manutenzione si può accedere dai DST (dedicated service tools) o dagli SST (system service tools). Gli ID utente dei programmi di manutenzione sono necessari per accedere a DST, SST e per utilizzare le funzioni di iSeries Navigator per la gestione di partizioni logiche (LPAR) e la gestione di unità disco.

DST è disponibile una volta avviato il LIC (Microprogramma interno su licenza), anche se non è stato caricato OS/400. SST è disponibile da OS/400. La seguente tabella evidenzia le differenze di base tra DST ed SST.

Caratteristiche	DST	SST
Modalità d'accesso	Accesso fisico tramite console durante IPL manuale o selezionando l'opzione 21 sul pannello di controllo.	Accesso tramite lavoro interattivo con capacità di collegamento tramite QSRV o le seguenti autorizzazioni: • Autorizzato al comando CL STRSST (Avvio SST). • Autorizzazione speciale al servizio (*SERVICE) o autorizzazione speciale a tutti gli oggetti (*ALLOBJ). • Privilegio funzionale all'utilizzo di SST.
Disponibilità	Disponibile quando il server ha capacità limitate. OS/400 non è necessario per accedere a DST.	Disponibile quando è stato avviato OS/400. OS/400 è necessario per accedere a SST.
Modalità di autenticazione	Richiede ID utente e parola d'ordine dei programmi di manutenzione.	Richiede ID utente e parola d'ordine dei programmi di manutenzione.

Consultare iSeries Information Center—>Sicurezza—>Programmi di manutenzione per informazioni sull'utilizzo dei programmi di manutenzione per svolgere le seguenti attività:

- Accedere ai programmi di manutenzione tramite DST
- Accedere ai programmi di manutenzione tramite SST
- Accedere ai programmi di manutenzione tramite iSeries Navigator
- Creare un ID utente dei programmi di manutenzione
- Modificare i privilegi funzionali per un ID utente dei programmi di manutenzione
- Modificare la descrizione per un ID utente dei programmi di manutenzione
- Visualizzare un ID utente dei programmi di manutenzione
- Abilitare o disabilitare un ID utente dei programmi di manutenzione
- Cancellare un ID utente dei programmi di manutenzione
- Modificare gli ID utente e le parole d'ordine dei programmi di manutenzione utilizzando SST o DST
- Modificare la parola d'ordine dell'ID utente dei programmi di manutenzione utilizzando STRSST
- Modificare ID utente e parole d'ordine dei programmi di manutenzione utilizzando l'API Modifica ID utente programmi di manutenzione (QSYCHGDS)

- Modificare l'API (QSYCHGDS) ID utente dei programmi di manutenzione
- Reimpostare la parola d'ordine del profilo utente QSECOFR OS/400
- Reimpostare l'ID utente e la parola d'ordine dei programmi di manutenzione QSECOFR
- Salvare i dati dei programmi di manutenzione Ripristinare i dati di sicurezza dei programmi di manutenzione
- Creare la propria versione dell'ID utente dei programmi di manutenzione QSECOFR
- Configurare il server dei programmi di manutenzione per DST
- Configurare il server dei programmi di manutenzione per OS/400
- Monitorare l'utilizzo della funzione di servizio tramite DST
- Monitorare l'utilizzo dei programmi di manutenzione tramite la registrazione del controllo di sicurezza OS/400

Consultare "Requisiti necessari e informazioni correlate" a pagina xii per informazioni sull'accesso all'iSeries Information Center.

Capitolo 7. Utilizzo della sicurezza delle partizioni logiche (LPAR)

L'utilizzo di più partizioni logiche su un singolo server iSeries potrebbe risultare vantaggioso nei seguenti scenari.

- **Conservazione di sistemi indipendenti**: se si dedica una parte delle risorse (unità di memoria disco, processori, memoria e unità I/E) alla partizione, si ottiene un isolamento logico del software. Le partizioni logiche dispongono inoltre di una certa tolleranza dell'errore hardware, se configurate correttamente. I carichi di lavoro batch e interattivi che potrebbero non funzionare bene insieme su una singola macchina possono essere isolati e venire eseguiti in modo efficiente in partizioni separate.
- **Consolidazione**: un sistema a partizioni logiche può ridurre il numero di sistemi server iSeries necessari all'interno di un'azienda. E' possibile consolidare numerosi sistemi in un singolo sistema a partizioni logiche. Ciò elimina la necessità e il dispendio di attrezzature aggiuntive. E' possibile spostare le risorse da una partizione logica a un'altra a seconda delle necessità.
- **Creazione di un ambiente di verifica e di produzione misto:** è possibile creare una combinazione di ambiente di verifica e di produzione. E' possibile creare una singola partizione di produzione nella partizione principale. Per più partizioni di produzione, consultare *Creazione di un ambiente a più partizioni di produzione* di seguito.

  Una partizione logica è una partizione di produzione o di verifica. Una partizione di produzione esegue le applicazioni aziendali principali. Un errore in una partizione di produzione potrebbe ostacolare significativamente le operazioni aziendali e causare un dispendio economico e di tempo. Una partizione di verifica verifica il software. Un errore in una partizione di verifica, anche se non è stato necessariamente pianificato, non impedirà le normali operazioni aziendali.
- **Creazione di un ambiente a partizioni di produzione multiple:** sarebbe opportuno creare più partizioni di produzione soltanto nelle partizioni secondarie. In questa situazione, la partizione principale viene dedicata alla gestione delle partizioni.
- **Copia di riserva rapida:** quando una partizione secondaria viene ripetuta su un'altra partizione logica all'interno dello stesso sistema, il passaggio alla copia di riserva durante un errore della partizione causerebbe inconvenienti minimi. Questa configurazione riduce al minimo l'effetto delle finestre di lungo salvataggio. E' possibile scollegare la partizione della copia di riserva e salvare, mentre l'altra partizione logica continua ad eseguire il lavoro di produzione. Sarà necessario un software speciale per utilizzare tale strategia della copia di riserva rapida.
- **Cluster integrato:** utilizzando OptiConnect/400 e un software dell'applicazione ad alta disponibilità, è possibile eseguire il sistema a partizioni come un cluster integrato. E' possibile utilizzare un cluster integrato per proteggere il sistema dalla maggior parte degli errori non pianificati all'interno di una partizione secondaria.

Nota: quando si imposta una partizione secondaria, è necessario fare delle considerazioni aggiuntive per le ubicazioni scheda. Se il processore di Immissione/Emissione (IOP) che si seleziona per la console dispone anche di una scheda LAN e la scheda LAN non è progettata per essere utilizzata con Operations Console, verrà attivato per essere utilizzato dalla console ed

© Copyright IBM Corp. 1996, 2004

è possibile che non si riesca ad utilizzarlo per gli scopi desiderati. Per ulteriori informazioni sulla gestione di Operations Console, consultare il Capitolo 8, “iSeries Operations Console”, a pagina 73.

Fare riferimento a ″Partizioni logiche″ in iSeries Information Center per informazioni più dettagliate su questo argomento.

Gestione sicurezza per partizioni logiche

Le attività correlate alla sicurezza che vengono eseguite su un sistema a partizioni non differiscono da quelle su un sistema senza partizioni logiche. Tuttavia, quando si creano le partizioni logiche, si gestiscono più sistemi indipendenti. Quindi, sarà necessario eseguire le stesse attività su ciascuna partizione logica invece che una sola volta su un sistema senza partizioni logiche.

Di seguito vengono riportate alcune regole di base da ricordare quando ci si occupa della sicurezza sulle partizioni logiche:

- Si aggiungono gli utenti al sistema una partizione logica alla volta. E’ necessario aggiungere utenti a ciascuna partizione logica a cui si desidera che essi accedano.
- Limitare il numero di utenti con l’autorizzazione ai DST (dedicated service tools) e agli SST (system service tools) sulla partizione principale. Fare riferimento all’argomento ″Gestione partizioni logiche utilizzando iSeries Navigator, DST e SST″ in iSeries Information Center per ulteriori informazioni su DST e SST. Fare riferimento a “Gestione programmi di manutenzione” a pagina 67 per informazioni sull’utilizzo dei profili utente del programma di manutenzione per controllare l’accesso alle attività della partizione.

  Nota: è necessario inizializzare STS (Service Tools Server) prima di utilizzare iSeries Navigator per accedere alle funzioni LPAR. Consultare iSeries Information Center—>Sicurezza—>programmi di manutenzione per informazioni correlate. Consultare “Requisiti necessari e informazioni correlate” a pagina xii per informazioni sull’accesso all’iSeries Information Center.
- Le partizioni secondarie non possono visualizzare o utilizzare la memoria principale e le unità disco di un’altra partizione logica.
- Le partizioni secondarie possono visualizzare soltanto le relative risorse hardware.
- La partizione principale può visualizzare tutte le risorse hardware del sistema nei pannelli Gestione partizioni del sistema di DST e SST.
- Il sistema operativo di una partizione principale ancora visualizza soltanto le relative risorse disponibili.
- Il pannello di controllo del sistema controlla la partizione principale. Quando si imposta la modalità del pannello su Sicura, non è possibile eseguire alcuna azione sul pannello Gestione stato partizione da SST. Per forzare DST dal pannello di controllo del sistema, è necessario modificare la modalità in Manuale.
- Quando si imposta la modalità operativa di una partizione secondaria su sicura, si limita l’utilizzo della relativa Gestione stato partizione nei modi seguenti:
  – E’ possibile utilizzare DST soltanto sulla partizione secondaria per modificare lo stato della partizione; non è possibile utilizzare SST per modificare lo stato della partizione.

- E' possibile forzare DST sulla partizione secondaria soltanto dal pannello Gestione stato partizione della partizione principale utilizzando DST o SST.
- E' possibile utilizzare DST soltanto sulla partizione primaria per modificare una modalità della partizione secondaria da sicura in qualsiasi altro valore.

Una volta che la modalità della partizione secondaria non è più sicura, è possibile utilizzare DST e SST sulla partizione secondaria per modificare lo stato della partizione.

Per ulteriori informazioni riguardo alla sicurezza sul server iSeries, fare riferimento al manuale Riferimenti alla sicurezza e alle pagine di pianificazione e sicurezza di base del sistema dell'iSeries Information Center.

Capitolo 8. iSeries Operations Console

Operations Console consente di utilizzare il PC per accedere e controllare il server iSeries. Operations Console include un supporto per il collegamento in entrata del PC remoto ai server iSeries senza unità console, consentendo ai PC remoti di diventare console. Quando si utilizza Operations Console, notare quanto segue:

- Da Operations Console è possibile effettuare qualsiasi attività che si potrebbe eseguire da una console tradizionale. Ad esempio, i profili utente con autorizzazione speciale *SERVICE o *ALLOBJ possono collegarsi alla sessione di Operations Console, anche se sono disabilitati.
- Operations Console utilizza i profili utente e le parole d'ordine dei Programmi di manutenzione per abilitare il collegamento al server iSeries. Ciò rende di particolare rilievo la modifica di tali profili utente e parole d'ordine. Gli hacker sembrano avere familiarità con gli ID utente e le parole d'ordine dei profili utente dei Programmi di manutenzione predefiniti e potrebbero utilizzarli per tentare una sessione della console remota sul server iSeries. Consultare "Modifica parole d'ordine note" a pagina 21 e "Come evitare parole d'ordine predefinite" a pagina 27 per suggerimenti e parole d'ordine.
- Per proteggere le informazioni quando si utilizza la console remota, utilizzare l'opzione di richiamata di Dial-Up Networking di Windows.
- Quando si imposta una partizione secondaria, è necessario fare delle considerazioni aggiuntive per le ubicazioni scheda. Se il processore di Immissione/Emissione (IOP) che si seleziona per la console dispone anche di una scheda LAN e la scheda LAN non è progettata per essere utilizzata con Operations Console, verrà attivato per essere utilizzato dalla console ed è possibile che non si riesca ad utilizzarlo per gli scopi desiderati.

In V5R1, Operations Console è stato migliorato per abilitare l'esecuzione delle attività della console su una LAN (local area network). L'autenticazione e la codifica dati potenziate forniscono la sicurezza di rete per le procedure della console. Per utilizzare Operations Console con connettività LAN, si consiglia vivamente di installare i seguenti prodotti:

- Cryptographic Access Provider, 5722–AC2 o 5722–AC3 sul server iSeries
- Client Encryption, 5722–CE2 o 5722–CE3 sul PC Operations Console

Per codificare i dati della console, è necessario che il server iSeries presenti uno dei prodotti Cryptographic Access Provider installati **e** che il PC abbia uno dei prodotti Client Encryption installati.

Nota: se non è installato alcun prodotto crittografico, non avverrà alcuna codifica dati.

La tabella riportata di seguito riassume i risultati della codifica dei prodotti disponibili:

Tabella 13. Risultati della codifica

Cryptographic Access Provider sul server iSeries	Client Encryption sul PC Operations Console	Codifica dati risultante
Nessuno	Nessuno	Nessuno
5722–AC2	5722–CE2	56 bit
5722–AC2	5722–CE3	56 bit

© Copyright IBM Corp. 1996, 2004

Tabella 13. Risultati della codifica (Continua)

Cryptographic Access Provider sul server iSeries	Client Encryption sul PC Operations Console	Codifica dati risultante
5722–AC3	5722–CE2	56 bit
5722–AC3	5722–CE3	128 bit

Per ulteriori informazioni sull'impostazione e la gestione di iSeries Operations Console, consultare l'iSeries Information Center.

Panoramica sulla sicurezza di Operations Console

La sicurezza di Operations Console consiste in:

- autenticazione dell'unità console
- autenticazione dell'utente
- riservatezza dei dati
- integrità dei dati

Operations Console con connettività diretta ha l'autenticazione unità, la riservatezza e l'integrità dei dati implicite grazie al collegamento point-to-point. La sicurezza di autenticazione dell'utente è richiesta per collegarsi al pannello della console.

Autenticazione dell'unità console

L'autenticazione dell'unità console garantisce l'unità fisica che funge da console. Operations Console con connettività diretta utilizza un collegamento fisico simile a una console biassiale. Operations Console utilizzando un collegamento diretto può essere protetta fisicamente in modo simile a un collegamento biassiale per controllare l'accesso all'unità console fisica.

Operations Console con connettività LAN utilizza una versione di SSL (secure sockets layer) che supporta l'autenticazione utente e unità ma senza utilizzare i certificati. Per tale forma di collegamento, l'autenticazione unità si basa su un profilo unità dei programmi di manutenzione. Fare riferimento a pagina 75 per ulteriori dettagli.

Autenticazione utente

L'autenticazione utente fornisce garanzie sull'utente che sta utilizzando l'unità console. Tutte le questioni relative all'autenticazione utente sono le stesse indipendentemente dal tipo di console.

Riservatezza dei dati

La riservatezza dei dati garantisce che i dati della console possano essere letti soltanto dal destinatario stabilito. Operations Console con connettività diretta utilizza un collegamento fisico simile a una console biassiale o un collegamento di rete protetto affinché la connettività LAN protegga i dati della console. Operations Console che utilizza un collegamento diretto ha la stessa riservatezza di dati di un collegamento biassiale. Se il collegamento fisico è sicuro, i dati della console rimangono protetti.

Operations Console con connettività LAN utilizza un collegamento di rete sicuro se sono installati i prodotti crittografici appropriati (ACx e CEx). La sessione della

console utilizza la codifica più potente possibile, a seconda dei prodotti crittografici installati sul server iSeries e sul PC che esegue Operations Console.

Nota: se non è installato alcun prodotto crittografico, non avverrà alcuna codifica dati.

Integrità dei dati

L'integrità dei dati garantisce che i dati della console non vengano cambiati nel percorso verso il destinatario. Operations Console con connettività diretta utilizza un collegamento fisico simile a una console biassiale o un collegamento di rete protetto affinché la connettività LAN protegga i dati della console. Operations Console che utilizza un collegamento diretto ha la stessa integrità di dati di un collegamento biassiale. Se il collegamento fisico è sicuro, i dati della console rimangono protetti.

Operations Console con connettività LAN utilizza un collegamento di rete sicuro se sono installati i prodotti crittografici appropriati (ACx e CEx). La sessione della console utilizza la codifica più potente possibile, a seconda dei prodotti crittografici installati sul server iSeries e sul PC che esegue Operations Console.

Nota: se non è installato alcun prodotto crittografico, non avverrà alcuna codifica dati.

Utilizzo di Operations Console con connettività LAN

Nota: qualsiasi unità Operations Console può essere una console, ma soltanto le configurazioni basate su LAN utilizzano il profilo utente dei programmi di manutenzione.

Il server iSeries viene fornito con un profilo unità dei programmi di manutenzione predefinito, QCONSOLE, con una parola d'ordine predefinita QCONSOLE. Operations Console con connettività LAN modificherà la parola d'ordine durante ciascun collegamento riuscito. Consultare "Utilizzo del wizard di configurazione di Operations Console" a pagina 76 per ulteriori informazioni.

Per ulteriori informazioni su iSeries Operations Console con connettività LAN, fare riferimento all'argomento, Configurazione di Operations Console con connettività LAN, nell'Information Center.

Protezione di Operations Console con connettività LAN

Quando si utilizza Operations Console con connettività LAN, si consiglia di eseguire le attività riportate di seguito:

- Creare un altro profilo utente dei programmi di manutenzione con attributi console e memorizzare le informazioni sul profilo in un'ubicazione protetta.
- Installare Cryptographic Access Provider, 5722–AC2 o 5722–AC3 sul server iSeries e Client Encryption, 5722–CE2 o 5722–CE3 sul PC Operations Console.
- Scegliere una parola d'ordine della informazioni sull'unità di servizio non banale.
- Proteggere il PC Operations Console nello stesso modo in cui si proteggerebbe una console biassiale o un'Operations Console con connettività diretta.

Utilizzo del wizard di configurazione di Operations Console

Il wizard di configurazione aggiungerà le informazioni necessarie sul PC quando si utilizza Operations Console con connettività LAN. Esso richiede il profilo unità dei programmi di manutenzione, la relativa parola d'ordine e una parola d'ordine per proteggere le informazioni su tale profilo unità.

Nota: la parola d'ordine delle informazioni sul profilo unità dei programmi di manutenzione viene utilizzata per vincolare e svincolare tali informazioni (parola d'ordine e profilo unità dei programmi di manutenzione) sul PC.

Quando si stabilisce un collegamento di rete, il wizard di configurazione Operations Console richiederà all'utente la parola d'ordine delle informazioni sull'unità di servizio per accedere alla parola d'ordine e al profilo unità crittografati dei programmi di manutenzione. Verranno inoltre richiesti all'utente una parola d'ordine e un identificativo utente dei programmi di manutenzione validi.

Capitolo 9. Rilevazione programmi sospetti

Recenti tendenze nell'uso dei computer hanno aumentato la probabilità che il proprio sistema abbia programmi provenienti da origini o programmi non garantiti che eseguono funzioni non riconosciute. Di seguito sono riportati alcuni esempi:

- Un utente di personal computer talvolta ottiene programmi da altri utenti PC. Se il PC è collegato al sistema iSeries, tale programma può interessare il server iSeries.
- Anche utenti che si collegano a reti possono ottenere programmi, ad esempio dalle bacheche.
- Gli hacker sono diventati più attivi e rinomati. Spesso pubblicano i loro metodi ed i risultati raggiunti. Questo può favorire l'imitazione da parte di programmatori che normalmente si attengono alla legge.

Queste tendenze hanno causato un problema nella sicurezza dei computer noto come **virus del computer**. Un virus è un programma che può modificare altri programmi in modo da includere una copia di sé stesso. Quindi si dice che gli altri programmi sono infettati dal virus. Inoltre, il virus può eseguire altre operazioni che possono sovraccaricare risorse di sistema o distruggere dati.

L'architettura del server iSeries fornisce qualche protezione dalle caratteristiche invasive di un virus del computer. "Protezione contro i virus del computer" descrive questo aspetto. Un responsabile della sicurezza del server iSeries deve essere più preoccupato dei programmi che seguono funzioni non autorizzate. Gli argomenti che restano in questo capitolo descrivono i modi in cui un malintenzionato potrebbe configurare programmi dannosi per l'esecuzione sul sistema. Gli argomenti forniscono suggerimenti per impedire l'esecuzione di funzioni non autorizzate da parte di programmi.

Suggerimenti sulla sicurezza

L'autorizzazione all'oggetto rappresenta sempre la prima linea difensiva. Se non si dispone di un buon piano per la protezione degli oggetti, il sistema è senza difese. Queste informazioni discutono i modi in cui un utente autorizzato potrebbe tentare di trarre vantaggio da buchi del loop nello schema di autorizzazione all'oggetto.

Protezione contro i virus del computer

Un computer infettato da virus ha un programma che può modificare altri programmi. L'architettura basata sugli oggetti di iSeries rende più difficile ad un malintenzionato produrre e diffondere questo tipo di virus di quanto sia con altre architetture di computer. Sul server iSeries, si utilizzano specifici comandi ed istruzioni per operare su ogni tipo di oggetto. Non è possibile utilizzare un'istruzione file per modificare un oggetto programma operativo (che è quello che fanno la maggior parte dei creatori di virus). Né è possibile creare facilmente un programma che modifichi un altro oggetto programma. Fare ciò, richiede una considerevole quantità di tempo, di sforzo e di esperienza e richiede l'accesso a strumenti e documentazione non generalmente disponibili.

© Copyright IBM Corp. 1996, 2004

Tuttavia, se nuove funzioni del server iSeries diventano disponibili a partecipare ad un ambiente di sistemi aperti, alcune delle funzioni di protezione basata sull'oggetto dei server iSeries non sono più applicabili. Ad esempio, con IFS (IFS (integrated file system)), gli utenti possono agire direttamente su alcuni oggetti negli indirizzari, come ad esempio i file di flusso.

Inoltre, sebbene l'architettura del server iSeries renda difficoltosa la diffusione di un virus attraverso i programmi del server iSeries, la suddetta architettura non impedisce che il server iSeries sia un portatore di virus. Come server dei file, il server iSeries può memorizzare programmi che molti utenti PC condividono. Uno qualsiasi di questi programmi potrebbe contenere un virus che il server iSeries non individua. Per impedire che questo tipo di virus infetti i PC collegati al server iSeries, è necessario utilizzare un software di scansione dei virus per il PC.

Vi sono diverse funzioni sul server iSeries atte ad impedire che qualcuno utilizzi un linguaggio di basso livello con capacità di puntatore per modificare un programma oggetto operativo:

- Se il sistema si esegue ad un livello di sicurezza di 40 o superiore, la protezione a tutela dell'integrità include protezioni contro oggetti programma che si modificano. Ad esempio, non è possibile eseguire con esito positivo un programma che contiene istruzioni macchina bloccate (protette).
- Il valore di convalida del programma serve anche a proteggere l'utente quando ripristina un programma che era stato salvato (e potenzialmente modificato) in un altro sistema. Il Capitolo 2 nel manuale *Riferimenti alla sicurezza iSeries* descrive le funzioni di protezione dell'integrità per il livello di sicurezza 40 e superiore, compresi i valori di convalida del programma.

  Nota: il valore di convalida del programma non è infallibile e non esonera dal prestare attenzione nella valutazione dei programmi ripristinati nel sistema.

Sono anche disponibili diversi strumenti per facilitare l'individuazione della presenza di un programma alterato nel sistema:

- E' possibile utilizzare il comando Controllo integrità oggetto (CHKOBJITG) per effettuare la scansione di oggetti (oggetti operativi) che corrispondono ai valori di ricerca per accertare che quegli oggetti non siano stati modificati. E' simile ad una funzione di scansione virus.
- E' possibile utilizzare la funzione di controllo sicurezza per monitorare programmi modificati o ripristinati. I valori *PGMFAIL, *SAVRST e *SECURITY per il valore di sistema del livello di autorizzazione forniscono record di controllo che possono facilitare l'individuazione di tentativi di introdurre un programma tipo virus nel sistema. Il Capitolo 9 e l'Appendice F nel manuale *Riferimenti alla sicurezza iSeries* forniscono ulteriori informazioni sui valori di controllo e sulle voci del giornale di controllo.
- E' possibile utilizzare il parametro forzatura creazione (FRCCRT) del comando Modifica programma (CHGPGM) per ricreare qualsiasi programma ripristinato nel sistema. Il sistema utilizza la mascherina del programma per ricreare il programma. Se l'oggetto programma è stato modificato dopo la compilazione, il sistema ricrea l'oggetto modificato e lo sostituisce. Se la mascherina del programma contiene istruzioni bloccate (protette), il sistema non ricreerà il programma con esito positivo.
- E' possibile utilizzare il valore di sistema QFRCCVNRST (forzatura conversione al ripristino) per ricreare qualsiasi programma al momento del ripristino sul

sistema. Il sistema utilizza la mascherina del programma per ricreare il programma. Questo valore di sistema fornisce diverse scelte riguardo a quali programmi ricreare.

- E' possibile utilizzare il valore di sistema QVFYOBJRST (verifica degli oggetti al ripristino) per impedire il ripristino di programmi che non hanno una firma digitale o non hanno una firma digitale valida. Quando una firma digitale non è valida, significa che il programma è stato modificato da quando è stato firmato dallo sviluppatore. Esistono delle API che consentono di firmare i propri programmi, i file di salvataggio ed i file di flusso.

Per ulteriori informazioni sulla firma e su come può essere utilizzata per proteggere il proprio sistema da attacchi, consultare "Firma oggetto" a pagina 90.

Monitoraggio dell'utilizzo dell'autorizzazione adottata

In un server iSeries, è possibile creare un programma che adotta l'autorizzazione del proprietario del programma. Questo significa che qualsiasi utente che esegue il programma ha le stesse autorizzazioni (autorizzazioni private ed autorizzazioni speciali) del profilo utente che possiede il programma.

L'autorizzazione adottata è uno strumento di sicurezza di valore quando è utilizzato correttamente. "Potenziamento del controllo accesso menu tramite la sicurezza dell'oggetto" a pagina 49, ad esempio, descrive come combinare autorizzazione adottata e menu per aiutare l'utente ad andare oltre il controllo accesso menu. E' possibile utilizzare l'autorizzazione adottata per proteggere i file importanti dal venire modificati al di fuori dei programmi di applicazione approvati mentre sono ancora consentite query rispetto ai file.

Come responsabile della sicurezza, ci si dovrebbe assicurare che l'autorizzazione adottata venga utilizzata in modo appropriato:

- I programmi dovrebbero adottare l'autorizzazione di un profilo utente che abbia solo l'autorizzazione sufficiente ad eseguire le funzioni necessarie, non un'autorizzazione eccessiva. Si dovrebbe essere particolarmente cauti rispetto a programmi che adottano l'autorizzazione di un profilo utente che dispone dell'autorizzazione speciale *ALLOBJ o possiede oggetti importanti.
- Programmi che adottano l'autorizzazione dovrebbero avere una funzione specifica, limitata e non dovrebbero fornire capacità di immissione comandi.
- Programmi che adottano l'autorizzazione dovrebbero essere protetti in modo appropriato.
- L'uso eccessivo dell'autorizzazione adottata può avere un impatto negativo sulle prestazioni del proprio sistema. Per assistenza nell'evitare problemi di prestazioni, esaminare i diagrammi di flusso e i suggerimenti per il controllo dell'autorizzazione per l'utilizzo dell'autorizzazione adottata nel Capitolo 5 del manuale *Riferimenti alla sicurezza iSeries*.

Opzioni menu SECBATCH:
1 *per l'inoltro immediato* **40 per utilizzare il programma di pianificazione lavoro**

E' possibile utilizzare il comando Stampa oggetti di adozione (PRTADPOBJ) (opzione 21 sul menu SECTOOLS) per facilitare il monitoraggio dell'utilizzo dell'autorizzazione sul sistema.

Il documento visualizza le autorizzazioni speciali del profilo utente specificato, i programmi che adottano l'autorizzazione del profilo utente ed anche le unità ASP che utilizzano le autorizzazioni del profilo. Una volta creata una base di informazioni, è possibile stampare regolarmente la versione modificata del documento relativo agli oggetti adottati. Questo elenca nuovi programmi che adottano l'autorizzazione e programmi che sono stati modificati per adottare l'autorizzazione dall'ultimo utilizzo del documento.

Se si sospetta un non corretto utilizzo dell'autorizzazione adottata sul sistema, è possibile impostare il valore di sistema QAUDLVL in modo da includere *PGMADP. Quando questo valore è attivo, il sistema crea una voce giornale di controllo ogni volta che qualcuno avvia o chiude un programma che adotta l'autorizzazione. La voce include il nome dell'utente che ha avviato il programma ed il nome del programma.

Limitazione dell'utilizzo dell'autorizzazione adottata

Quando si esegue un programma iSeries, il programma può utilizzare l'autorizzazione adottata per ottenere l'accesso agli oggetti in due modi diversi:

- Il programma stesso può adottare l'autorizzazione del relativo proprietario. Questo è specificato nel parametro profilo utente (USRPRF) del programma o del programma di servizio.
- Il programma può utilizzare (ereditare) l'autorizzazione adottata da un precedente programma che si trova ancora nello stack di chiamate del lavoro. Un programma può ereditare l'autorizzazione adottata da precedenti programmi anche se il programma stesso non adotta l'autorizzazione. Il parametro di utilizzo autorizzazione adottata (USEADPAUT) di un programma o di un programma di servizio controlla se il programma eredita l'autorizzazione adottata da precedenti programmi nello stack dei programmi.

Quello che segue è un esempio di come funziona l'utilizzo dell'autorizzazione adottata da precedenti programmi.

Supponiamo che il profilo utente ICOWNER abbia l'autorizzazione *CHANGE per il file ITEM e che l'autorizzazione pubblica al file ITEM sia *USE. Nessun altro profilo utente dispone di alcuna autorizzazione esplicitamente definita per il file ITEM. La Tabella 14 riporta gli attributi per tre programmi che utilizzano il file ITEM:

Tabella 14. Esempio di Utilizzo autorizzazione adottata (USEADPAUT)

Nome programma	Proprietario programma	Valore USRPRF	Valore USEADPAUT
PGMA	ICOWNER	*OWNER	*YES
PGMB	ICOWNER	*USER	*YES
PGMC	ICOWNER	*USER	*NO

Esempio 1–Adozione autorizzazione:
1. USERA esegue il programma PGMA.
2. Il programma PGMA tenta di aprire il file ITEM con capacità di aggiornamento.

Risultato: il tentativo ha avuto esito positivo. USERA ha accesso *CHANGE al file ITEM poiché PGMA adotta l'autorizzazione di ICOWNER.

Esempio 2–Utilizzo autorizzazione adottata:

1. USERA esegue il programma PGMA.
2. Il programma PGMA richiama il programma PGMB.
3. Il programma PGMB tenta di aprire il file ITEM con capacità di aggiornamento.

Risultato: il tentativo ha avuto esito positivo. Anche se il programma PGMB non adotta l'autorizzazione (*USRPRF è *USER), consente l'utilizzo di una precedente autorizzazione adottata (*USEADPAUT è *YES). Il programma PGMA è ancora nello stack dei programmi. Perciò, USERA ottiene accesso *CHANGE al file ITEM poiché PGMA adotta l'autorizzazione di ICOWNER.

Esempio 3–Non utilizzo dell'autorizzazione adottata:
1. USERA esegue il programma PGMA.
2. Il programma PGMA richiama il programma PGMC.
3. Il programma PGMC tenta di aprire il file ITEM con capacità di aggiornamento.

Risultato: errore di autorizzazione. Il programma PGMC non adotta l'autorizzazione. Il programma PGMC non consente l'utilizzo dell'autorizzazione adottata da programmi precedenti. Anche se PGMA si trova ancora nello stack delle chiamate, la sua autorizzazione adottata non viene utilizzata.

Prevenzione dell'utilizzo dell'autorizzazione adottata da parte di nuovi programmi

Il passaggio dell'autorizzazione adottata a programmi successivi nello stack fornisce un'opportunità per un programmatore esperto di creare un programma Trojan horse (cavallo di Troia). Il programma Trojan horse (cavallo di Troia) può basarsi su programmi precedenti nello stack per ottenere l'autorizzazione necessaria ad eseguire qualche azione dannosa. Per impedire ciò, è possibile limitare gli utenti a cui è consentito creare programmi che utilizzano l'autorizzazione adottata di precedenti programmi.

Quando si crea un nuovo programma, il sistema imposta automaticamente il parametro USEADPAUT su *YES. Se non si desidera che il programma erediti l'autorizzazione adottata, si deve utilizzare il comando Modifica programma (CHGPGM) o il comando Modifica programma servizio (CHGSRVPGM) per impostare il parametro USEADPAUT su *NO.

E' possibile utilizzare un elenco di autorizzazioni ed il valore di sistema di utilizzo autorizzazione adottata (QUSEADPAUT) per controllare chi può creare programmi che ereditano l'autorizzazione adottata. Quando si specifica un nome elenco autorizzazioni nel valore di sistema QUSEADPAUT, il sistema utilizza questo elenco di autorizzazioni per determinare la modalità di creazione di nuovi programmi.

Quando un utente crea un programma o un programma di servizio, il sistema controlla l'autorizzazione dell'utente nell'elenco autorizzazioni. Se l'utente dispone dell'autorizzazione *USE, il parametro USEADPAUT per il nuovo programma è impostato su *YES. Se l'utente non ha l'autorizzazione *USE, il parametro USEADPAUT è impostato su *NO. L'autorizzazione dell'utente nell'elenco autorizzazioni non può provenire dall'autorizzazione adottata.

L'elenco autorizzazioni che si specifica nel valore di sistema QUSEADPAUT controlla anche se un utente può utilizzare un comando CHGxxx per impostare il valore USEADPAUT per un programma o un programma di servizio.

Note:

1. Non è necessario denominare il proprio elenco autorizzazioni QUESADPAUT. E' possibile creare un elenco autorizzazioni con un nome differente. Quindi specificare tale elenco autorizzazioni per il valore di sistema QUSEADPAUT. Nei comandi riportati in questo esempio, sostituire il nome dell'elenco autorizzazioni.
2. Il valore di sistema QUSEADPAUT non interessa i programmi esistenti sul sistema. Utilizzare il comando CGHPGM o il comando CHGSRVPGM per impostare il parametro USEADPAUT per programmi esistenti.

Ambiente più restrittivo: se si desidera che la maggior parte degli utenti crei nuovi programmi con il parametro USEADPAUT impostato su *NO, effettuare quanto segue:

1. Per impostare l'autorizzazione pubblica per l'elenco autorizzazioni su *EXCLUDE, immettere quanto segue:

   ```
   CHGAUTLE AUTL(QUSEADPAUT) USER(*PUBLIC)
            AUT(*EXCLUDE)
   ```

2. Per impostare utenti specifici in modo che creino programmi che utilizzano l'autorizzazione adottata di precedenti programmi, immettere quanto segue:

   ```
   ADDAUTLE AUTL(QUSEADPAUT) USER(nome-utente)
        AUT(*USE)
   ```

Ambiente meno restrittivo: se si desidera che la maggior parte degli utenti crei nuovi programmi con il parametro USEADPAUT impostato su *YES, effettuare quanto segue:

1. Lasciare l'autorizzazione pubblica per l'elenco autorizzazioni impostata su *USE.
2. Per impedire a specifici utenti di creare programmi che utilizzano l'autorizzazione adottata di precedenti programmi, immettere quanto segue:

   ```
   ADDAUTLE AUTL(QUSEADPAUT)
      USER(nome-utente) AUT(*EXCLUDE)
   ```

Monitoraggio dell'utilizzo di programmi trigger

UDB DB2 fornisce la capacità di associare programmi trigger a file di database. La capacità di programmi trigger è comune in tutto il settore industriale per gestori database ad elevata funzionalità.

Quando si associa un programma trigger ad un file di database, si specifica quando viene eseguito il programma trigger. Ad esempio, è possibile impostare il file ordini del cliente in modo che esegua un programma trigger ogni volta che si aggiunge un nuovo record al file. Quando il saldo in sospeso del cliente supera il limite di credito, il programma trigger può stampare una lettera d'avviso per il cliente ed inviare un messaggio al gestore del credito.

I programmi trigger rappresentano un modo efficiente sia per fornire funzioni applicative che per gestire informazioni. I programmi trigger danno anche la possibilità ad utenti con intenzioni poco chiare di creare un "Trojan horse (cavallo di Troia)" sul sistema. Un programma distruttivo potrebbe essere pronto e in attesa di esecuzione quando si verifica un certo evento in un file di database sul sistema.

Nota: secondo la storia, il Cavallo di Troia era un grande cavallo di legno cavo che fu riempito di guerrieri greci. Una volta introdotto il cavallo entro le mura della città di Troia, i soldati ne uscirono e sconfissero i Troiani. Nel mondo

dell'informatica, un programma che nasconde al suo interno funzioni distruttive viene spesso chiamato Trojan horse (cavallo di Troia).

Opzioni menu SECBATCH:
27 *per l'inoltro immediato* **66** *per utilizzare il programma di pianificazione lavoro*

Quando il sistema viene fornito, la capacità di aggiungere un programma trigger ad un file di database è limitata. Se si sta effettuando un'attenta gestione dell'autorizzazione all'oggetto, l'utente ordinario non disporrà di un'autorizzazione sufficiente per aggiungere un programma trigger ad un file di database. L'Appendice D nel manuale *Riferimenti alla sicurezza iSeries* indica l'autorizzazione richiesta o tutti i comandi, incluso il comando Aggiunta trigger file fisico (ADDPFTRG).

E' possibile utilizzare il comando Stampa programmi trigger (PRTTRGPGM) per stampare un elenco di tutti i programmi trigger in una specifica libreria o in tutte le librerie.

E' possibile utilizzare il documento iniziale come base per valutare qualsiasi programma trigger già presente nel sistema. Quindi, è possibile stampare regolarmente il documento modificato per verificare se sono stati aggiunti nuovi programmi trigger al sistema.

Quando si valutano i programmi trigger, considerare quanto segue:

- Chi ha creato il programma trigger? E' possibile utilizzare il comando Visualizzazione descrizione oggetto (DSPOBJD) per stabilirlo.
- Quali sono le funzioni del programma? Si dovrà esaminare il programma origine o parlare con il creatore del programma per stabilirlo. Ad esempio, il programma trigger effettua un controllo per verificare l'identità dell'utente? Forse il programma trigger è in attesa di un particolare utente (QSECOFR) per ottenere l'accesso alle risorse di sistema.

Una volta creata una base di informazioni, è possibile stampare regolarmente il documento modificato per monitorare i nuovi programmi trigger aggiunti al sistema.

Controllo di programmi nascosti

I programmi trigger non sono l'unico mezzo possibile per introdurre un cavallo di Troia nel sistema. I programmi trigger sono l'esempio di un **programma di uscita**. Quando si verifica un determinato evento, come un aggiornamento di un file nel caso di un programma trigger, il sistema esegue il programma di uscita associato a tale evento.

La Tabella 15 a pagina 84 descrive altri esempi di programmi di uscita che potrebbero trovarsi sul sistema. Sarebbe opportuno utilizzare gli stessi metodi per valutare l'utilizzo e il contenuto di tali programmi di uscita utilizzati per i programmi trigger.

Nota: la Tabella 15 a pagina 84 non è un elenco completo di possibili programmi di uscita.

.

Tabella 15. Programmi di uscita forniti dal sistema

Nome programma	Quando si esegue il programma
Nome specificato dall'utente sull'attributo di rete DDMACC.	Quando un utente tenta di aprire un file DDM sul sistema o esegue un collegamento DRDA.
Nome specificato dall'utente sull'attributo di rete PCSACC.	Quando un utente tenta di utilizzare le funzioni Client Access che utilizzano i client originali per accedere agli oggetti sul sistema.
Nome specificato dall'utente sul valore di sistema QPWDVLDPGM	Quando un utente esegue la funzione Modifica parola d'ordine.
Nome specificato dall'utente sul valore di sistema QRMTSIGN.	Quando un utente tenta di collegarsi in modo interattivo da un sistema remoto.
QSYS/QEZUSRCLNP	Quando viene eseguita la funzione di ripulitura automatica.
Nome specificato dall'utente sul parametro EXITPGM del comando CHGBCKUP.	Quando si utilizza la funzione di copia di riserva di Operation Assistant.
Nomi specificati dall'utente sul comando CRTPRDLOD.	Prima e dopo il salvataggio, il ripristino o la cancellazione del prodotto creato con il comando.
Nome specificato dall'utente sul parametro DFTPGM del comando CHGMSGD.	Se si specifica un programma predefinito per un messaggio, il sistema esegue il programma al momento dell'emissione di tale messaggio. A causa dell'ingente numero di descrizioni messaggio su un sistema tipico, l'utilizzo dei programmi predefiniti è di difficile monitoraggio. Per impedire a utenti pubblici di aggiungere dei programmi predefiniti per i messaggi, considerare di impostare l'autorizzazione pubblica per i file di messaggio (oggetti *MSGF) su *USE.
Nome specificato dall'utente sul parametro FKEYPGM del comando STREML3270.	Quando l'utente preme un tasto funzionale durante la sessione di emulazione dell'unità 3270. Il sistema riporta il controllo alla sessione di emulazione dell'unità 3270 al termine del programma di uscita.
Nome specificato dall'utente sul parametro EXITPGM dei comandi di monitoraggio prestazioni	Per elaborare i dati raccolti dai seguenti comandi: STRPFRMON, ENDPFRMON, ADDPFRCOL e CHGPFRCOL. Il programma viene eseguito al termine della raccolta dati.
Nome specificato dall'utente sul parametro EXITPGM del comando RCVJRNE.	Per ciascuna voce del giornale o gruppo di voci del giornale che vengono lette dal giornale e dai ricevitori di giornale specificati.
Nome specificato dall'utente sull'API QTNADDCR.	Durante un'operazione di COMMIT o ROLLBACK.
Nomi specificati dall'utente sull'API QHFRGFS.	Per eseguire funzioni del file system.
Nome specificato dall'utente sul parametro SEPPGM di una descrizione dell'unità di stampa	Per stabilire cosa stampare sulla pagina separatore prima o dopo un file di spool o un lavoro di stampa.
QGPL/QUSCLSXT	Quando un file di database viene chiuso per consentire la cattura delle informazioni sull'utilizzo del file.
Nome specificato dall'utente sul parametro FMTSLR di un file logico.	Quando si scrive un record sul file di database e il nome formato record non è incluso nel programma di linguaggio ad elevato livello. Il programma selettore riceve il record come immissione, stabilisce il formato record utilizzato e lo restituisce al database.
Nome specificato dall'utente indicato nel valore di sistema QATNPGM, nel parametro ATNPGM in un profilo utente o nel parametro PGM del comando SETATNPGM.	Quando un utente preme il tasto di Attenzione.

Tabella 15. Programmi di uscita forniti dal sistema (Continua)

Nome programma	Quando si esegue il programma
Nome specificato dall'utente sul parametro EXITPGM del comando TRCJOB.	Prima di avviare la procedura di Traccia lavoro.

Per i comandi che consentono di specificare un programma di uscita, sarebbe opportuno accertarsi che il valore predefinito del comando non sia stato modificato per specificare un programma di uscita. Ci si dovrebbe assicurare che l'autorizzazione pubblica per tali comandi non sia sufficiente per modificare il valore predefinito del comando. Il comando CHGCMDDFT richiede l'autorizzazione *OBJMGT al comando. Non è necessaria l'autorizzazione *OBJMGT per eseguire un comando.

Valutazione di programmi di uscita registrati

E' possibile utilizzare la funzione di registrazione del sistema per registrare i programmi di uscita da eseguire nel caso si verifichino determinate situazioni. Per elencare le informazioni di registrazione sul sistema, immettere `WRKREGINF OUTPUT(*PRINT)`. La Figura 8 visualizza un esempio del documento:

```
              Gestione informazioni registrazione
Punto di uscita . . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
Formato punto di uscita . . . . . . . . :   NJE00100
Punto di uscita registrato  . . . . . . :   *YES
Consentire la non registrazione . . . . :   *YES
Numero massimo di programmi di uscita . :   *NOMAX
Numero corrente di programmi di uscita. :   0
Preelaborazione per aggiunta  . . . . . :   *NONE
Libreria  . . . . . . . . . . . . . . . :
Formato . . . . . . . . . . . . . . . . :
Preelaborazione per rimozione . . . . . :   *NONE
Libreria  . . . . . . . . . . . . . . . :
Formato . . . . . . . . . . . . . . . . :
Preelaborazione per duplicazione  . . . :   *NONE
Libreria  . . . . . . . . . . . . . . . :
```

Figura 8. Gestione informazioni registrazione-Esempio

Per ciascun punto di uscita sul sistema, la documentazione visualizza se qualche programma di uscita è correntemente registrato. Quando un punto di uscita presenta dei programmi correntemente registrati, è possibile selezionare l'opzione 8 (Visualizzazione programmi) dalla versione del pannello WRKREGINF per visualizzare le informazioni sui programmi:

```
                    Gestione informazioni registrazione

Immettere le opzioni e premere Invio.
5=Visualizzazione punto di uscita   8=Gestione programmi di uscita

                          Formato
     Punto di             punto di
Opz  uscita               uscita    Registrato  Testo
     QIBM_QGW_NJEOUTBOUND NJEO0100     *YES     Pr. uscita voce lavoro rete
8    QIBM_QHQ_DTAQ        DTAQ0100     *YES     Server originario coda dati
     QIBM_QLZP_LICENSE    LICM0100     *YES     Server originario gestione licenza
     QIBM_QMF_MESSAGE     MESS0100     *YES     Server originario messaggi
     QIBM_QNPS_ENTRY      ENTR0100     *YES     Server di stampa rete - voce
     QIBM_QNPS_SPLF       SPLF0100     *YES     Server di stampa rete - file
     QIBM_QNS_CRADDACT    ADDA0100     *YES     Aggiunta attività descriz. CRQ
     QIBM_QNS_CRCHGACT    CHGA0100     *YES     Modifica attività descriz. CRQ
```

Per valutare questi programmi di uscita utilizzare lo stesso metodo che si utilizza per altri programmi di uscita e programmi trigger.

Controllo programmi pianificati

iSeries fornisce numerosi metodi per pianificare i lavori da eseguire in un secondo momento, incluso il programma di pianificazione lavoro. Normalmente, tali metodi non rappresentano un rischio per la sicurezza poiché l'utente che pianifica il lavoro deve avere la stessa autorizzazione richiesta per inoltrare il lavoro in batch.

Tuttavia, sarebbe opportuno controllare periodicamente i lavori pianificati nel futuro. Un utente scontento che non fa più parte della società potrebbe utilizzare tale metodo per pianificare un disastro.

Limitazione della funzione Salvataggio e ripristino

La maggior parte degli utenti non ha necessità di salvare e ripristinare gli oggetti sul sistema. I comandi di salvataggio forniscono la possibilità di copiare importanti risorse della società su supporti magnetici o su un altro sistema. La maggior parte dei comandi di salvataggio supportano file di salvataggio che è possibile inviare a un altro sistema (utilizzando il comando file SNDNETF) senza accedere ai supporti magnetici o a un'unità di salvataggio/ripristino.

I comandi di ripristino consentono di ripristinare oggetti non autorizzati, come ad esempio programmi, comandi e file, sul sistema. E' inoltre possibile ripristinare informazioni senza accedere ai supporti magnetici o a un'unità di salvataggio/ripristino utilizzando i file di salvataggio. E' possibile inviare i file di salvataggio da un altro sistema utilizzando il comando SNDNETF o la funzione FTP.

Di seguito vengono riportati dei suggerimenti per limitare le operazioni di salvataggio e di ripristino sul sistema:

- Controllare quali utenti hanno l'autorizzazione speciale *SAVSYS. L'autorizzazione speciale *SAVSYS consente all'utente di salvare e ripristinare gli oggetti anche quando l'utente non dispone dell'autorizzazione necessaria agli oggetti.
- Controllare l'accesso fisico alle unità di salvataggio e ripristino.
- Limitare l'accesso ai comandi di salvataggio e ripristino. Quando si installano i programmi su licenza OS/400, l'autorizzazione pubblica per i comandi RSTxxx è *EXCLUDE. L'autorizzazione pubblica per i comandi SAVxxx è *USE.

Considerare di modificare l'autorizzazione pubblica per i comandi SAVxxx su *EXCLUDE. Limitare con attenzione gli utenti che si autorizzano ai comandi RSTxxx.

- Utilizzare il valore di sistema QALWOBJRST per limitare il ripristino di programmi stato del sistema, programmi che adottano l'autorizzazione e oggetti con errori di convalida.
- Utilizzare il valore di sistema QVFYOBJRST per controllare il ripristino di oggetti firmati sul sistema..
- Utilizzare il valore di sistema QFRCCVNRST per controllare la nuova creazione di alcuni oggetti ripristinati sul sistema.
- Utilizzare il controllo di sicurezza per monitorare le operazioni di ripristino. Includere *SAVRST nel valore di sistema QAUDLVL e stampare periodicamente i record di controllo creati dalle operazioni di ripristino. (Il capitolo 9 e l'Appendice F del manuale *Riferimenti alla sicurezza iSeries* forniscono ulteriori informazioni sulle operazioni delle voci di controllo).

Controllo degli oggetti utente nelle librerie protette

Ogni lavoro server iSeries ha un elenco librerie. L'elenco librerie stabilisce la sequenza in base alla quale il sistema ricerca un oggetto se non viene specificato un nome libreria con il nome oggetto. Ad esempio, quando si chiama un un programma senza specificare dove è ubicato, il sistema effettua una ricerca nell'elenco librerie secondo l'ordine ed esegue la prima copia del programma individuata.

Il manuale *Riferimenti alla sicurezza iSeries* fornisce ulteriori informazioni sui rischi per la sicurezza degli elenchi librerie e del chiamare programmi senza specificare un nome libreria (detta **chiamata non qualificata**). Fornisce anche suggerimenti per controllare il contenuto degli elenchi librerie e la capacità di modificare gli elenchi librerie del sistema.

Per un corretto funzionamento del sistema, certe librerie di sistema, come ad esempio QSYS e QGPL, devono trovarsi nell'elenco librerie di ogni lavoro. Si dovrebbe utilizzare l'autorizzazione all'oggetto per controllare chi può aggiungere programmi in queste librerie. Questo aiuta ad impedire che qualcuno inserisca un programma falso in una di queste librerie con lo stesso nome di un programma che compare in una libreria successiva nell'elenco librerie.

Si dovrebbe anche valutare chi dispone dell'autorizzazione al comando CHGSYSLIBL e monitorare i record SV nel giornale controllo sicurezza. Un utente malintenzionato potrebbe inserire una libreria prima di QSYS nell'elenco librerie e fare sì che altri utenti eseguano comandi non autorizzati con gli stessi nomi dei comandi forniti da IBM.

Opzioni menu SECBATCH:
28 *per l'inoltro immediato* **67** *per utilizzare il programma di pianificazione lavoro*

E' possibile utilizzare il comando Stampa oggetti utente (PRTUSROBJ) per stampare un elenco di oggetti utente (oggetti non creati da IBM) in una libreria specificata. E' possibile quindi valutare i programmi nell'elenco per stabilire chi li ha creati e quali funzioni eseguono.

Gli oggetti utente diversi dai programmi possono anche rappresentare un rischio per la sicurezza quando si trovano nelle librerie di sistema. Ad esempio, se un programma scrive dati riservati in un file il cui nome non è completo, tale programma potrebbe essere ingannato con l'apertura di una versione falsa di quel file in una libreria di sistema.

Capitolo 10. Prevenzione e rilevazione di tentativi di violazione

Queste informazioni costituiscono una raccolta di suggerimenti di vario genere per aiutare l'utente a individuare i potenziali rischi di sicurezza e i pirati informatici.

Sicurezza fisica

L'unità del sistema rappresenta un'importante risorsa aziendale e una potenziale porta nel sistema. Alcuni componenti all'interno del sistema sono di piccole dimensioni ma di grande valore. Sarebbe opportuno collocare l'unità del sistema in un'ubicazione controllata per impedire che estranei rimuovano i componenti importanti del sistema.

L'unità del sistema ha un pannello di controllo che fornisce la possibilità di eseguire le funzioni di base senza una stazione di lavoro. Ad esempio, è possibile utilizzare il pannello di controllo per effettuare le seguenti operazioni:

- Arrestare il sistema.
- Avviare il sistema.
- Caricare il sistema operativo.
- Avviare le funzioni di servizio.

Tutte queste attività possono disturbare gli utenti del sistema. Rappresentano inoltre un potenziale rischio di sicurezza sul sistema. E' possibile utilizzare la chiave di blocco fornita con il sistema per controllare quando tali attività sono consentite. Per impedire l'utilizzo del pannello di controllo, collocare la chiave di blocco nella posizione Sicura, rimuovere la chiave e custodirla in un posto sicuro.

Note:

1. Se è necessario eseguire degli IPL remoti o una diagnostica remota sul sistema, è possibile che sia necessario scegliere un'altra impostazione per la chiave di blocco. L'argomento Informazioni preliminari nell'iSeries Information Center fornisce ulteriori informazioni sulle impostazioni della chiave di blocco (consultare "Requisiti necessari e informazioni correlate" a pagina xii per dettagli).
2. Non tutti i modelli di sistema vengono forniti con una chiave di blocco come funzione standard.

Monitoraggio dell'attività del profilo utente

I profili utente forniscono una possibilità di entrare nel sistema. I parametri nel profilo utente determinano l'ambiente dell'utente e le caratteristiche di sicurezza dell'utente. Come responsabile della sicurezza, è necessario controllare le modifiche che si verificano sui profili utente del sistema.

E' possibile impostare il controllo di sicurezza in modo che il sistema scriva un record di modifiche sui profili utente. E' possibile utilizzare il comando DSPAUDJRNE per stampare un documento di tali modifiche.

E' possibile creare dei programmi di uscita per valutare le azioni richieste sui profili utente. La Tabella 16 a pagina 90 visualizza i punti di uscita disponibili per i comandi del profilo utente.

© Copyright IBM Corp. 1996, 2004

Tabella 16. Punti di uscita per l'attività del profilo utente

Comando profilo utente	Nome punto di uscita
Creazione Profilo utente (CRTUSRPRF)	QIBM_QSY_CRT_PROFILE
Modifica profilo utente (CHGUSRPRF)	QIBM_QSY_CHG_PROFILE
Cancellazione profilo utente (DLTUSRPRF)	QIBM_QSY_DLT_PROFILE
Ripristino profilo utente (RSTUSRPRF)	QIBM_QSY_RST_PROFILE

Il programma di uscita può, per esempio, ricercare le modifiche che potrebbero fare sì che l'utente esegua una versione non autorizzata di un programma. E' possibile che tali modifiche assegnino una descrizione lavoro differente o una nuova libreria corrente. E' possibile inoltre che il programma di uscita invii notifica a una coda messaggi o intraprenda un'azione (come la modifica o la disabilitazione del profilo utente) in base alle informazioni che il programma di uscita riceve.

Il manuale *Riferimenti alla sicurezza iSeries* fornisce ulteriori informazioni circa i programmi di uscita per le azioni del profilo utente.

Firma oggetto

Tutte le precauzioni per la sicurezza applicate sono insignificanti se esiste la possibilità che qualcuno le possa evitare introducendo dati manomessi nel sistema. Il server iSeries dispone di numerose funzioni incorporate che è possibile utilizzare per impedire che il software manomesso venga caricato sul sistema e per rilevare un software di tale tipo già presente sul sistema. Una delle tecniche aggiunte in V5R1 è la firma di oggetti.

La firma di oggetti è l'implementazione del server iSeries di un concetto crittografico noto come "firme digitali". L'idea è relativamente semplice: una volta che un produttore software è pronto a fornire il software ai clienti, il produttore "firma" il software. Questa firma non garantisce che il software esegua funzioni specifiche. Tuttavia, fornisce un modo per provare che il software provenga dal produttore che lo ha firmato e che il software non sia stato modificato dal momento in cui è stato prodotto e firmato. Ciò è particolarmente importante se il software è stato trasmesso tramite Internet o memorizzato su un supporto magnetico che si pensa sia stato modificato.

L'utilizzo di firme digitali fornisce all'utente maggior controllo su quale software è possibile caricare sul sistema e consente maggiore possibilità di individuare le modifiche una volta che è stato caricato. Il nuovo valore di sistema Verifica ripristino oggetto (QVFYOBJRST) fornisce un meccanismo per impostare una normativa limitativa che richiede che tutto il software caricato sul sistema sia firmato da origini software note. E' inoltre possibile scegliere una normativa più aperta e verificare semplicemente le firme, se sono presenti.

Tutto il software OS/400, così come il software per le opzioni e i programmi su licenza del server iSeries sono stati firmati da un'origine di sistema garantita. Tali firme aiutano il sistema a proteggere la propria integrità e vengono controllate quando si applicano le correzioni al sistema per accertarsi che la correzione provenga da un'origine di sistema garantita e che non sia stata modificata durante il trasferimento. E' inoltre possibile controllare tali firme una volta che il software si trova sul sistema. Il comando Controllo integrità oggetto (CHKOBJITG) è stato espanso per controllare le firme oltre ad altre funzioni di integrità degli oggetti sul

sistema. Inoltre, il DCM (Digital Certificate Manager) dispone di pannelli che è possibile utilizzare per controllare le firme sugli oggetti, inclusi gli oggetti nel sistema operativo.

Appena firmato il sistema operativo, è possibile utilizzare le firme digitali per proteggere l'integrità del software, che è di fondamentale importanza per l'azienda. E' possibile acquistare il software che è stato firmato da un fornitore software o è possibile firmare il software che è stato acquistato o scritto. E' possibile che parte della normativa di sicurezza utilizzi periodicamente CHKOBJITG o il DCM (Digital Certificate Manager), per verificare che le firme su tale software siano ancora valide —che gli oggetti non siano stati modificati dal momento in cui sono stati firmati. E' possibile inoltre richiedere che tutto il software ripristinato sul sistema sia firmato dall'utente o da un'origine nota. Tuttavia, dal momento che il software del server iSeries che non è prodotto da IBM non è firmato correntemente, ciò potrebbe essere troppo limitativo per il sistema. Il nuovo supporto di firma digitale fornisce la flessibilità di decidere qual è il modo migliore per proteggere l'integrità del proprio software.

Le firme digitali che proteggono il software rappresentano soltanto uno degli utilizzo dei certificati digitali. Per ulteriori informazioni sulla gestione dei certificati digitali, consultare l'argomento Gestione certificato digitale nell'Information Center (consultare "Requisiti necessari e informazioni correlate" a pagina xii per dettagli).

Monitoraggio delle descrizioni del sottosistema

Quando si avvia un sottosistema su un server iSeries, il sistema crea un ambiente di lavoro per entrare nel sistema ed eseguirlo. Una descrizione sottosistema definisce l'aspetto dell'ambiente. Le descrizioni sottosistema, quindi, possono fornire una possibilità per utenti malintenzionati. Un utente malintenzionato potrebbe utilizzare una descrizione sottosistema per avviare automaticamente un programma o per rendere possibile il collegamento senza un profilo utente.

Quando si esegue il comando Revoca autorizzazione pubblica, (RVKPUBAUT), il sistema imposta l'autorizzazione pubblica ai comandi di descrizione del sottosistema su *EXCLUDE. Ciò impedisce agli utenti che non sono autorizzati in modo specifico (e che non dispongono dell'autorizzazione speciale *ALLOBJ) di modificare o creare le descrizioni del sottosistema.

Gli argomenti riportati di seguito forniscono suggerimenti per esaminare le descrizioni del sottosistema che esistono correntemente sul sistema. E' possibile utilizzare il comando Gestione descrizioni sottosistemi (WRKSBSD) per creare un elenco di tutte le descrizioni del sottosistema. Quando si seleziona 5 (Visualizzazione) dall'elenco, viene visualizzato un menu per la descrizione sottosistema selezionata. Esso contiene un elenco delle parti di un ambiente sottosistema.

Si selezionano le opzioni per visualizzare i dettagli relativi alle parti. Utilizzare il comando Modifica descrizione sottosistema (CHGSBSD) per modificare le prime due voci sul menu. Per modificare altre voci, utilizzare il comando di aggiunta, rimozione o modifica appropriato per il tipo di voce. Ad esempio, per modificare una voce della stazione di lavoro, utilizzare il comando Modifica voce della stazione di lavoro (CHGWSE).

Il manuale *Work Management* fornisce ulteriori informazioni sulla gestione delle descrizioni sottosistema. Esso elenca inoltre i valori indicati per le descrizioni del sottosistema fornite da IBM.

Voci di avvio automatico lavoro

Una voce di avvio automatico lavoro contiene il nome di una descrizione lavoro. La descrizione lavoro potrebbe contenere dati di richiesta (RQSDTA) che causano l'esecuzione di un programma o di un comando. Ad esempio, è possibile che RQSDTA sia `CALL LIB1/PROGRAM1`. Ad ogni avvio del sottosistema, il sistema eseguirà il programma PROGRAM1 nella libreria LIB1.

Esaminare le voci di avvio automatico lavoro e le descrizioni lavoro associate. Accertarsi di avere compreso la funzione di qualsiasi programma da eseguire automaticamente all'avvio di un sottosistema.

Nomi e tipi di stazioni di lavoro

Quando viene avviato un sottosistema, ad esso si assegnano tutte le stazioni di lavoro non assegnate che sono elencate (in modo specifico o generico) nelle relative voci per i nomi e i tipi di stazioni di lavoro. Quando un utente si collega, il collegamento avviene al sottosistema a cui è assegnata la stazione di lavoro.

La voce della stazione di lavoro indica quale descrizione lavoro verrà utilizzata all'avvio del lavoro in tale ubicazione. E' possibile che la descrizione lavoro contenga i dati di richiesta che causano l'esecuzione di un programma o un comando. Ad esempio, il parametro RQSDTA potrebbe essere `CALL LIB1/PROGRAM1`. Ogni qualvolta un utente si collega a una stazione di lavoro in tale sottosistema, il sistema eseguirà PROGRAM1 in LIB1.

Esaminare le voci della stazione di lavoro e le descrizioni lavoro associate. Accertarsi che nessuno abbia aggiunto o aggiornato alcuna voce per eseguire i programmi di cui non si è a conoscenza.

E' possibile che una voce della stazione di lavoro specifichi inoltre un profilo utente predefinito. Per alcune configurazioni del sottosistema, ciò consente il collegamento semplicemente premendo il tasto Invio. Se il livello di sicurezza (valore di sistema QSECURITY) sul sistema è inferiore a 40, sarebbe opportuno esaminare le voci della stazione di lavoro per gli utenti predefiniti.

Voci di una coda lavori

Quando viene avviato un sottosistema, ad esso si assegnano tutte le code lavori elencate nella descrizione del sottosistema. Le voci della coda lavori non presentano alcun rischio diretto per la sicurezza. Tuttavia, danno la possibilità a dei malintenzionati di manomettere il sistema modificandone le prestazioni, causando l'esecuzione dei lavori in ambienti non pianificati.

Sarebbe opportuno esaminare periodicamente le voci della coda lavori nelle descrizioni del sottosistema per accertarsi che i lavori batch siano in esecuzione dove previsto.

Voci di instradamento

Una voce di instradamento definisce l'attività di un lavoro una volta immesso nel sottosistema. Il sottosistema utilizza le voci di instradamento per tutti i tipi di lavoro: lavori batch, interattivi e di comunicazioni. Una voce di instradamento specifica quanto segue:

- La classe del lavoro. Come le voci della coda lavori, la classe associata a un lavoro può influenzarne le relative prestazioni ma non rappresenta un rischio per la sicurezza.
- Il programma in esecuzione all'avvio del lavoro. Esaminare le voci di instradamento e accertarsi che nessuno abbia aggiunto o aggiornato alcuna voce per eseguire programmi di cui non si è a conoscenza.

Voci di comunicazioni e nomi ubicazione remota

Quando un lavoro di comunicazioni viene immesso sul sistema, il sistema utilizza le voci di comunicazioni e le voci nome ubicazione remota nel sottosistema attivo per stabilire in che modo tale lavoro verrà eseguito. Esaminare i seguenti punti relativi a queste voci:

- Tutti i sottosistemi possono eseguire i lavori di comunicazioni. Se un sottosistema pensato per le comunicazioni non è attivo, è possibile che un lavoro che tenta di accedere al sistema rilevi una voce in un'altra descrizione del sottosistema che corrisponda alle sue esigenze. E' necessario esaminare le voci in tutte le descrizioni del sottosistema.
- Una voce di comunicazioni contiene una descrizione lavoro. E' possibile che la descrizione lavoro contenga dati di richiesta che causano l'esecuzione di un programma o un comando. Esaminare le voci di comunicazioni e le descrizioni lavoro associate per accertarsi di comprendere la modalità di avvio dei lavori.
- Una voce di comunicazioni specifica inoltre un profilo utente predefinito che il sistema utilizza in alcune situazioni. Accertarsi di comprendere il ruolo dei profili predefiniti. Se il sistema contiene dei profili predefiniti, sarebbe opportuno accertarsi che tali profili abbiano un'autorizzazione minima. Consultare il Capitolo 12, "Comunicazioni APPC protette" per ulteriori informazioni sui profili utente predefiniti.

  E' possibile utilizzare il comando Stampa descrizione sottosistema (PRTSBSDAUT) per identificare le voci di comunicazioni che specificano un nome profilo utente.

Voci lavoro di preavvio

E' possibile utilizzare le voci di preavvio lavoro per rendere un sottosistema pronto per alcuni tipi di lavori in modo che vengano avviati più rapidamente. E' possibile che il preavvio dei lavori inizi all'avvio del sottosistema o secondo le necessità. Una voce di preavvio lavoro specifica quanto segue:

- Un programma da eseguire

  Un profilo utente predefinito

  Una descrizione lavoro

Tutti gli elementi sopra citati presentano rischi per la sicurezza. Sarebbe opportuno accertarsi che le voci di preavvio lavoro eseguano soltanto funzioni pianificate e autorizzate.

Lavori e descrizioni lavoro

Le descrizioni lavoro contengono dati di richiesta e dati di instradamento che potrebbero causare l'esecuzione di un programma specifico al momento dell'utilizzo di tale descrizione lavoro. Quando la descrizione lavoro specifica un programma nel parametro dati di richiesta, il sistema esegue il programma. Quando la descrizione lavoro specifica dati di instradamento, il sistema esegue il programma specificato nella voce di instradamento che corrisponde a tali dati.

Il sistema utilizza le descrizioni lavoro sia per i lavori batch che interattivi. Per i lavori interattivi, la voce della stazione di lavoro specifica la descrizione lavoro. Normalmente, il valore della voce della stazione di lavoro è *USRPRF, quindi il sistema utilizza la descrizione lavoro specificata nel profilo utente. Per i lavori batch, si specifica la relativa descrizione quando si inoltra il lavoro.

Sarebbe opportuno esaminare periodicamente le descrizioni lavoro per accertarsi che non eseguano programmi non pianificati. Sarebbe inoltre opportuno utilizzare l'autorizzazione all'oggetto per impedire modifiche alle descrizioni lavoro. L'autorizzazione *USE è sufficiente per eseguire un lavoro con una descrizione lavoro. Per un utente tipico non è necessaria l'autorizzazione *CHANGE alle descrizioni lavoro.

opzioni del menu SECBATCH:
15 *per l'inoltro immediato* **54** *per utilizzare il programma di pianificazione lavoro*

Le descrizioni lavoro possono inoltre specificare sotto quale profilo utente va eseguito il lavoro. Con il livello di sicurezza 40 e superiore, è necessario avere l'autorizzazione *USE alla descrizione lavoro e al profilo utente specificato nella descrizione lavoro. Con i livelli di sicurezza inferiori a 40, è necessaria l'autorizzazione *USE soltanto alla descrizione lavoro.

E' possibile utilizzare il comando Stampa autorizzazione descrizione lavoro (PRTJOBDAUT) per stampare un elenco di descrizioni lavoro che specificano dei profili utente e dispongono di autorizzazione pubblica *USE.

La documentazione visualizza le autorizzazioni speciali del profilo utente specificato nella descrizione lavoro. La documentazione include le autorizzazioni speciali di qualsiasi profilo gruppo di cui dispone il profilo utente. E' possibile utilizzare il seguente comando per visualizzare le autorizzazioni private del profilo utente:

```
DSPUSRPRF USRPRF(nome-profilo) TYPE(*OBJAUT)
```

La descrizione lavoro specifica l'elenco librerie che il lavoro utilizza quando viene eseguito. Se è possibile modificare un elenco librerie dell'utente, tale utente può eseguire una versione non pianificata di un programma in una libreria differente. Sarebbe opportuno esaminare periodicamente gli elenchi librerie specificati nelle descrizioni lavoro sul sistema.

Infine, sarebbe opportuno accertarsi che i valori predefiniti per il comando Inoltro lavoro (SBMJOB) e per il comando Creazione profilo utente (CRTUSRPRF) non siano stati modificati per fare riferimento a descrizioni lavoro non pianificate.

TPN (transaction program name) strutturati

Alcune richieste di comunicazioni inviano un tipo di segnale specifico al sistema. Tale richiesta è denominata **TPN (transaction program name) della struttura** poiché il nome del programma di transazione fa parte della struttura APPC per il sistema. Una richiesta di pass-through di una stazione video è un esempio di TPN della struttura. I TPN della struttura costituiscono una normale modalità di funzionamento delle comunicazioni e non rappresentano necessariamente un rischio per la sicurezza. Tuttavia, i TPN della struttura possono fornire un accesso imprevisto al sistema.

Alcuni TPN non passano un profilo sulla richiesta. Se la richiesta si associa a una voce di comunicazioni il cui utente predefinito è *SYS, è possibile avviare la richiesta sul sistema. Tuttavia, è possibile che il profilo *SYS esegua soltanto le funzioni del sistema, non le applicazioni dell'utente.

Se non si desidera l'esecuzione dei TPN della struttura con un profilo predefinito, è possibile modificare l'utente predefinito da *SYS a *NONE nelle voci di comunicazioni. "Richieste TPN strutturati" elenca i TPN della struttura e i profili utente associati.

Se non si desidera affatto l'esecuzione di un TPN specifico sul sistema, attenersi alla procedura riportata di seguito:

1. Creare un programma CL che accetta numerosi parametri. Sarebbe opportuno che il programma non eseguisse alcuna funzione. Dovrebbe semplicemente disporre delle istruzioni (DCL) Declare per i parametri e quindi terminare.
2. Aggiungere una voce di instradamento per il TPN a ciascun sottosistema che disponga di voci di comunicazioni o di voci nome ubicazione remota. Sarebbe opportuno che la voce di instradamento specificasse quanto segue:
   - Un valore *Valore di confronto* (CMPVAL) uguale al nome programma per il TPN (consultare Richieste TPN strutturati) con una posizione iniziale 37.
   - Un valore *Programma da chiamare* (PGM) uguale al nome del programma creato nella fase 1. Ciò impedisce a TPN di individuare un'altra voce di instradamento, come ad esempio *ANY.

Numerosi TPN dispongono già della relativa voce di instradamento nel sottosistema QCMN. Queste sono state aggiunte per ragioni relative alle prestazioni.

Richieste TPN strutturati

Tabella 17. Programmi e utenti per richieste TPN

Richiesta TPN	Programma	Profilo utente	Descrizione
X'30F0F8F1'	AMQCRC6A	*NONE	Coda messaggi
X'06F3F0F1'	QACSOTP	QUSER	Programma di transazione collegamento APPC
X'30F0F2D1'	QANRTP	QADSM	Configurazione APPC ADSM/400
X'30F0F1F9'	QCNPCSUP	*NONE	Cartelle condivise
X'07F0F0F1'	QCNTEDDM	QUSER	DDM
X'07F6C4C2'	QCNTEDDM	QUSER	SQL remoto–DRDA1
X'30F0F7F7'	QCQNRBAS	QSVCCS	SNA CC_Server
X'30F0F1F4'	QDXPRCV	QUSER	DSNX–ricevitore PC
X'30F0F1F3'	QDXPSEND	QUSER	DSNX–mittente PC
X'30F0F2C4'	QEVYMAIN	QUSER	Server ENVY**/400
X'30F0F6F0'	QHQTRGT	*NONE	Coda dati PC
X'30F0F8F0'	QLZPSERV	*NONE	Gestore licenza Client Access
X'30F0F1F7'	QMFRCVR	*NONE	Ricevitore messaggio PC
X'30F0F1F8'	QMFSNDR	*NONE	Mittente messaggio PC
X'30F0F6F6'	QND5MAIN	QUSER	Programma di controllo stazione di lavoro APPN 5394
DB2DRDA	QCNTEDDDM	QUSER	DB2DRDA

Tabella 17. Programmi e utenti per richieste TPN (Continua)

Richiesta TPN	Programma	Profilo utente	Descrizione
APINGD	QNMAPINGD	QUSER	APINGD
X'30F0F5F4'	QNMEVK	QUSER	Programmi di utilità per gestione sistema
X'30F0F2C1'	QNPSERVR	*NONE	Server di stampa rete PWS-I
X'30F0F7F9'	QOCEVOKE	*NONE	Calendario a sistemi incrociati
X'30F0F6F1'	QOKCSUP	QDOC	Copia indirizzario
X'20F0F0F7'	QOQSESRV	QUSER	DIA Versione 2
X'20F0F0F8'	QOQSESRV	QUSER	DIA Versione 2
X'30F0F5F1'	QOQSESRV	QUSER	DIA Versione 2
X'20F0F0F0'	QOSAPPC	QUSER	DIA Versione 1
X'30F0F0F5'	QPAPAST2	QUSER	Pass-through S/36—S/38
X'30F0F0F9'	QPAPAST2	QUSER	Pass-through stampante
X'30F0F4F6'	QPWFSTP0	*NONE	Cartelle condivise di tipo 2
X'30F0F2C8'	QPWFSTP1	*NONE	Server dei file Client Access
X'30F0F2C9'	QPWFSTP2	*NONE	Server dei file Windows** Client Access
X'30F0F6F9'	QRQSRVX	*NONE	Server con convergenza–SQL remoto
X'30F0F6F5'	QRQSRV0	*NONE	SQL remoto senza sincronizzazione
X'30F0F6F4'	QRQSRV1	*NONE	SQL remoto senza sincronizzazione
X'30F0F2D2'	QSVRCI	QUSER	SOC/CT
X'21F0F0F8'	QS2RCVR	QGATE	Ricevitore SNADS FS2
X'21F0F0F7'	QS2STSND	QGATE	Mittente SNADS FS2
X'30F0F1F6'	QTFDWNLD	*NONE	Funzione trasferimento PC
X'30F0F2F4'	QTIHNPCS	QUSER	Funzione TIE
X'30F0F1F5'	QVPPRINT	*NONE	Stampa virtuale PC
X'30F0F2D3'	QWGMTP	QWGM	Ultimedia Mail/400 Server
X'30F0F8F3'	QZDAINIT	QUSER	Server di accesso dati PWS-I
X'21F0F0F2'	QZDRCVR	QSNADS	Ricevitore SNADS
X'21F0F0F1'	QZDSTSND	QSNADS	Mittente SNADS
X'30F0F2C5'	QZHQTRG	*NONE	Server coda dati PWS-I
X'30F0F2C6'	QZRCSRVR	*NONE	Server comando remoto PWS-I
X'30F0F2C7'	QZSCSRVR	*NONE	Server centrale PWS-I

Metodi per monitorare gli eventi di sicurezza

L'impostazione della sicurezza non è un'operazione da svolgere una sola volta. E' necessario valutare costantemente sia le modifiche sul sistema che i problemi di sicurezza. Quindi, apportare le modifiche all'ambiente di sicurezza in base a quanto scoperto.

La documentazione della sicurezza consente di monitorare le modifiche rilevanti per la sicurezza che si verificano sul sistema. Di seguito vengono riportate altre funzioni del sistema che è possibile utilizzare come aiuto per individuare problemi o rischi per la sicurezza:

- Il controllo sicurezza è uno strumento efficace che è possibile utilizzare per osservare i numerosi tipi differenti di eventi rilevanti per la sicurezza che si verificano sul sistema. Ad esempio, è possibile impostare il sistema in modo che scriva un record di controllo ogni qualvolta un utente apre un particolare file di database per l'aggiornamento. E' possibile controllare tutte le modifiche ai valori di sistema. E' possibile controllare cosa accade quando gli utenti ripristinano gli oggetti.

  Il capitolo 9 nel manuale *Riferimenti alla sicurezza iSeries* fornisce informazioni complete sulla funzione di controllo sicurezza. E' possibile utilizzare il comando Modifica controllo riservatezza (CHGSECAUD) per impostare il controllo sicurezza sul sistema. E' inoltre possibile utilizzare il comando Visualizzazione voci giornale di controllo (DSPAUDJRNE) per stampare le informazioni selezionate dal giornale di controllo sicurezza.
- E' possibile creare la coda messaggi QSYSMSG per catturare i messaggi critici dell'operatore di sistema. La coda messaggi QSYSOPR riceve numerosi messaggi di importanza variabile durante tutto un tipico giorno lavorativo. E' possibile che messaggi critici rilevanti per la sicurezza vengano ignorati a causa dell'ingente volume di messaggi nella coda messaggi QSYSOPR.

  Se si crea una coda messaggi QSYSMSG nella libreria QSYS sul sistema, il sistema indirizza automaticamente alcuni messaggi critici alla coda messaggi QSYSMSG invece che alla coda messaggi QSYSOPR.

  E' possibile creare un programma per monitorare la coda messaggi QSYSMSG o è possibile assegnarla in modalità di interruzione all'utente stesso o a un altro utente garantito.

Parte 3. Comunicazioni di rete e applicazioni

© Copyright IBM Corp. 1996, 2004

Capitolo 11. Utilizzo di IFS (Integrated File System) per proteggere i file

L'IFS (integrated file system) fornisce numerose modalità per memorizzare e visualizzare le informazioni sul server iSeries. L'IFS (integrated file system) fa parte del sistema operativo OS/400 che supporta le operazioni di immissione e emissione flusso. Fornisce metodi di gestione memoria simili a (e compatibili con) i sistemi operativi del PC e ai sistemi operativi UNIX.

Con l'IFS (integrated file system), è possibile visualizzare tutti gli oggetti sul sistema dalla prospettiva di una struttura indirizzario gerarchica. Tuttavia, nella maggior parte dei casi, gli utenti visualizzano gli oggetti nel modo più comune per un particolare file system. Ad esempio, gli oggetti iSeries ″tradizionali″ si trovano nel file system QSYS.LIB. Normalmente, gli utenti visualizzano tali oggetti dalla prospettiva delle librerie. Gli utenti visualizzano solitamente gli oggetti nel file system QDLS dalla prospettiva dei documenti all'interno delle cartelle. I file system definiti dall'utente, principali (/) e QOpenSys presentano una struttura di indirizzari (nidificati) gerarchici.

Come responsabile della sicurezza, è necessario comprendere quanto segue:

- Quali file system vengono utilizzati sul sistema
- Le caratteristiche univoche di sicurezza di ciascun file system

Gli argomenti riportati di seguito forniscono alcune considerazioni generali per la sicurezza dell'IFS (integrated file system).

L'approccio dell'IFS (Integrated File System) alla sicurezza

Il file system principale funziona come un ombrello (o fondamenta) per tutti gli altri file system sui server iSeries. A un elevato livello, fornisce una vista integrata di tutti gli oggetti sul sistema. Altri file system che possono esistere sui server iSeries forniscono vari approcci all'integrazione e alla gestione di oggetti, in base allo scopo di fondo di ciascun file system. Il file system (ottico) QOPT, ad esempio, consente alle applicazioni e ai server iSeries (incluso il server dei file iSeries Access per Windows) di accedere all'unità CD-ROM sul server iSeries. Allo stesso modo, il file system QFileSvr.400 consente alle applicazioni di accedere ai dati IFS (integrated file system) sui server remoti iSeries. Il server dei file QLANSrv consente l'accesso ai file memorizzati su Integrated xSeries Server for iSeries o ad altri server collegati alla rete.

L'approccio di sicurezza per ciascun file system dipende dai dati che il file system rende disponibili. Il file system QOPT, ad esempio, non fornisce sicurezza a livello di oggetti, poiché non esiste alcuna tecnologia per scrivere informazioni relative all'autorizzazione su un CD-ROM. Per il file system QFileSvr.400, il controllo di accesso si verifica sul sistema remoto (dove i file vengono fisicamente memorizzati e gestiti). Per i file system come QLANSrv, l'Integrated xSeries Server for iSeries fornisce controllo di accesso. Nonostante i differenti modelli di sicurezza, molti file system supportano una gestione di controllo accesso considerevole tramite i comandi dell'IFS (integrated file system), come ad esempio Modifica autorizzazione (CHGAUT) e Modifica proprietario (CHGOWN).

© Copyright IBM Corp. 1996, 2004

Di seguito vengono riportati una serie di suggerimenti correlati alla totalità di informazioni relative alla sicurezza dell'integrated file system. L'IFS è progettato per seguire il più fedelmente possibile gli standard POSIX. Ciò porta ad una funzionalità interessante dove l'autorizzazione del server iSeries e i permessi POSIX sono ″mescolati″:

1. Non rimuovere l'autorizzazione privata per un utente a un indirizzario di cui è proprietario, anche se tale utente è autorizzato tramite l'autorizzazione pubblica, un gruppo o un elenco di autorizzazioni. Quando si gestiscono le librerie o le cartelle nel modello di sicurezza standard del server iSeries, la rimozione dell'autorizzazione privata del proprietario ridurrebbe la quantità di informazioni sull'autorizzazione memorizzate per un profilo utente e non influenzerebbe altre operazioni. Ma, a causa della modalità in cui lo standard POSIX definisce l'eredità di permessi per gli indirizzari, il proprietario di un indirizzario appena creato avrà le stesse autorizzazioni all'oggetto per tale indirizzario che il proprietario dell'indirizzario principale ha rispetto all'indirizzario principale, anche se il proprietario dell'indirizzario appena creato ha altre autorizzazioni private per quello principale. Ciò può essere difficile da comprendere, quindi di seguito viene riportato un esempio: USERA possiede l'indirizzario /DIRA, ma le autorizzazioni private di USERA sono state rimosse. USERB ha un'autorizzazione privata per /DIRA. USERB crea l'indirizzario /DIRA/DIRB. Dal momento che USERA non ha autorizzazioni all'oggetto per /DIRA, USERB non avrà alcuna autorizzazione all'oggetto per /DIRA/DIRB. USERB non potrà ridenominare o cancellare /DIRA/DIRB senza un'ulteriore azione per modificare le autorizzazioni all'oggetto di USERB. Ciò si verifica anche durante la creazione dei file con l'API open() utilizzando l'indicatore O_INHERITMODE. Se USERB creasse un file /DIRA/FILEB, USERB non avrebbe alcuna autorizzazione all'oggetto E nessuna autorizzazioni ai dati su di esso. USERB non potrebbe scrivere sul nuovo file.
2. L'autorizzazione adottata non è rispettata dalla maggior parte dei file system fisici. Ciò include i file system principali (/), QOpenSys, QDLS e definiti dall'utente.
3. Qualsiasi oggetto è di proprietà del profilo utente che ha creato gli oggetti, anche se il campo OWNER del profilo utente è impostato su *GRPPRF.
4. Molte operazioni del file system richiedono l'autorizzazione dati *RX per qualsiasi componente del percorso, incluso l'indirizzario principale (/). Quando si presentano problemi di autorizzazione, accertarsi di controllare l'autorizzazione utente all'indirizzario principale stesso.
5. La visualizzazione o il richiamo dell'indirizzario di lavoro corrente (DSPCURDIR, getcwd(), ecc.) richiede l'autorizzazione dati *RX per ciascun componente nel percorso. Tuttavia, la modifica dell'indirizzario di lavoro corrente (CD, chdir(), ecc.) richiede soltanto l'autorizzazione dati *X per ciascun componente. Quindi, un utente può modificare l'indirizzario di lavoro corrente per un determinato percorso e poi non essere in grado di visualizzare il percorso.
6. Lo scopo del comando COPY è di duplicare un oggetto. Le impostazioni di autorizzazione sul nuovo file saranno le stesse dell'originale, ad eccezione del proprietario. L'intento del comando CPYTOSTMF, tuttavia, è semplicemente di duplicare i dati. Le impostazioni di autorizzazione sul nuovo file non possono essere controllate dall'utente. Il creatore/proprietario avrà l'autorizzazione dati *RWX, ma le autorizzazioni di gruppo e pubblica saranno *EXCLUDE. E' necessario che l'utente utilizzi altri mezzi (CHGAUT, chmod(), ecc.) per assegnare le autorizzazioni desiderate.
7. E' necessario che un utente sia il proprietario o disponga dell'autorizzazione oggetto *OBJMGT a un oggetto per richiamare le informazioni

sull'autorizzazione relative all'oggetto. Queste vengono visualizzate in ubicazioni impreviste, come COPY, che deve richiamare le informazioni sull'autorizzazione nell'oggetto di origine per impostare le autorizzazioni equivalenti nell'oggetto di destinazione.

8. Quando si modifica il proprietario o il gruppo di un oggetto, l'utente non deve disporre soltanto dell'autorizzazione appropriata all'oggetto, ma deve anche avere l'autorizzazione dati *ADD per il nuovo profilo utente gruppo/proprietario e l'autorizzazione dati *DELETE per il precedente profilo gruppo/proprietario. Tali autorizzazioni dati non sono correlate alle autorizzazioni dati del file system. E' possibile visualizzarle utilizzando il comando DSPOBJAUT e modificarle con il comando EDTOBJAUT. Anche queste vengono visualizzate in modo imprevisto su COPY quando tenta di impostare l'ID gruppo per un nuovo oggetto.
9. Il comando MOV tenta di risolvere errori relativi all'autorizzazione, soprattutto durante lo spostamento da un file system fisico a un altro o durante l'esecuzione di una conversione dati. In tali casi, lo spostamento diventa effettivamente un'operazione di copia e cancellazione. Quindi, tutte le considerazioni sull'autorizzazione che riguardano il comando COPY (vedere punti 7 e 8 riportati in precedenza) e il comando RMVLNK si applicano anche al comando MOV, oltre ad altre specifiche considerazioni su MOV.

Le sezioni seguenti forniscono ulteriori considerazioni per numerosi file system rappresentativi. Per ulteriori informazioni su un file system specifico sul server iSeries, sarà necessario consultare la documentazione per il programma su licenza che utilizza il file system.

File system principali (/), QOpenSys e definiti dall'utente

Di seguito vengono riportate delle considerazioni sulla sicurezza per i file system principali, QOpenSys e definiti dall'utente.

Funzionamento dell'autorizzazione

I file system principali, QOpenSys e definiti dall'utente forniscono una serie di funzioni PC, UNIX** e server iSeries sia per la gestione oggetto che per la sicurezza. Quando si utilizzano i comandi IFS (integrated file system) da una sessione del server iSeries (WRKAUT e CHGAUT), è possibile impostare tutte le normali autorizzazioni all'oggetto del server iSeries. Ciò include le autorizzazioni *R, *W e *X compatibili con Spec 1170 (sistemi operativi di tipo UNIX).

Nota: i file system principali, QOpenSys e definiti dall'utente sono funzionalmente equivalenti. Il file system QOpenSys è sensibile al maiuscolo e al minuscolo. Il file system principale non lo è. I file system definiti dall'utente possono essere definiti sensibili al maiuscolo e al minuscolo. Dal momento che tali file system hanno le stesse caratteristiche di sicurezza, è possibile presupporre che, negli argomenti riportati di seguito, i loro nomi vengano utilizzati in modo interscambiabile.

Quando si accede al file system principale come amministratore da una sessione PC, è possibile impostare gli attributi dell'oggetto che il PC utilizza per limitare alcuni tipi di accesso:
- Sistema
- Nascosto
- Archivio
- Di sola lettura

Tali attributi PC sono un'aggiunta, non delle sostituzioni, per i valori di autorizzazione all'oggetto del server iSeries.

Quando un utente tenta di accedere a un oggetto nel file system principale, OS/400 applica tutti i valori di autorizzazione all'oggetto e gli attributi per l'oggetto, indipendentemente dal fatto che tali autorizzazioni siano ″visibili″ o meno dall'interfaccia utente. Ad esempio, supponiamo che l'attributo di sola lettura per un oggetto sia impostato su attivato. Un utente PC non può cancellare l'oggetto tramite l'interfaccia iSeries Access. Neanche un utente del server iSeries con una stazione di lavoro a funzione fissa può cancellare l'oggetto, anche se tale utente del server iSeries ha l'autorizzazione speciale *ALLOBJ. Prima di potere cancellare l'oggetto, è necessario che un utente autorizzato utilizzi una funzione PC per reimpostare il valore di sola lettura su `disattivato`. In modo simile, è possibile che un utente PC non abbia sufficiente autorizzazione OS/400 per modificare gli attributi di sicurezza di un oggetto rilevanti per il PC.

Le applicazioni di tipo UNIX eseguite sui server iSeries utilizzano API di tipo UNIX per accedere ai dati nel file system principale. Con API di tipo UNIX, le applicazioni possono riconoscere e conservare le seguenti informazioni sulla sicurezza:
- Proprietario oggetto
- Proprietario gruppo (autorizzazione gruppo principale server iSeries)
- Lettura (file)
- Scrittura (modifica contenuto)
- Esecuzione (esecuzione di programmi o ricerca indirizzari)

Il sistema mette in corrispondenza tali autorizzazioni dati alle autorizzazioni dati e oggetto del server iSeries esistenti:
- Lettura (*R) = *OBJOPR e *READ
- Scrittura (*W) = *OBJOPR, *ADD, *UPD, *DLT
- Esecuzione (*X) = *OBJOPR e *EXECUTE

I concetti per le altre autorizzazioni all'oggetto (*OBJMGT, *OBJEXIST, *OBJALTER e *OBJREF) non esistono in un ambiente di tipo UNIX.

Tuttavia, tali autorizzazioni all'oggetto esistono per tutti gli oggetti nel file system principale. Quando si crea un oggetto utilizzando un'API di tipo UNIX, l'oggetto eredita tali autorizzazioni dall'indirizzario principale, dando come risultato quanto segue:
- Il nuovo proprietario dell'oggetto ha la stessa autorizzazione all'oggetto del proprietario dell'indirizzario principale.
- Il nuovo gruppo principale dell'oggetto ha la stessa autorizzazione all'oggetto del gruppo principale dell'indirizzario.
- I nuovi utenti pubblici hanno la stessa autorizzazione all'oggetto degli utenti pubblici dell'indirizzario principale.

La nuova autorizzazione dati dell'oggetto per proprietario, gruppo principale e utenti pubblici viene specificata sull'API con parametro modalità. Quando tutte le autorizzazioni all'oggetto sono impostate su 'attivato', si acquisisce la funzionalità di autorizzazioni che ci si aspetterebbe in un ambiente di tipo UNIX. E' preferibile lasciare queste impostate su 'attivato' a meno che non si desideri una funzionalità di tipo POSIX.

Quando si eseguono applicazioni che utilizzano API di tipo UNIX, il sistema applica tutte le autorizzazioni all'oggetto indipendentemente dal fatto che siano

visibili o meno sulle applicazioni di tipo UNIX. Ad esempio, il sistema applicherà l'autorizzazione relativa agli elenchi di autorizzazioni anche se il concetto di elenchi di autorizzazioni non esiste nei sistemi operativi di tipo UNIX.

Quando si dispone di un ambiente con applicazioni miste, è necessario accertarsi che non si apportino modifiche alle autorizzazioni in un ambiente che interromperanno le applicazioni in un altro ambiente.

Gestione della sicurezza per i file sistemi principali (/), QOpenSys e definiti dall'utente

Con l'introduzione dell'IFS (integrated file system), i server iSeries forniscono inoltre una nuova serie di comandi per la gestione di oggetti in più file system. Questa serie di comandi include i comandi per gestire la sicurezza:

- Modifica controllo (CHGAUD)
- Modifica autorizzazione (CHGAUT)
- Modifica proprietario (CHGOWN)
- Modifica gruppo principale (CHGPGP)
- Visualizzazione autorizzazione (DSPAUT)
- Gestione autorizzazione (WRKAUT)

Tali comandi raggruppano i dati sottostanti e le autorizzazioni all'oggetto nelle sottoserie di autorizzazioni di tipo UNIX.

***RWX** Lettura/scrittura/esecuzione
***RW** Lettura/scrittura
***R** Lettura
***WX** Scrittura/esecuzione
***W** Scrittura
***X** Esecuzione

Inoltre, le API di tipo UNIX sono disponibili per gestire la sicurezza.

Autorizzazione pubblica all'indirizzario principale

Quando viene fornito il sistema, l'autorizzazione pubblica all'indirizzario principale è *ALL (tutte le autorizzazioni all'oggetto e ai dati). Tale impostazione fornisce flessibilità e compatibilità sia con le aspettative delle applicazioni di tipo UNIX che con le aspettative degli utenti tipici del server iSeries. Un utente del server iSeries che dispone delle funzioni della riga comandi può creare una nuova libreria nel file system QSYS.LIB semplicemente utilizzando il comando CRTLIB. Normalmente, l'autorizzazione su un server iSeries tipico consente ciò. In modo simile, con l'impostazione fornita per il file system principale, un utente tipico può creare un nuovo indirizzario nel file system principale (allo stesso modo in cui è possibile creare un nuovo indirizzario sul PC).

Come responsabile della sicurezza, è necessario istruire gli utenti sulla protezione adeguata degli oggetti creati. Quando un utente crea una libreria, probabilmente l'autorizzazione pubblica alla libreria non dovrebbe essere *CHANGE (valore predefinito). L'utente dovrebbe impostare l'autorizzazione pubblica su *USE o su *EXCLUDE, a seconda del contenuto della libreria.

Se è necessario che gli utenti creino nuovi indirizzari nei file system principale (/), QOpenSys o definito dall'utente, sono disponibili numerose opzioni di sicurezza:

- E' possibile consigliare agli utenti di sostituire l'autorizzazione predefinita quando creano nuovi indirizzari. Il valore predefinito è ereditare l'autorizzazione dall'indirizzario principale immediato. Nel caso di un indirizzario appena creato nell'indirizzario principale, per impostazione predefinita l'autorizzazione pubblica sarà *ALL.

- E' possibile creare un sottoindirizzario ″principale″ sotto l'indirizzario principale. Impostare l'autorizzazione pubblica in quell'indirizzario principale su un'impostazione appropriata per la propria azienda. Quindi consigliare agli utenti di creare qualsiasi nuovo indirizzario personale in tale sottoindirizzario principale. I nuovi indirizzari erediteranno la relativa autorizzazione.
- E' possibile considerare la modifica dell'autorizzazione pubblica per l'indirizzario principale per impedire agli utenti di creare oggetti in tale indirizzario. (Rimuovere le autorizzazioni *W, *OBJEXIST, *OBJALTER, *OBJREF e *OBJMGT.) Tuttavia, è necessario valutare se tale modifica causerà dei problemi per qualcuna delle applicazioni. E' possibile, ad esempio, disporre di applicazioni di tipo UNIX che si prevede possano cancellare gli oggetti dall'indirizzario principale.

Comando Stampa autorizzazioni private (PRTPVTAUT)

Il comando Stampa autorizzazioni private (PRTPVTAUT) consente di stampare una documentazione di tutte le autorizzazioni private per gli oggetti di un tipo specificato in un indirizzario, cartella o libreria specificati. La documentazione elenca tutti gli oggetti del tipo specificato e gli utenti autorizzati all'oggetto. Questo è un modo per controllare le differenti origini di autorizzazione agli oggetti.

Questo comando stampa tre prospetti per gli oggetti selezionati. La prima documentazione (documentazione completa) contiene tutte le autorizzazioni private per ciascuno degli oggetti selezionati. La seconda documentazione (documentazione modificata) contiene aggiunte e modifiche alle autorizzazioni private agli oggetti selezionati se il comando PRTPVTAUT era stato eseguito precedentemente per gli oggetti specificati nella libreria, cartella o indirizzario specificati. Qualsiasi nuovo oggetto del tipo selezionato, le nuove autorizzazioni agli oggetti esistenti o le modifiche alle autorizzazioni esistenti agli oggetti esistenti vengono elencate nella 'Documentazione modificata'. Se il comando PRTPVTAUT non era stato eseguito precedentemente per gli oggetti specificati nella libreria, cartella o indirizzario specificati, non esisterà alcuna 'Documentazione modificata'. Se il comando è stato eseguito precedentemente, ma non è stata apportata alcuna modifica alle autorizzazioni sugli oggetti, la 'Documentazione modificata' viene stampata, ma non esiste alcun oggetto elencato.

La terza documentazione (Documentazione cancellata) contiene qualsiasi cancellazione di utenti autorizzati privatamente dagli oggetti specificati dalla precedente esecuzione del comando PRTPVTAUT. Qualsiasi oggetto cancellato o utente rimosso come utente autorizzato privatamente viene elencato come 'Documentazione cancellata'. Se il comando PRTPVTAUT non era stato eseguito precedentemente, non esisterà alcuna 'Documentazione cancellata'. Se il comando è stato eseguito precedentemente, ma non è stata eseguita alcuna operazione di cancellazione sugli oggetti, la 'Documentazione cancellata' viene stampata, ma non esiste alcun oggetto elencato.

Limitazione: è necessario disporre dell'autorizzazione speciale *ALLOBJ per utilizzare tale comando.

Esempi:

Questo comando crea le documentazioni completa, modificata e cancellata per tutti gli oggetti file nella PAYROLLLIB:

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

Questo comando crea le documentazioni completa, modificata e cancellata per tutti gli oggetti del file di flusso nell'indirizzario Garry:

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

Questo comando crea le documentazioni completa, modificata e cancellata per tutti gli oggetti del file di flusso nella struttura del sottoindirizzario che inizia nell'indirizzario Garry:

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

Comando Stampa oggetti autorizzati pubblicamente (PRTPUBAUT)

Il comando Stampa oggetti autorizzati pubblicamente (PRTPUBAUT) consente di stampare una documentazione degli oggetti specificati che non dispongono di autorizzazione pubblica *EXCLUDE. Per gli oggetti *PGM, soltanto i programmi che non dispongono di autorizzazione pubblica *EXCLUDE che un utente può chiamare (il programma è un dominio utente o il livello di sicurezza del sistema (valore di sistema QSECURITY) è 30 o un valore inferiore) verranno inclusi nella documentazione. Questo è un modo per controllare gli oggetti a cui ogni utente sul sistema è autorizzato ad accedere.

Questo comando stamperà due documentazioni. La prima documentazione (Documentazione completa) conterrà tutti gli oggetti specificati che non dispongono di autorizzazione pubblica *EXCLUDE. La seconda documentazione (Documentazione modificata) conterrà gli oggetti che ora non dispongono di autorizzazione pubblica di *EXCLUDE, che disponevano di autorizzazione pubblica *EXCLUDE o che non esistevano durante la precedente esecuzione del comando PRTPUBAUT. Se il comando PRTPUBAUT non era stato eseguito precedentemente per gli oggetti, la libreria, la cartella o l'indirizzario specificati, non esisterà alcuna 'Documentazione modificata'. Se il comando è stato eseguito precedentemente, ma nessun oggetto aggiuntivo è privo dell'autorizzazione pubblica di *EXCLUDE, la 'Documentazione modificata' viene stampata, ma non verrà elencato alcun oggetto.

Limitazioni: è necessario disporre dell'autorizzazione speciale *ALLOBJ per utilizzare tale comando.

Esempi:

Questo comando crea le documentazioni completa e modificata per tutti gli oggetti del file nella libreria Garry che non dispongono di un'autorizzazione pubblica *EXCLUDE:

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

Questo comando crea le documentazioni completa, modificata e cancellata per tutti gli oggetti del file di flusso nella struttura del sottoindirizzario che inizia nell'indirizzario Garry che non dispongono di un'autorizzazione pubblica *EXCLUDE:

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

Limitazione dell'accesso al file system QSYS.LIB

Dal momento che il file system principale è il file system ombrello, il file system QSYS.LIB viene visualizzato come sottoindirizzario all'interno dell'indirizzario principale. Quindi, qualsiasi utente di PC con accesso al server iSeries può gestire gli oggetti memorizzati nelle librerie del server iSeries (il file system QSYS.LIB) con

azioni e comandi PC normali. Un utente del PC potrebbe, ad esempio, trascinare un oggetto QSYS.LIB (come ad esempio la libreria con i file di dati critici) nel cestino.

Come è stato spiegato in "File system principali (/), QOpenSys e definiti dall'utente" a pagina 103, il sistema applica tutte le autorizzazioni all'oggetto indipendentemente dal fatto che siano visibili o meno sull'interfaccia. Quindi, un utente non può cestinare (cancellare) un oggetto a meno che non abbia l'autorizzazione *OBJEXIST all'oggetto. Tuttavia, se iSeries dipende dalla sicurezza di accesso al menu piuttosto che dalla sicurezza dell'oggetto, l'utente del PC potrebbe scoprire molto facilmente gli oggetti nel file system QSYS.LIB disponibili per essere eliminati.

Nel momento in cui si espandono gli utilizzi del sistema e i differenti metodi di accesso forniti, si scoprirà presto che la sicurezza di accesso al menu non è sufficiente. Il Capitolo 5, "Protezione delle informazioni tramite autorizzazione oggetto", a pagina 47 discute le strategie per aggiungere al controllo accesso menu la sicurezza degli oggetti. Tuttavia, i server iSeries forniscono inoltre un semplice modo per impedire l'accesso al file system QSYS.LIB tramite la struttura dell'indirizzario del file system principale. E' possibile utilizzare l'elenco di autorizzazioni QPWFSERVER per controllare quali utenti possono accedere al file system QSYS.LIB tramite l'indirizzario principale.

Quando l'autorizzazione di un utente all'elenco di autorizzazioni QPWFSERVER è *EXCLUDE, l'utente non può accedere all'indirizzario QSYS.LIB dalla struttura dell'indirizzario principale. Quando l'autorizzazione di un utente è *USE, l'utente può accedere all'indirizzario. Una volta che l'utente ha l'autorizzazione per accedere all'indirizzario, la normale autorizzazione all'oggetto si applica per qualsiasi azione l'utente tenti di eseguire su un oggetto all'interno del file system QSYS.LIB. In altre parole, l'autorizzazione all'elenco di autorizzazioni QPWFSERVER funziona come una porta nell'intero file system QSYS.LIB. Per l'utente con autorizzazione *EXCLUDE, la porta è chiusa. Per l'utente con autorizzazione *USE (o con qualsiasi altra autorizzazione maggiore), la porta è aperta.

Per la maggior parte delle situazioni, gli utenti non hanno necessità di utilizzare un'interfaccia indirizzario per accedere agli oggetti nel file system QSYS.LIB. Probabilmente, si desidererà impostare l'autorizzazione pubblica all'elenco di autorizzazioni QPWFSERVER su *EXCLUDE. Tenere presente che tale autorizzazione all'elenco di autorizzazioni apre o chiude la porta a tutte le librerie all'interno del file system QSYS.LIB, incluse le librerie utente. Se vi sono utenti che obiettano a tale esclusione, è possibile valutare i loro requisiti su una base individuale. Se è adeguato, è possibile autorizzare in modo esplicito un singolo utente all'elenco di autorizzazioni. Tuttavia, è necessario accertarsi che l'utente disponga dell'autorizzazione appropriata agli oggetti all'interno del file system QSYS.LIB. Altrimenti, è possibile che l'utente cancelli involontariamente oggetti o intere librerie.

Note:

1. Quando viene fornito il sistema, l'autorizzazione pubblica all'elenco di autorizzazioni è *USE.
2. Se si autorizza in modo esplicito un singolo utente, l'elenco di autorizzazioni controlla l'accesso soltanto con la gestione file di iSeries Access, di NetServer e la gestione file tra server iSeries. Ciò non impedisce l'accesso agli stessi indirizzari tramite FTP, ODBC e altre reti.

Protezione indirizzari

Per accedere a un oggetto all'interno del file system principale, si legge l'intero percorso al tale oggetto. Per ricercare un indirizzario, è necessario disporre dell'autorizzazione *X (*OBJOPR e *EXECUTE) a tale indirizzario. Supponiamo, ad esempio, che si desidera accedere al seguente oggetto:

```
/companya/customers/custfile.dat
```

E' necessario disporre dell'autorizzazione *X all'indirizzario `companya` e all'indirizzario `customers`.

Con il file system principale, è possibile creare un collegamento simbolico ad un oggetto. Concettualmente, un collegamento simbolico è un alias per un nome percorso. Solitamente, è più breve e semplice da ricordare rispetto al nome percorso completo. Un collegamento simbolico non crea, tuttavia, un percorso fisico differente all'oggetto. L'utente ha comunque bisogno dell'autorizzazione *X a ciascun indirizzario e sottoindirizzario nel percorso fisico all'oggetto.

Per oggetti nel file system principale, è possibile utilizzare la sicurezza dell'indirizzario come si potrebbe utilizzare la sicurezza della libreria nel file system QSYS.LIB. E' possibile, ad esempio, impostare l'autorizzazione pubblica di un indirizzario su *EXCLUDE per impedire agli utenti pubblici di accedere agli oggetti all'interno di tale albero.

Protezione per nuovi oggetti

Quando si crea un nuovo oggetto nel file system principale, l'interfaccia che si utilizza per crearlo stabilisce le relative autorizzazioni. Ad esempio, se si utilizza il comando CRTDIR e i relativi valori predefiniti, il nuovo indirizzario eredita tutte le caratteristiche dell'autorizzazione dell'indirizzario principale, incluse le autorizzazioni private, l'autorizzazione del gruppo principale e l'associazione dell'elenco di autorizzazioni. Le seguenti sezioni descrivono in che modo vengono stabilite le autorizzazioni per ciascun tipo di interfaccia.

L'autorizzazione deriva dall'indirizzario principale immediatamente adiacente, non dagli indirizzari in posizione più elevata nell'albero. Quindi, come responsabile della sicurezza, è necessario visualizzare l'autorizzazione assegnata agli indirizzari in una gerarchia da due prospettive:

- In che modo l'autorizzazione influenza l'accesso agli oggetti nell'albero (come l'autorizzazione alla libreria).
- In che modo l'autorizzazione influenza gli oggetti appena creati (come il valore CRTAUT per le librerie).

Consiglio: è possibile che si voglia fornire agli utenti che operano nell'IFS (integrated file system) un indirizzario principale (ad esempio, /home/usrxxx), quindi impostare la sicurezza in modo appropriato (come ad esempio PUBLIC *EXCLUDE). Qualsiasi indirizzario creato dall'utente nell'indirizzario principale erediterà quindi le autorizzazioni.

Di seguito vengono riportate le descrizioni dell'eredità dell'autorizzazione per le differenti interfacce:

Utilizzo del comando Creazione indirizzario

Quando si crea un nuovo sottoindirizzario utilizzando il comando CRTDIR, sono disponibili due opzioni per specificare l'autorizzazione:

- E' possibile specificare l'autorizzazione pubblica (autorizzazione dati, autorizzazione oggetto o entrambe).
- E' possibile specificare *INDIR per l'autorizzazione dati, oggetto o per entrambe. Quando si specifica *INDIR sia per l'autorizzazione dati che oggetto, il sistema crea una copia esatta di tutte le informazioni sull'autorizzazione dall'indirizzario principale al nuovo oggetto, incluso l'elenco di autorizzazioni, il gruppo principale, l'autorizzazione pubblica e le autorizzazioni private. (Il sistema non copia l'autorizzazione privata che il profilo QSYS o QSECOFR ha all'oggetto.)

Creazione di un indirizzario con un'API

Quando si crea un indirizzario utilizzando l'API mkdir(), si specificano le autorizzazioni dati per il proprietario, il gruppo principale e gli utenti pubblici (utilizzando la definizione autorizzazione di *R, *W e *X). Il sistema utilizza le informazioni nell'indirizzario principale per impostare le autorizzazioni all'oggetto per il proprietario, il gruppo principale e gli utenti pubblici.

Dal momento che i sistemi operativi di tipo UNIX non hanno il concetto di autorizzazioni all'oggetto, l'API mkdir() non supporta la specifica di autorizzazioni all'oggetto. Se si desiderano autorizzazioni all'oggetto differenti, è possibile utilizzare il comando del server iSeries (CHGAUT). Tuttavia, quando si rimuovono alcune autorizzazioni all'oggetto, è possibile che l'applicazione di tipo UNIX non funzioni come previsto.

Creazione di un file di flusso con l'API open() o creat()

Quando si utilizza l'API creat() per creare un file di flusso, è possibile specificare le autorizzazioni dati per il proprietario, il gruppo principale e gli utenti pubblici (utilizzando le autorizzazioni di tipo UNIX *R, *W e *X). Il sistema utilizza le informazioni nell'indirizzario principale per impostare le autorizzazioni all'oggetto per il proprietario, il gruppo principale e gli utenti pubblici.

E' inoltre possibile specificare tali autorizzazioni quando si utilizza l'API open() per creare un file di flusso. In alternativa, quando si utilizza l'API open(), è possibile specificare che l'oggetto dovrebbe ereditare tutte le autorizzazioni dall'indirizzario principale. Ciò viene chiamato `modalità di eredità`. Quando si specifica la modalità di eredità, il sistema crea una corrispondenza totale per le autorizzazioni principali, incluso l'elenco di autorizzazioni, il gruppo principale, l'autorizzazione pubblica e le autorizzazioni private. Questa opzione funziona come se si specificasse *INDIR sul comando CRTDIR.

Creazione di un oggetto utilizzando un'interfaccia del PC

Quando si utilizza un'applicazione del PC per creare un oggetto nel file system principale, il sistema eredita automaticamente tutte le autorizzazioni dall'indirizzario principale. Ciò include l'elenco di autorizzazioni, il gruppo principale, l'autorizzazione pubblica e le autorizzazioni private. Le applicazioni PC non dispongono di alcun equivalente per specificare l'autorizzazione quando si crea un oggetto.

File system QFileSvr.400

Con il file system QFileSvr.400, un utente (USERX) su un sistema iSeries (SYSTEMA) può accedere ai dati su un altro sistema iSeries collegato (SYSTEMB). USERX ha un'interfaccia esattamente equivalente all'interfaccia Client Access. Il server iSeries remoto (SYSTEMB) è come un indirizzario con tutti i relativi file system come sottoindirizzari.

Quando USERX tenta di accedere a SYSTEMB con questa interfaccia, SYSTEMA invia il nome del profilo utente e la parola d'ordine codificata di USERX a SYSTEMB. E' necessario che lo stesso profilo utente e parola d'ordine esistano su SYSTEMB, altrimenti SYSTEMB rifiuta la richiesta.

Se SYSTEMB accetta la richiesta, USERX appare a SYSTEMB come qualsiasi utente Client Access. Le stesse regole di controllo autorizzazione si applicano alle azioni tentate da USERX.

Come responsabile della sicurezza, è necessario essere consapevoli che il file system QFileSvr.400 rappresenta un'altra possibile porta al sistema. Non è possibile presupporre che si stiano limitando gli utenti remoti a un collegamento interattivo con un pass-through del terminale. Se il sottosistema QSERVER è in esecuzione e il sistema è collegato a un altro sistema iSeries, gli utenti remoti possono accedere al sistema come se si trovassero su un PC locale che esegue Client Access. Con tutta probabilità, il sistema avrà un collegamento per cui è necessario che il sottosistema QSERVER sia in esecuzione. Questa è un'altra ragione per cui è essenziale un buono schema di autorizzazione all'oggetto.

File system di rete

L'NFS (Network File System - File system di rete) fornisce l'accesso a e da sistemi che hanno implementazioni NFS. NFS è un metodo standard aziendale per condividere le informazioni tra utenti su sistemi collegati in rete. La maggior parte dei sistemi operativi principali (inclusi i sistemi operativi PC) forniscono NFS. Per i sistemi UNIX, NFS è il metodo principale per accedere ai dati. I server iSeries possono funzionare sia come client NFS che come server NFS.

Quando si è un responsabile della sicurezza di un sistema iSeries che funziona come server NFS, è necessario comprendere e gestire gli aspetti della sicurezza di NFS. Di seguito vengono riportati suggerimenti e considerazioni:

- E' necessario avviare in modo esplicito la funzione del server NFS utilizzando il comando STRNFSSVR. Controllare quale utente ha l'autorizzazione a utilizzare tale comando.
- Si rende un indirizzario o un oggetto disponibile per i client NFS `esportandolo`. Quindi, si ha un controllo molto specifico su quali parti del sistema si renderanno disponibili per i client NFS nella rete.
- Quando si esegue un'esportazione, è possibile specificare quali client hanno accesso agli oggetti. Un client viene identificato tramite un nome sistema o un indirizzo IP. Un client può essere un singolo PC o un intero server iSeries o un sistema UNIX. Nella terminologia NFS, il client (indirizzo IP) viene chiamato `macchina`.
- Quando si esegue un'esportazione, è possibile specificare un accesso di sola lettura o di lettura/scrittura per ciascuna macchina che abbia accesso a un oggetto o a un indirizzario esportato. Nella maggioranza dei casi, si desidererà probabilmente fornire un accesso di sola lettura.

- NFS non fornisce protezione della parola d'ordine. E' progettato e pensato per la condivisione di dati all'interno di una comunità garantita di sistemi. Quando un utente richiede l'accesso, il server riceve l'`uid` dell'utente. Di seguito vengono riportate alcune considerazioni sull'`uid`:
  - Il server iSeries tenta di individuare un profilo utente con lo stesso `uid`. Se individua un `uid` corrispondente, utilizza le credenziali del profilo utente. Credenziali è un termine NFS per descrivere l'utilizzo dell'autorizzazione di un utente. Ciò è simile al passaggio di profili in altre applicazioni del server iSeries.
  - Quando si esporta un indirizzario o un oggetto, è possibile specificare se si consentirà l'accesso tramite profilo con autorizzazione principale. Il server NFS sui server iSeries considera l'autorizzazione principale uguale all'autorizzazione speciale *ALLOBJ. Se si specifica che non si consentirà l'autorizzazione principale, un utente NFS con uno `uid` correlato a un profilo utente con autorizzazione speciale *ALLOBJ non potrà accedere all'oggetto sotto tale profilo. Al contrario, se viene consentito un accesso anonimo, il richiedente verrà correlato al profilo anonimo.
  - Quando si esporta un indirizzario o un oggetto, è possibile specificare se si consentiranno richieste anonime. Una richiesta anonima è una richiesta con `uid` che non corrisponde ad alcun `uid` sul sistema. Se si sceglie di consentire richieste anonime, il sistema mette in corrispondenza l'utente anonimo con il profilo utente QNFSANON fornito dall'IBM. Tale profilo utente non dispone di alcuna autorizzazione speciale o esplicita. (Al momento dell'esportazione, è possibile specificare un profilo utente differente per le richieste anonime se si ritiene opportuno).
- Quando il server iSeries fa parte di una rete NFS (o in qualsiasi rete con sistemi UNIX che dipendono da `uid`), sarà probabilmente necessario gestire gli `uid` invece di lasciare che il sistema li assegni automaticamente. Sarà necessario coordinare gli `uid` con altri sistemi nella rete.

  E' possibile che ci si renda conto che è necessario modificare gli `uid` (anche per i profili utente forniti dall'IBM) in modo che siano compatibili con altri sistemi nella rete. E' disponibile un programma per rendere più semplice la modifica dell'`uid` per un profilo utente. (Quando si modifica l' `uid` per un profilo utente, è inoltre necessario modificare l'`uid` per tutti gli oggetti di proprietà del profilo nell'indirizzario principale o nell'indirizzario QOpenSrv.) Il programma QSYCHGID modifica automaticamente l'`uid` sia nel profilo utente che in tutti gli oggetti di proprietà. Per informazioni su come utilizzare tale programma, consultare il manuale *iSeries System API Reference*.

Capitolo 12. Comunicazioni APPC protette

Quando il sistema fa parte di una rete con altri sistemi, una nuova serie di porte e finestre sul sistema diventa disponibile. Come responsabile della sicurezza, è necessario conoscere le opzioni che è possibile utilizzare per controllare gli accessi al sistema in un ambiente APPC.

APPC (Advanced program-to-program communications) è un modo tramite il quale i computer, inclusi i personal computer, comunicano tra di loro. Il pass-through di una stazione video, DDM (distributed data management) e iSeries Access per Windows possono tutti utilizzare le comunicazioni APPC.

Gli argomenti seguenti forniscono le informazioni di base sulle modalità di funzionamento delle comunicazioni APPC e sulla corretta impostazione della sicurezza. Tali argomenti si concentrano principalmente sugli elementi di rilievo per la sicurezza di una configurazione APPC. Per adattare tale esempio alla propria situazione, sarà necessario collaborare con chi gestisce la rete di comunicazioni e probabilmente con i fornitori dell'applicazione. Utilizzare le presenti informazioni come aiuto per comprendere le questioni relative alla sicurezza e le opzioni disponibili per APPC.

La sicurezza non è mai "semplice". E' possibile che alcuni suggerimenti per rendere la sicurezza di rete più semplice rendano la gestione della rete più complicata. Ad esempio, le presenti informazioni non pongono l'accento su APPN (Advanced Peer-to-Peer Networking), poiché è più semplice comprendere e gestire la sicurezza senza APPN. Tuttavia, senza APPN, l'amministratore di rete deve creare manualmente le informazioni sulla configurazione che APPN crea, invece, automaticamente.

Anche i PC utilizzano le comunicazioni

Molti metodi per collegare i PC ai server iSeries dipendono dalle comunicazioni, come ad esempio APPC o TCP/IP. Leggendo i seguenti argomenti, accertarsi di considerare le questioni sulla sicurezza per collegarsi sia ad altri sistemi che ai PC. Quando si pianifica la protezione della rete, accertarsi di non influenzare in modo negativo i PC collegati al sistema.

Terminologia APPC

APPC fornisce la possibilità per un utente su un sistema di eseguire le attività su un altro sistema. Il sistema da cui viene avviata la richiesta viene chiamato in uno dei seguenti modi:

- **Sistema di origine**
- **Sistema locale**
- **Client**

Il sistema che riceve la richiesta viene chiamato in uno dei seguenti modi:

- **Sistema di destinazione**
- **Sistema remoto**
- **Server**

© Copyright IBM Corp. 1996, 2004

Elementi di base delle comunicazioni APPC

Dalla prospettiva di responsabile della sicurezza, è necessario che si verifichino le seguenti condizioni prima che un utente su un sistema (SYSTEMA) possa eseguire un'attività significativa su un altro sistema (SYSTEMB):

- E' necessario che il sistema di origine (SYSTEMA) fornisca un percorso al sistema di destinazione (SYSTEMB). Questo percorso viene chiamato **sessione APPC**.
- E' necessario che il sistema di destinazione identifichi l'utente e lo associ a un profilo utente. E' necessario che il sistema di destinazione supporti l'algoritmo di codifica del sistema di origine (consultare "Livelli di una parola d'ordine" a pagina 16 per ulteriori informazioni).
- E' necessario che il sistema di destinazione avvii un lavoro per l'utente con un ambiente appropriato (valori di gestione lavoro).

I seguenti argomenti discutono tali elementi e il modo in cui essi sono correlati alla sicurezza. Il responsabile della sicurezza sul sistema di destinazione ha la responsabilità principale per accertarsi che gli utenti APPC non violino la sicurezza. Tuttavia, quando i responsabili della sicurezza su entrambi i sistemi collaborano, il lavoro di gestione della sicurezza APPC è più semplice.

Esempio: sessione APPC di base

In un ambiente APPC, quando un utente o un'applicazione su un sistema richiede l'accesso a un altro sistema, i due sistemi impostano una sessione. Per stabilire la sessione, è necessario che i sistemi colleghino due descrizioni unità APPC corrispondenti. Il parametro relativo al nome dell'ubicazione remota (RMTLOCNAME) nella descrizione unità SYSTEMA deve corrispondere al parametro relativo al nome dell'ubicazione locale (LCLLOCNAME) nella descrizione unità SYSTEMB e viceversa.

Affinché i due sistemi stabiliscano una sessione APPC, è necessario che le parole d'ordine dell'ubicazione nelle descrizioni unità APPC su SYSTEMA e SYSTEMB siano identiche. Entrambe devono specificare *NONE o lo stesso valore.

Se le parole d'ordine sono un valore diverso da *NONE, vengono memorizzate e trasmesse in formato codificato. Se le parole d'ordine corrispondono, i sistemi stabiliscono una sessione. Se le parole d'ordine non corrispondono, la richiesta dell'utente viene rifiutata. Quando i sistemi specificano delle parole d'ordine di ubicazione per stabilire una sessione, ciò viene chiamato **collegamento sicuro**.

Nota: non tutti i sistemi di computer forniscono supporto per la funzione di collegamento sicuro.

Limitazione delle sessioni APPC

Come responsabile della sicurezza su un sistema di origine, è possibile utilizzare l'autorizzazione all'oggetto per controllare gli utenti che tentano di accedere ad altri sistemi. Impostare l'autorizzazione pubblica per le descrizioni unità APPC su *EXCLUDE e fornire l'autorizzazione *CHANGE a utenti specifici. Utilizzare il valore di sistema QLMTSECOFR per impedire agli utenti con autorizzazione speciale *ALLOBJ di utilizzare le comunicazioni APPC.

Come responsabile della sicurezza su un sistema di destinazione, è inoltre possibile utilizzare l'autorizzazione alle unità APPC per impedire agli utenti di avviare una sessione APPC sul sistema. Tuttavia, è necessario comprendere quale ID utente

tenterà di accedere alla descrizione unità APPC. “Accesso di un utente APPC al sistema di destinazione” descrive in che modo i server iSeries associano un ID utente ad una richiesta per una sessione APPC.

Nota: E' possibile utilizzare il comando Stampa oggetti autorizzati pubblicamente (PRTPVTAUT *DEVD) e il comando Stampa autorizzazioni private. (PRTPVTAUT *DEVD) per individuare quale utente ha l'autorizzazione alle descrizioni unità sul sistema.

Quando il sistema utilizza APPN, crea automaticamente una nuova unità APPC quando nessuna unità esistente è disponibile per l'instradamento scelto dal sistema. Un metodo per limitare l'accesso alle unità APPC su un sistema che utilizza APPN è creare un elenco di autorizzazioni. L'elenco di autorizzazioni contiene l'elenco di utenti che dovrebbero essere autorizzati alle unità APPC. Si utilizza quindi il comando Modifica valori predefiniti comando (CHGCMDDFT) per modificare il comando CRTDEVAPPC. Per il parametro relativo all'autorizzazione (AUT) sul comando CRTDEVAPPC, impostare il valore predefinito sull'elenco di autorizzazioni che è stato creato.

Nota: se il sistema ha una lingua diversa dall'Inglese, è necessario modificare i valori predefiniti del comando nella libreria QSYSxxxx per ciascuna lingua nazionale che si trova sul sistema.

Si utilizza il parametro relativo alla parola d'ordine dell'ubicazione (LOCPWD) nella descrizione unità APPC per convalidare l'identità di un altro sistema che richiede una sessione sul sistema (per conto di un utente o di un'applicazione). La parola d'ordine dell'ubicazione può aiutare l'utente a individuare il sistema falso.

Quando si utilizzano le parole d'ordine dell'ubicazione, è necessario collaborare con i responsabili della sicurezza per altri sistemi nella rete. E' inoltre necessario controllare chi può creare o modificare le descrizioni unità APPC e gli elenchi di configurazioni. Il sistema richiede l'autorizzazione speciale *IOSYSCFG per utilizzare i comandi che gestiscono le unità APPC e gli elenchi di configurazioni.

Nota: quando si utilizza APPN, le parole d'ordine dell'ubicazione sono memorizzate nell'elenco di configurazioni QAPPNRMT piuttosto che nelle descrizioni unità.

Accesso di un utente APPC al sistema di destinazione

Quando i sistemi stabiliscono la sessione APPC, creano un percorso per l'utente richiedente per accedere al sistema di destinazione. Numerosi altri elementi stabiliscono le possibili azioni dell'utente per accedere all'altro sistema.

Gli argomenti che seguono descrivono gli elementi che stabiliscono in che modo un utente APPC ottiene l'accesso al sistema di destinazione.

Metodi del sistema per inviare le informazioni relative a un utente

L'architettura APPC fornisce tre metodi per inviare informazioni di sicurezza relative a un utente dal sistema di origine al sistema di destinazione. Si fa riferimento a tali metodi come **valori di sicurezza progettati**. La Tabella 18 a pagina 116 visualizza tali metodi:

Nota: il manuale *APPC Programming* fornisce ulteriori informazioni sui valori di sicurezza progettati.

Tabella 18. Valori di sicurezza nell'architettura APPC

Valore di sicurezza progettato	ID utente inviato al sistema di destinazione	Parola d'ordine inviata al sistema di destinazione
Nessuna	No	No
Identico	Sì[1]	Consultare la nota 2.
Programma	Sì	Sì[3]

Note:

1. Il sistema di origine invia l'ID utente se il sistema di destinazione specifica SECURELOC(*YES) o SECURELOC(*VFYENCPWD).
2. L'utente non immette una parola d'ordine sulla richiesta poiché tale parola d'ordine è già verificata dal sistema di origine. Per SECURELOC(*YES) e SECURELOC(*NO), il sistema di origine non invia la parola d'ordine. Per SECURELOC(*VFYENCPWD), il sistema di origine richiama la parola d'ordine codificata, memorizzata e la invia (in formato codificato).
3. Il sistema invia la parola d'ordine in formato codificato se sia il sistema di origine sia quello di destinazione supportano la codifica della parola d'ordine. In caso contrario, la parola d'ordine non è codificata.

L'applicazione che l'utente richiede stabilisce il valore di sicurezza progettato. Ad esempio, SNADS utilizza sempre SECURITY(NONE). DDM utilizza SECURITY(SAME). Con un pass-through della stazione video, l'utente specifica il valore di sicurezza utilizzando i parametri sul comando STRPASTHR.

In tutti i casi, il sistema di destinazione sceglie se accettare una richiesta con il valore di sicurezza specificato sul sistema di origine. In alcune situazioni, è possibile che il sistema di destinazione rifiuti completamente la richiesta. In altre situazioni, è possibile che il sistema di destinazione forzi un valore di sicurezza differente. Ad esempio, quando un utente specifica un ID utente e una parola d'ordine sul comando STRPASTHR, la richiesta utilizza SECURITY(PGM). Tuttavia, se il valore di sistema QRMTSIGN è *FRCSIGNON sul sistema di destinazione, l'utente visualizza ancora il pannello collegamento. Con l'impostazione *FRCSIGNON, i sistemi utilizzano sempre SECURITY(NONE), che è l'equivalente dell'utente che non immette né parola d'ordine né ID utente sul comando STRPASTHR.

Note:

1. I sistemi di origine e di destinazione negoziano il valore di sicurezza prima dell'invio dei dati. Nella situazione in cui il sistema di destinazione specifica SECURELOC(*NO) e la richiesta è SECURITY(SAME), ad esempio, il sistema di destinazione indica al sistema di origine di utilizzare SECURITY(NONE). Il sistema di origine non invia l'ID utente.
2. Il sistema di destinazione rifiuta una richiesta di sessione quando la parola d'ordine dell'utente sul sistema di destinazione è scaduta. Ciò si applica soltanto a richieste di collegamento che inviano una parola d'ordine, incluse le seguenti:
   - Richieste di sessione di tipo SECURITY(PROGRAM).
   - Richieste di sessione di tipo SECURITY(SAME) quando il valore SECURELOC è *VFYENCPWD.

Opzioni per distribuire la responsabilità della sicurezza di rete

Quando il sistema fa parte di una rete, è necessario decidere se considerare affidabili altri sistemi per convalidare l'identità di un utente che tenta di accedere al sistema. E' affidabile SYSTEMA nell'assicurare che USERA è realmente USERA (o QSECOFR è realmente QSECOFR)? O si richiederà ad un utente di fornire nuovamente un ID utente e una parola d'ordine?

Il parametro relativo all'ubicazione protetta (SECURELOC) nella descrizione unità APPC sul sistema di destinazione specifica se il sistema di origine è un'ubicazione protetta (garantita).

Quando entrambi i sistemi eseguono un release che supporta *VFYENCPWD, SECURELOC(*VFYENCPWD) fornisce ulteriore protezione quando le applicazioni utilizzano SECURITY(SAME). Sebbene il richiedente non immetta una parola d'ordine nella richiesta, il sistema di origine richiama la parola d'ordine dell'utente e la invia con la richiesta. Affinché la richiesta abbia esito positivo, è necessario che l'utente abbia lo stesso ID utente e parola d'ordine su entrambi i sistemi.

Quando il sistema di destinazione specifica SECURELOC(*VFYENCPWD) e il sistema di origine non supporta tale valore, il sistema di destinazione gestisce la richiesta come SECURITY(NONE).

La Tabella 19 visualizza le modalità del funzionamento congiunto del valore di sicurezza progettato e del valore SECURELOC:

Tabella 19. Modalità di funzionamento congiunto del valore di sicurezza APPC e del valore SECURELOC

Sistema di origine	**Sistema di destinazione**	
Valore di sicurezza progettato	**valore SECURELOC**	**Profilo utente per lavoro**
Nessuno	Qualunque valore	Utente predefinito[1]
Identico	*NO	Utente predefinito[1]
	*YES	Stesso nome profilo utente del richiedente dal sistema di origine
	*VFYENCPWD	Stesso nome profilo utente del richiedente dal sistema di origine. L'utente deve avere la stessa parola d'ordine su entrambi i sistemi.
Programma	Qualunque valore	I profili utente specificati sulla richiesta dal sistema di origine.

Note:

1. L'utente predefinito è stabilito dalla voce comunicazioni nella descrizione del sottosistema. "Assegnazione a un sistema di destinazione di profili utente per lavori" descrive tale argomento.

Assegnazione a un sistema di destinazione di profili utente per lavori

Quando un utente richiede un lavoro APPC su un altro sistema, la richiesta ha un nome modalità associato ad essa. E' possibile che il nome modalità provenga dalla richiesta dell'utente o che possa essere un valore predefinito dagli attributi di rete del sistema di origine.

Il sistema di destinazione utilizza il nome modalità e il nome unità APPC per stabilire in che modo il lavoro verrà eseguito. Il sistema di destinazione ricerca i sottosistemi attivi per una voce di comunicazione che sia la migliore corrispondenza per il nome unità APPC e il nome modalità.

La voce di comunicazione specifica quale profilo utente il sistema utilizzerà per le richieste SECURITY(NONE). Di seguito viene riportato un esempio di una voce di comunicazione in una descrizione del sottosistema:

```
                        Visualizzazione voci di comunicazione

Descrizione sottosistema: QCMN          Stato:    ACTIVE

                          Descrizione                   Utente          Max
Unità        Modalità       lavoro       Libreria      predefinito   attivo
*ALL          *ANY        *USRPRF                      *SYS          *NOMAX
*ALL          QPCSUPP     *USRPRF                      *NONE         *NOMAX
```

La Tabella 20 visualizza i possibili valori per il parametro utente predefinito in una voce di comunicazione:

Tabella 20. Possibili valori per il parametro utente predefinito

Valore	Risultato
***NONE**	Nessun utente predefinito è disponibile. Se il sistema di origine non fornisce un ID utente sulla richiesta, il lavoro non verrà eseguito.
***SYS**	Verranno eseguiti soltanto i programmi (lavori di sistema) forniti dall'IBM. Non verrà eseguita alcuna applicazione utente.
nome-utente	Se il sistema di origine non invia un ID utente, il lavoro viene eseguito sotto tale profilo utente.

E' possibile utilizzare il comando Stampa descrizione sottosistema (PRTSBSDAUT) per stampare un elenco di tutti i sottosistemi che che dispongono di voci di comunicazione con un profilo utente predefinito.

Opzioni di pass-through di una stazione video

Il pass-through di una stazione video è un esempio di un'applicazione che utilizza le comunicazioni APPC. E' possibile utilizzare il pass-through di una stazione video per collegarsi a un altro sistema collegato al sistema dell'utente tramite una rete.

La Tabella 21 a pagina 119 visualizza esempi di richieste di pass-through (comando STRPASTHR) e in che modo il sistema di destinazione le gestisce. Per un pass-through di una stazione video, il sistema utilizza gli elementi di base delle comunicazioni APPC e il valore di sistema di collegamento remoto (QRMTSIGN).

Nota: le richieste di pass-through di una stazione video non vengono più instradate tramite i sottosistemi QCMN o QBASE. A partire da V4R1, vengono instradate tramite il sottosistema QSYSWRK. Prima di V4R1 era possibile presupporre che, se i sottosistemi QCMD o QBASE non fossero stati avviati, il pass-through di una stazione video non avrebbe funzionato. Ciò non si verifica più. E' possibile forzare il pass-through di una stazione video in modo che passi per QCMN (o QBASE se è attivo) modificando il valore di sistema QPASTHRSVR in 0.

Tabella 21. Richieste di collegamento pass-through di esempio

Valori sul comando STRPASTHR		**Sistema di destinazione**		
ID utente	**Parola d'ordine**	**valore SECURELOC**	**valore QRMTSIGN**	**risultato**
*NONE	*NONE	Qualunque valore	Qualunque valore	E' necessario che l'utente si colleghi al sistema di destinazione.
Un nome profilo utente	Non immesso	Qualunque valore	Qualunque valore	La richiesta ha esito negativo.
*CURRENT	Non immesso	*NO	Qualunque valore	La richiesta ha esito negativo
		*YES	*SAMEPRF	Un lavoro interattivo viene avviato con lo stesso nome profilo utente del profilo utente sul sistema di origine. Non viene passata alcuna parola d'ordine al sistema remoto.E' necessario che il nome profilo utente esista sul sistema di destinazione.
			*VERIFY	
			*FRCSIGNON	E' necessario che l'utente si colleghi al sistema di destinazione.
		*VFYENCPWD	*SAMEPRF	Un lavoro interattivo viene avviato con lo stesso nome profilo utente del profilo utente sul sistema di origine. Il sistema di origine richiama la parola d'ordine dell'utente e la invia al sistema remoto. E' necessario che il nome profilo utente esista sul sistema di destinazione.
			*VERIFY	
			*FRCSIGNON	E' necessario che l'utente si colleghi al sistema di destinazione.
*CURRENT (o il nome del profilo utente corrente per il lavoro)	Immesso	Qualunque valore	*SAMEPRF	Un lavoro interattivo viene avviato con lo stesso nome profilo utente del profilo utente sul sistema di origine. La parola d'ordine *viene* inviata al sistema remoto. E' necessario che il nome profilo utente esista sul sistema di destinazione.
			*VERIFY	
			*FRCSIGNON	E' necessario che l'utente si colleghi al sistema di destinazione.

Tabella 21. Richieste di collegamento pass-through di esempio (Continua)

Valori sul comando STRPASTHR		Sistema di destinazione		
ID utente	**Parola d'ordine**	**valore SECURELOC**	**valore QRMTSIGN**	**risultato**
Un nome profilo utente (un nome differente dal profilo utente corrente per il lavoro)	Immesso	Qualunque valore	*SAMEPRF	La richiesta ha esito negativo.
			*VERIFY	Un lavoro interattivo viene avviato con lo stesso nome profilo utente del profilo utente sul sistema di origine. La parola d'ordine *viene* inviata al sistema remoto. E' necessario che il nome profilo utente esista sul sistema di destinazione.
			*FRCSIGNON	Un lavoro interattivo si avvia con il nome profilo utente specificato. La parola d'ordine viene inviata al sistema di destinazione. E' necessario che il nome profilo utente esista sul sistema di destinazione.

Come evitare assegnazioni unità impreviste

Quando si verifica un errore su un'unità attiva, il sistema tenta il ripristino. In alcune circostanze, quando si interrompe il collegamento, è possibile che un altro utente ristabilisca in modo non intenzionale la sessione in errore. Ad esempio, presumiamo che USERA abbia disattivato una stazione di lavoro senza scollegarsi. USERB potrebbe attivare la stazione di lavoro e riavviare la sessione di USERA senza collegarsi.

Per impedire tale possibilità, impostare il valore di sistema Azione errore I/E unità (QDEVRCYACN) su *DSCMSG. Quando un'unità ha esito negativo, il sistema termina il lavoro dell'utente.

Controllo di comandi remoti e lavori batch

Sono disponibili numerose opzioni per controllare quali comandi remoti e lavori è possibile eseguire sul sistema, incluso quanto segue:

- Se il sistema utilizza DDM, è possibile limitare l'accesso ai file DDM per impedire agli utenti di utilizzare il comando Inoltro comando remoto (SBMRMTCMD) da un altro sistema. Per utilizzare SBMRMTCMD, è necessario che l'utente possa aprire un file DDM. E' inoltre necessario limitare la capacità di creare i file DDM.
- E' possibile specificare un programma di uscita per il valore di sistema (DDMACC) relativo a un accesso richiesta DDM. Nel programma di uscita, è possibile valutare tutte le richieste DDM prima di consentirle.
- E' possibile utilizzare l'attributo di rete (JOBACN) relativo all'azione del lavoro di rete per prevenire l'inoltro dei lavori di rete o la relativa esecuzione automatica.
- E' possibile specificare esplicitamente quali richieste del programma è possibile eseguire in un ambiente di comunicazioni rimuovendo la voce di instradamento

PGMEVOKE dalle descrizioni del sottosistema. La voce di instradamento PGMEVOKE consente al richiedente di specificare il programma che si sta eseguendo. Quando si rimuove tale voce di instradamento dalle descrizioni del sottosistema, come ad esempio la descrizione del sottosistema QCMN, è necessario aggiungere delle voci di instradamento per le richieste di comunicazioni che è necessario eseguire correttamente.

"Richieste TPN strutturati" a pagina 95 elenca i nomi programma per le richieste di comunicazioni da parte delle applicazioni fornite dall'IBM. Per ciascuna richiesta che si desidera consentire, è possibile aggiungere una voce di instradamento con il valore di confronto e il nome programma entrambi uguali al nome programma.

Quando si utilizza questo metodo, è necessario comprendere l'ambiente di gestione lavoro sul sistema e i tipi di richieste di comunicazione che si verificano sul sistema. Se possibile, sarebbe opportuno verificare tutti i tipi di richieste di comunicazione per accertarsi che funzionino correttamente dopo avere modificato le voci di instradamento. Quando una richiesta di comunicazione non individua una voce di instradamento disponibile, si riceve un messaggio CPF1269. Un'altra alternativa (meno incline agli errori ma probabilmente leggermente meno efficace) è impostare l'autorizzazione pubblica su *EXCLUDE per i programmi di transazione che non si desidera eseguire sul sistema.

Nota: il manuale *Work Management* fornisce ulteriori informazioni sulle voci di instradamento e su come il sistema gestisce le richieste di avvio programma.

Valutazione della configurazione APPC

E' possibile utilizzare il comando Stampa riservatezza di comunicazione (PRTCMNSEC) o le opzioni di menu per stampare i valori rilevanti per la sicurezza nella configurazione APPC. Gli argomenti che seguono descrivono le informazioni sui documenti.

Parametri rilevanti per le unità APPC

La Figura 9 riporta un esempio del Documento di informazioni sulla comunicazione per descrizioni unità. La Figura 10 a pagina 122 riporta un esempio del documento per gli elenchi di configurazioni. Dopo i documenti vi sono delle spiegazioni dei campi in essi contenuti.

```
                    Informazioni sulla comunicazione (Documento completo)
                                                                        SYSTEM4
Tipo oggetto  . . . . . . . . . :   *DEVD

                                                                      Sessione       Avvio
Nome          Tipo          Categoria      Ubicazione   Par. d'ord.  Supporto    Sessione     pre-         programma
oggetto       oggetto        unità          protetta    ubicazione    APPN       singola     stabilita      SNUF

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

Figura 9. Descrizioni unità APPC-Documento di esempio

```
                  Visualizzazione elenco configurazioni                        Pagina     1
                              SYSTEM4  12/17/95  07:24:36
Elenco configurazioni . . . . . . . . . :   QAPPNRMT
Tipo elenco configurazioni  . . . . . :   *APPNRMT
Testo . . . . . . . . . . . . . . . . :
-----------------Ubicazioni remote APPN------------------
           ID                 Punto    ID rete
Ubicaz.    rete      Ubicaz.  control.  punto     Ubicazione
remota     remota    locale   remoto    control.   protetta
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
--------------------------Ubicazioni remote APPN---------------------------
           ID                                          Punto      Sessione
Ubicaz.    rete       Ubicaz.  Sessione     Numero    controllo     pre-
remota     remota     locale   singola   conversazioni  locale     stabilita
SYSTEM36   APPN      SYSTEM4    *NO             10      *NO        *NO
SYSTEM32   APPN      SYSTEM4    *NO             10      *NO        *NO
```

Figura 10. Documento elenco configurazioni-Esempio

Campo Ubicazione protetta

Il campo Ubicazione protetta (SECURELOC) specifica se il sistema locale consente al sistema remoto di eseguire la verifica della parola d'ordine per conto del sistema locale. Il campo SECURELOC si applica unicamente alle applicazioni che utilizzano il valore SECURITY(SAME), come ad esempio DDM ed applicazioni che utilizzano l'API CPI-Comunicazioni.

SECURELOC(*YES) rende il sistema locale vulnerabile per le possibili debolezze nel sistema remoto. Qualsiasi utente che sia presente in entrambi i sistemi può richiamare programmi sul sistema locale. Questo è particolarmente pericoloso poiché il profilo utente QSECOFR (responsabile della riservatezza) esiste in tutti i sistemi iSeries e dispone dell'autorizzazione speciale *ALLOBJ. Se un sistema sulla rete non osserva un'attenta protezione della parola d'ordine di QSECOFR, gli altri sistemi che considerano tale sistema un'ubicazione protetta sono a rischio.

Quando si utilizza SECURELOC(*VFYENCPWD), il sistema è meno vulnerabile nei confronti di altri sistemi che non proteggono adeguatamente le parole d'ordine. Un utente che richede un'applicazione che utilizza SECURITY(SAME) deve avere lo stesso ID utente e la stessa parola d'ordine in entrambi i sistemi. SECURELOC(*VFYENCPWD) richiede normative di gestione della parola d'ordine attraverso la rete in modo che gli utenti abbiano la stessa parola d'ordine su tutti i sistemi.

Nota: SECURELOC(*VFYENCPWD) è supportato solo tra sistemi su cui è in esecuzione V3R2, V3R7 o V4R1. Se il sistema di destinazione specifica SECURELOC(*VFYENCPWD) ed il sistema origine non supporta tale funzione, la richiesta viene considerata come SECURITY(NONE).

Se un sistema specifica SECURELOC(*NO), le applicazioni che utilizzano SECURITY(SAME) avranno bisogno di un utente predefinito per l'esecuzione dei programmi. L'utente predefinito dipende sia dalla descrizione unità che dalla modalità associate alla richiesta. (Consultare "Assegnazione a un sistema di destinazione di profili utente per lavori" a pagina 117.)

Campo Parola d'ordine ubicazione
Il campo Parola d'ordine ubicazione determina se i due sistemi si scambieranno le parole d'ordine per verificare che il sistema richiedente non sia un sistema fittizio. "Esempio: sessione APPC di base" a pagina 114 fornisce ulteriori informazioni sulle parole d'ordine ubicazione.

Campo Supporto APPN
Il campo Supporto-APPN (APPN) specifica se il sistema remoto può supportare funzioni di rete avanzate o si limita a collegamenti hop-singolo. APPN(*YES) ha il seguente significato:

- Se il sistema remoto è un nodo di rete, può essere in grado di collegare il sistema locale ad altri sistemi. Questo viene detto **instradamento nodo intermedio**. Significa che utenti sul sistema possono essere in grado di utilizzare il sistema remoto come instradamento ad una rete più vasta.
- Se il sistema locale è un nodo di rete, il sistema remoto può utilizzare il sistema locale per collegarsi ad altri sistemi. Gli utenti sul sistema remoto possono essere in grado di utilizzare il sistema come instradamento ad una rete più vasta.

  Nota: è possibile utilizzare il comando DSPNETA per stabilire se un sistema è un nodo di rete o un nodo finale.

Campo Sessione singola
Il campo Sessione singola (SNGSSN) specifica se il sistema remoto può eseguire più di una sessione alla volta utilizzando la stessa descrizione unità APPC. Si utilizza di solito SNGSSN(*NO) poiché elimina la necessità di creare più descrizioni unità per un sistema remoto. Ad esempio, un utente PC spesso richiede più di una sessione emulazione 5250 e sessioni per le funzioni server file e server di stampa. Con SNGSSN(*NO), è possibile fornire questa funzione con una descrizione unità per il PC nel sistema iSeries.

SNGSSN(*NO) sta ad indicare che bisogna contare su procedure operative che applicano la sicurezza degli utenti PC ed altri utenti APPC. Il sistema è vulnerabile rispetto a qualcuno sul sistema remoto che avvii una sessione non autorizzata che utilizza la stessa descrizione unità di una sessione esistente. (A volte ci si riferisce a questa pratica come **sfruttamento-identità**.)

Campo Sessione pre-stabilita
Il campo Sessione pre-stabilita (PREESTSSN) per un'unità a sessione singola controlla se il sistema locale avvia una sessione con il sistema remoto quando il sistema remoto contatta per la prima volta il sistema locale. PREESTSSN(*NO) significa che il sistema locale attende ad avviare una sessione fin quando un'applicazione non richiede una sessione con il sistema. PREESTSSN(*YES) è utile per ridurre al minimo il tempo che occorre ad un programma dell'applicazione per completare il collegamento.

PREESTSSN(*YES) impedisce al sistema di scollegare una linea commutata (collegamento remoto) che non si sta più utilizzando. L'applicazione o l'utente devono disattivare la linea in modo esplicito. PREESTSSN(*YES) può allungare il periodo in cui il sistema locale è vulnerabile allo sfruttamento-identità nella sessione.

Campo Avvio programma SNUF
Il campo Avvio programma SNUF specifica se il sistema remoto può avviare programmi sul sistema locale. *YES significa che lo schema di autorizzazione

all'oggetto sul sistema locale deve essere adeguato a proteggere gli oggetti quando utenti sul sistema remoto avviano lavori ed eseguono programmi sul sistema locale.

Parametri per le unità di controllo APPC

La Figura 11 riporta un esempio del Documento di informazioni sulla comunicazione per descrizioni unità di controllo. Dopo il documento, si troveranno spiegazioni dei campi contenuti nel documento.

```
                    Informazioni sulla comunicazione (Documento completo)
                                                                        SYSTEM4
Tipo oggetto  . . . . . . . . . :   *CTLD

Nome      Tipo     Categoria     Creaz.   Unità contr. Direzione  Supporto  Sessioni   Tempific.    Secondi   Nome
oggetto   oggetto  unità contr.  autom.    commutata    chiamata    APPN       CP       scolleg.     cancel.   unità
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
```

Figura 11. Descrizioni unità di controllo APPC-Documento di esempio

Campo Creazione automatica

In una descrizione linea, il campo Creazione automatica (AUTOCRTCTL) specifica se il sistema locale crea automaticamente una descrizione dell'unità di controllo quando una richiesta in entrata non riesce a trovare una descrizione dell'unità di controllo corrispondente. In una descrizione del programma di controllo, il campo Creazione automatica (AUTOCRTDEV) specifica se il sistema locale crea automaticamente una descrizione unità quando una richiesta in entrata non riesce a trovare una descrizione unità corrispondente.

Per unità di controllo che supportano APPN, il campo Creazione automatica non ha alcun effetto. Il sistema crea automaticamente descrizioni unità quando è necessario, indipendentemente dall'impostazione del campo Creazione automatica.

Quando si specifica *YES per una descrizione di linea, chiunque abbia accesso alla linea può collegarsi al sistema. Questo include siti collegati tramite bridge e router.

Campo Sessioni CP (Control point/punto di controllo)

Per unità di controllo con supporto APPN, il campo Sessioni CP (CPSSN) controlla se il sistema stabilisce automaticamente un collegamento APPC con il sistema remoto. Il sistema utilizza la sessione CP per scambiare informazioni e stato della rete con il sistema remoto. Lo scambio di informazioni aggiornate tra nodi di rete APPN è molto importante per il funzionamento regolare della rete.

Quando si specifica *YES, una linea commutata inattiva non si scollega automaticamente. Questo rende il sistema più vulnerabile allo sfruttamento di identità di una sessione.

Campo Tempificatore scollegamento

Per un'unità di controllo APPC, il campo Tempificatore scollegamento specifica per quanto tempo un'unità di controllo deve rimanere inutilizzata (senza sessioni attive) prima che il sistema scolleghi la linea al sistema remoto. Questo campo ha due valori. Il primo valore specifica per quanto tempo l'unità di controllo rimarrà attiva a partire dal momento in cui viene contattata. Il secondo valore determina per quanto tempo il sistema rimane in attesa dopo che l'ultima sessione è terminata sull'unità di controllo prima di rilasciare la linea.

Il sistema utilizza il tempificatore scollegamento solo quando il campo Scollegamento commutato (SWTDSC) è impostato su *YES.

Se si estendono questi valori, il sistema è più vulnerabile allo sfruttamento di identità delle sessioni .

Parametri per le descrizioni di linea

La Figura 12 riporta un esempio del Documento di informazioni sulla comunicazione per descrizioni linea. Dopo il documento, si troveranno spiegazioni dei campi contenuti nel documento.

```
                    Informazioni sulla comunicazione (Documento completo)

Tipo oggetto  . . . . . . . . . :   *LIND
Nome
oggetto        Tipo           Categoria      Creaz.     Secondi     Risposta   Composiz.
autom.         oggetto         linea         autom.     cancell.     autom.     autom.
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
```

Figura 12. Descrizioni linea APPC-Documento di esempio

Campo Risposta automatica

Il campo Risposta automatica (AUTOANS) specifica se la linea commutata accetterà chiamate in entrata senza intervento dell'operatore.

Quando si specifica *YES, il sistema risulta meno sicuro poiché è possibile accedervi più facilmente. Per minimizzare il rischio per la sicurezza quando si specifica *YES, si dovrebbe disattivare la linea quando non è necessaria.

Campo Composizione automatica

Il campo Composizione automatica (AUTODIAL) specifica se la linea commutata può effettuare chiamate in uscita senza intervento dell'operatore. Quando si specifica *YES, si consente ad utenti locali senza accesso fisico alle linee di comunicazione e ai modem di collegarsi ad altri sistemi.

Capitolo 13. Comunicazioni TCP/IP protette

TCP/IP (Transmission Control Protocol/Internet Protocol) è un modo comune attraverso cui i computer di tutti i tipi comunicano tra di loro. Le applicazioni TCP/IP sono molto note e ampiamente utilizzate in tutta la "rete di diffusione delle informazioni".

Questo capitolo fornisce dei suggerimenti per effettuare le seguenti operazioni:

- Impedire alle applicazioni TCP/IP di essere eseguite sul sistema.
- Proteggere le risorse del sistema quando si consente l'esecuzione delle applicazioni TCP/IP sul sistema.

Il sito web iSeries Information Center—>Rete—>TCP/IP è una fonte completa di informazioni su tutte le applicazioni TCP/IP. *SecureWay: iSeries e Internet* (iSeries Information Center—>Sicurezza—>SecureWay descrive le considerazioni sulla sicurezza quando ci si collega al server iSeries su Internet (una rete TCP/IP molto ampia) o su un'intranet. Consultare "Requisiti necessari e informazioni correlate" a pagina xii per informazioni sull'accesso all'iSeries Information Center.

Tenere a mente che i server iSeries supportano molte possibili applicazioni TCP/IP. Quando si decide di consentire un'applicazione TCP/IP sul sistema, è possibile che si stiano abilitando anche altre applicazioni TCP/IP. Come responsabile della sicurezza, è necessario essere consapevoli della gamma di applicazioni TCP/IP e delle implicazioni sulla sicurezza di tali applicazioni.

Come impedire l'elaborazione TCP/IP

I lavori del server TCP/IP vengono eseguiti nel sottosistema QSYSWRK. Si utilizza il comando Avvio TCP/IP (STRTCP) per avviare TCP/IP sul sistema. Se non si desidera che venga eseguita alcuna elaborazione o applicazione TCP/IP, non utilizzare il comando STRTCP. Il sistema viene fornito con l'autorizzazione pubblica per il comando STRTCP impostata su *EXCLUDE.

Se si sospetta che qualcuno con l'accesso al comando stia avviando TCP/IP (durante le ore non di punta), è possibile impostare il controllo dell'oggetto sul comando STRTCP. Il sistema scriverà una voce del giornale di controllo ogni qualvolta un utente esegue il comando.

Componenti di sicurezza TCP/IP

E' possibile sfruttare i numerosi componenti della sicurezza TCP/IP che migliorano la sicurezza della rete e aggiungono flessibilità. Sebbene alcune di tali tecnologie si trovino anche nei prodotti firewall, tali componenti di sicurezza TCP/IP per OS/400 non sono pianificati per essere utilizzati come firewall. Tuttavia, è possibile utilizzare alcune di tali funzioni, in alcune istanze per eliminare la necessità di un prodotto firewall separato. E' inoltre possibile utilizzare tali funzioni TCP/IP per fornire ulteriore sicurezza negli ambienti in cui si utilizza già un firewall.

E' possibile utilizzare i seguenti componenti per migliorare la sicurezza TCP/IP:

- Regole del pacchetto
- Server proxy HTTP
- VPN (virtual private networking)

© Copyright IBM Corp. 1996, 2004

- SSL (secure sockets layer)

Utilizzo delle regole del pacchetto per proteggere il traffico TCP/IP

Le regole del pacchetto, che sono una combinazione del filtro IP e di NAT (network address translation) funzionano come un firewall per proteggere la rete interna dagli intrusi. Il filtro IP consente di controllare quale traffico IP consentire all'interno e all'esterno della rete. Fondamentalmente, protegge la rete filtrando i pacchetti secondo regole definite dall'utente. NAT, d'altra parte, consente di nascondere gli indirizzi IP privati non registrati dietro una serie di indirizzi IP registrati. Ciò aiuta a proteggere la rete interna dalle reti esterne. NAT aiuta inoltre a limitare il problema dell'esaurimento di indirizzi IP, poiché molti indirizzi privati possono essere rappresentati da una serie ridotta di indirizzi registrati. Consultare iSeries Information Center per ulteriori dettagli.

Server proxy HTTP

Il server proxy HTTP viene fornito con l'IBM HTTP Server for iSeries. Il server HTTP fa parte di OS/400. Il server proxy riceve le richieste HTTP dai browser Web e le reinvia ai server Web. I server Web che ricevono la richieste conoscono soltanto l'indirizzo IP del server proxy e non possono stabilire i nomi o gli indirizzi dei PC che hanno dato origine alle richieste. Il server proxy può gestire le richieste URL per HTTP, FTP, Gopher e WAIS.

Il server proxy memorizza nella cache le pagine web restituite dalle richieste effettuate da tutti gli utenti del server proxy. Di conseguenza, quando gli utenti richiedono una pagina, il server proxy controlla se la pagina si trova nella cache. In questo caso, il server proxy restituisce la pagina memorizzata nella cache. Utilizzando le pagine memorizzate nella cache, il server proxy può gestire le pagine web più velocemente, eliminando le richieste che potenzialmente fanno consumare tempo al server web.

Il server proxy può inoltre registrate tutte le richieste URL per scopi di traccia. E' quindi possibile esaminare le registrazioni per monitorare l'utilizzo e l'errato uso delle risorse di rete.

E' possibile utilizzare il supporto proxy HTTP nell'IBM HTTP Server per consolidare l'accesso al Web. Gli indirizzi dei client PC sono nascosti dai server web a cui accedono; soltanto l'indirizzo IP del server proxy è noto. La memorizzazione di una pagina web nella cache riduce inoltre i requisiti di ampiezza banda di comunicazione e il carico di lavoro del firewall. Consultare la homepage relativa all'IBM HTTP Server for iSeries per ulteriori informazioni: http://www-1.ibm.com/servers/eserver/iseries/software/http/index.html

VPN (Virtual Private Networking)

Una VPN (virtual private network) consente alla società di estendere in modo sicuro l'intranet privata sulla framework esistente di una rete pubblica, come Internet. Con VPN, la società può controllare il traffico della rete fornendo importanti funzioni di sicurezza come l'autenticazione e la riservatezza dei dati.

VPN OS/400 è un componente installabile facoltativamente di iSeries Navigator, la GUI (graphical user interface) per OS/400. Consente di creare un percorso protetto da un punto finale all'altro tra una qualsiasi combinazione di host e gateway. VPN

OS/400 VPN utilizza metodi di autenticazione, algoritmi di codifica e altre precauzioni per accertarsi che i dati inviati tra i due punti finali del relativo collegamento rimangano protetti.

VPN viene eseguito sul livello di rete del modello stack delle comunicazioni suddiviso in livelli di TCP/IP. In modo specifico, VPN utilizza la framework aperta IPSec (IP Security Architecture). IPSec fornisce funzioni di sicurezza di base per internet, oltre a fornire blocchi di creazione flessibili da cui è possibile creare reti private virtuali, protette e robuste.

VPN supporta inoltre soluzioni VPN L2TP (Layer 2 Tunnel Protocol). I collegamenti L2TP, denominati anche linee virtuali, forniscono accesso poco dispendioso per utenti remoti consentendo a un server di rete aziendale di gestire gli indirizzi IP assegnati ai relativi utenti remoti. Inoltre, i collegamenti L2TP forniscono un accesso protetto al sistema o alla rete quando questi vengono protetti tramite IPSec.

E' importante comprendere l'impatto che VPN avrà sull'intera rete. Una pianificazione e un'implementazione appropriate sono essenziali per il successo dell'attività. Sarebbe opportuno esaminare l'argomento VPN nell'iSeries Information Center per accertarsi che si sappia come funziona VPN e come è possibile utilizzarla. Per ulteriori informazioni, consultare iSeries Information Center—>Sicurezza—>VPN (Virtual Private Networking). Consultare "Requisiti necessari e informazioni correlate" a pagina xii per informazioni sull'accesso all'iSeries Information Center.

SSL (Secure Sockets Layer)

SSL (Secure Sockets Layer) è diventata uno standard aziendale per l'abilitazione di applicazioni per le sessioni di comunicazione sicure su una rete non protetta, come ad esempio Internet. Il protocollo SSL stabilisce dei collegamenti sicuri tra le applicazioni client e server che forniscono l'autenticazione di uno o più punti finali della sessione di comunicazione. SSL fornisce inoltre la riservatezza e l'integrità dei dati scambiati tra le applicazioni client e server. Per ulteriori informazioni, consultare iSeries Information Center–>Sicurezza—>SSL (Secure Sockets Layer). Consultare "Requisiti necessari e informazioni correlate" a pagina xii per informazioni sull'accesso all'iSeries Information Center.

Protezione dell'ambiente TCP/IP

Questo argomento fornisce suggerimenti generici per i passi da intraprendere per ridurre i rischi per la sicurezza nell'ambiente TCP/IP nel proprio sistema. Questi suggerimenti si applicano all'intero ambiente TCP/IP piuttosto che a specifiche applicazioni discusse nei capitoli che seguono.

- Quando si scrive un'applicazione per una porta TCP/IP, accertarsi che l'applicazione sia protetta in modo appropriato. Si dovrebbe prevedere che un estraneo possa tentare di accedere alla suddetta applicazione tramite quella porta. Un esperto dall'esterno può tentare di eseguire il TELNET a tale applicazione.
- Monitorare l'utilizzo delle porte TCP/IP sul sistema. Un'applicazione utente che è associata ad una porta TCP/IP può fornire un'entrata dalla "porta-di-servizio" al proprio sistema senza ID utente o parola d'ordine. Qualcuno con livello di autorizzazione sufficiente sul sistema può associare un'applicazione ad una porta TCP o UDP.
- Come responsabile della sicurezza, si dovrebbe essere a conoscenza di una tecnica detta *spoofing IP* utilizzata dagli hacker. Ogni sistema in una rete TCP/IP

ha un indirizzo IP. Chi utilizza lo spoofing IP imposta un sistema (di solito un PC) in modo che simuli di essere un indirizzo IP esistente o un indirizzo IP garantito. Così, il malintenzionato può stabilire un collegamento con il sistema simulando di essere un sistema a cui normalmente ci si collega.

Se si esegue TCP/IP sul sistema ed il sistema partecipa ad una rete non fisicamente protetta (tutte linee non commutate e link predefiniti), si è a rischio di spoofing IP. Per proteggere il proprio sistema dai danni da parte di uno "spoofer", iniziare dai suggerimenti in questo capitolo, come ad esempio protezione del collegamento e sicurezza dell'oggetto. Ci si dovrebbe anche assicurare che sul sistema siano impostati limiti di memoria ausiliaria ragionevoli. Questo impedisce ad uno spoofer di sovraccaricare il sistema di posta o di file di spool al punto da rendere il sistema non operativo.

Inoltre, si dovrebbe monitorare regolarmente l'attività TCP/IP sul sistema. Se si rileva lo spoofing IP, si può tentare di individuare i punti deboli nella configurazione TCP/IP ed effettuare degli adattamenti.

- Per l'intranet (rete di sistemi che non devono collegarsi direttamente all'esterno), utilizzare gli indirizzi IP riutilizzabili. Gli indirizzi riutilizzabili sono destinati all'uso entro una rete privata. Il sistema di trasmissioni di Internet non instrada pacchetti con indirizzo IP riutilizzabile. Perciò, gli indirizzi IP riutilizzabili forniscono un ulteriori livello di protezione all'interno del firewall.

  Il sito web iSeries Information Center—>Rete—>TCP/IP fornisce ulteriori informazioni sulla modalità di assegnazione degli indirizzi IP e sugli intervalli di indirizzi IP ed anche informazioni relative alla sicurezza su TCP/IP.
- Se si sta pensando di collegare il sistema ad Internet o ad un'intranet, esaminare le informazioni sulla sicurezza in *SecureWay: iSeries e Internet* (iSeries Information Center—>Sicurezza—>SecureWay). Consultare "Requisiti necessari e informazioni correlate" a pagina xii per informazioni sull'accesso all'iSeries Information Center.

Controllo dei server TCP/IP con avvio automatico

Come responsabile della sicurezza, è necessario controllare quali applicazioni TCP/IP si avviano automaticamente quando si avvia TCP/IP. Sono disponibili due comandi per l'avvio di TCP/IP. Per ogni comando, il sistema utilizza un metodo differente per stabilire quali applicazioni (server) avviare.

La Tabella 22 contiene i due comandi ed i consigli sulla sicurezza ad essi relativi. La Tabella 23 a pagina 131 contiene i valori di avvio automatico predefiniti per i server. Per modificare il valore di avvio automatico per un server, utilizzare il comando CHGxxxA (Modifica attributi xxx) per il server. Ad esempio, il comando per TELNET è CHGTELNA.

Tabella 22. Come i comandi TCP/IP stabiliscono quali server avviare

Comando	Quali server avviare	Consigli sulla sicurezza
Avvio TCP/IP (STRTCP)	Il sistema avvia ogni server con la specifica AUTOSTART(*YES). La Tabella 23 a pagina 131 mostra il valore fornito per ogni server TCP/IP.	• Assegnare l'autorizzazione speciale *IOSYSCFG con cautela per controllare chi può modificare le impostazioni di avvio automatico. • Controllare attentamente chi ha l'autorizzazione ad utilizzare il comando STRTCP. L'autorizzazione pubblica predefinita per il comando è *EXCLUDE. • Impostare il controllo oggetto per i comandi Modifica attributi *nome-server* (come ad esempio CHGTELNA) in modo da monitorare gli utenti che tentano di modificare il valore AUTOSTART per un server.

Tabella 22. Come i comandi TCP/IP stabiliscono quali server avviare (Continua)

Comando	Quali server avviare	Consigli sulla sicurezza
Avvio server TCP/IP (STRTCPSVR)	Si utilizza un parametro per specificare quali server avviare. Il valore predefinito quando viene fornito questo comando è di avviare tutti i server.	• Utilizzare il comando Modifica valori predefiniti comando (CHGCMDDFT) per impostare il comando STRTCPSVR in modo che avvii solo uno specifico server. Questo non impedisce agli utenti di avviare altri server. Tuttavia, modificando il valore predefinito del comando, è meno probabile che gli utenti avviino involontariamente tutti i server. Ad esempio, utilizzare il seguente comando per impostare il valore predefinito in modo che avvii solo il server TELNET:`CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)')` **Nota:** quando si modifica il valore predefinito, è possibile specificare solo un singolo server. Scegliere un server che si utilizza regolarmente o un server con minori probabilità di provocare rischi per la sicurezza (come TFTP). • Controllare con attenzione chi ha l'autorizzazione di utilizzare il comando STRTCPSVR. L'autorizzazione pubblica predefinita per il comando è *EXCLUDE.

La tabella seguente contiene i valori di avvio automatico per i server TCP/IP. Per ulteriori informazioni su ognuno di questi server, consultare l'iSeries Information Center (**Rete—>TCP/IP**). Consultare "Requisiti necessari e informazioni correlate" a pagina xii per dettagli sull'accesso all'iSeries Information Center.

Tabella 23. Valori di avvio automatico per i server TCP/IP

Server	Valore predefinito	Valore dell'utente
TELNET	AUTOSTART(*YES)	
FTP (file transfer protocol)	AUTOSTART(*YES)	
BOOTP (Bootstrap Protocol)	AUTOSTART(*NO)	
TFTP (trivial file transfer protocol)	AUTOSTART(*NO)	
REXEC (Remote EXECution server)	AUTOSTART(*NO)	
RouteD (Route Daemon)	AUTOSTART(*NO)	
SMTP (SMTP (simple mail transfer protocol))	AUTOSTART(*YES)	
POP (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)	

Tabella 23. Valori di avvio automatico per i server TCP/IP (Continua)

Server	Valore predefinito	Valore dell'utente
Note: 1. Con il server IBM HTTP Server per iSeries, si utilizza il comando CHGHTTPA per impostare il valore AUTOSTART.		

Considerazioni di sicurezza per l'utilizzo di SLIP

Il supporto TCP/IP del server iSeries include SLIP (Serial Interface Line Protocol). SLIP fornisce connettività point-to-point a basso costo. Un utente SLIP può collegarsi ad una LAN o una WAN stabilendo un collegamento point to point con un sistema che fa parte della LAN o della WAN.

SLIP si esegue su un collegamento asincrono. E' possibile utilizzare SLIP per un collegamento remoto ai e dai server iSeries. Ad esempio, si potrebbe utilizzare SLIP per collegarsi in entrata dal PC ad un sistema iSeries. Una volta stabilito il collegamento, è possibile utilizzare l'applicazione TELNET sul PC per collegarsi al server TELNET iSeries. Oppure, è possibile utilizzare l'applicazione FTP per trasferire file tra i due sistemi.

Non esiste configurazione SLIP sul sistema quando viene consegnato. Perciò, se non si desidera che SLIP (e TCP/IP di collegamento remoto) sia eseguito sul sistema, non configurare alcun profilo di configurazione per SLIP. Si utilizza il comando Gestione Point-to-Point TCP/IP (WRKTCPPTP) per creare configurazioni SLIP. E' necessario disporre dell'autorizzazione speciale *IOSYSCFG per utilizzare il comando WRKTCPPTP.

Se si desidera che SLIP venga eseguito sul proprio sistema, si creano uno o più profili di configurazione (point-to-point) SLIP. E' possibile creare profili di configurazione con le seguenti modalità operative:
- Collegamento in entrata (*ANS)
- Collegamento in uscita (*DIAL)

Gli argomenti che seguono discutono come si può configurare la sicurezza per profili di configurazione SLIP.

Nota: un **profilo utente** è un oggetto server iSeries che consente il collegamento. Ogni lavoro server iSeries deve avere un profilo utente per l'esecuzione. Un **profilo di configurazione** memorizza informazioni utilizzate per stabilire un collegamento SLIP con un sistema iSeries. Quando si avvia un collegamento SLIP ai server iSeries, si sta semplicemente creando un link. Non ci si è ancora collegati e non si è avviato un lavoro server iSeries. Perciò, non si ha necessariamente bisogno di un profilo utente per avviare un collegamento SLIP ai server iSeries. Tuttavia, come si potrà notare dalle discussioni che seguono, il profilo di configurazione SLIP può richiedere un profilo utente per stabilire se consentire il collegamento.

Controllo dei collegamenti SLIP in entrata

Prima che qualcuno possa stabilire un collegamento in entrata al sistema tramite SLIP, è necessario avviare un profilo di configurazione *ANS SLIP. Per creare o modificare un profilo di configurazione SLIP, si utilizza il comando Gestione Point-to-Point TCP/IP (WRKTCPPTP). Per avviare un profilo di configurazione, si utilizza il comando Avvio Point-to-Point TCP/IP (STRTCPPTP) o un'opzione dal

pannello WRKTCPPTP. Quando viene inviato il sistema, l'autorizzazione pubblica per i comandi STRTCPPTP e ENDTCPPTP è *EXCLUDE. Le opzioni per aggiungere, modificare e cancellare profili di configurazione SLIP sono disponibili solo se si ha l'autorizzazione speciale *IOSYSCFG. Come responsabile della sicurezza, è possibile utilizzare sia l'autorizzazione al comando che l'autorizzazione speciale per stabilire chi può configurare il sistema in modo da consentire collegamenti in entrata.

Protezione di un collegamento SLIP in entrata

Se si desidera convalidare sistemi che effettuano collegamenti in entrata al proprio sistema, si vuole che il sistema richiedente invii un ID utente e una parola d'ordine. Il proprio sistema può quindi verificare l'ID utente e la parola d'ordine. Se l'ID utente e la parola d'ordine non sono validi, il proprio sistema può respingere la richiesta di sessione.

Per impostare una convalida del collegamento in entrata, attenersi alle seguenti istruzioni:

__ Passo 1. Creare un profilo utente che il sistema richiedente può utilizzare per stabilire il collegamento. L'ID utente e la parola d'ordine che il richiedente invia devono corrispondere a questo nome profilo utente e alla parola d'ordine.

Nota: perché il sistema esegua la convalida della parola d'ordine, il valore di sistema QSECURITY deve essere impostato su 20 o un valore superiore.

Come ulteriore protezione, si desidera probabilmente creare profili utente in modo specifico per stabilire collegamenti SLIP. I profili utente dovrebbero avere autorizzazione limitata nel sistema. Se non si intende utilizzare i profili per alcuna funzione tranne che per stabilire collegamenti SLIP, è possibile impostare i seguenti valori nei profili utente:

- Un menu iniziale (INLMNU) con valore *SIGNOFF
- Un programma iniziale (INLPGM) con valore *NONE.
- Possibilità limitate (LMTCPB) con valore *YES

Questi valori impediscono a chiunque di collegarsi in modo interattivo al profilo utente.

__ Passo 2. Creare un elenco di autorizzazioni relativo al sistema per controllare quando un richiedente tenta di stabilire un collegamento SLIP.

Nota: si specifica questo elenco di autorizzazioni nel campo *Elenco autorizzazioni di accesso al sistema* quando si crea o si modifica il profilo SLIP. (Consultare il passo 4.)

__ Passo 3. Utilizzare il comando Aggiunta voce lista di autorizzazioni (ADDAUTLE) per aggiungere il profilo utente creato nel passo 1 all'elenco di autorizzazioni. E' possibile creare un elenco di autorizzazioni univoco per ogni profilo di configurazione point-to-point oppure si può creare un elenco di autorizzazioni condiviso da diversi profili di configurazione.

__ Passo 4. Utilizzare il comando WRKTCPPTP per configurare un profilo *ANS point-to-point TCP/IP con le seguenti caratteristiche:

- Il profilo di configurazione deve utilizzare uno script di finestra di dialogo per il collegamento che includa la funzione di convalida utente. La convalida utente include l'accettazione di ID utente e

parola d'ordine dal richiedente e la relativa convalida. Il sistema viene inviato con diversi script di finestra di dialogo di esempio che forniscono questa funzione.

- Il profilo di configurazione deve specificare il nome dell'elenco di autorizzazioni creato nel passo 2. L'ID utente che lo script di finestra di dialogo per il collegamento riceve deve trovarsi nell'elenco di autorizzazioni.

Tenere a mente che il valore della configurazione della sicurezza del collegamento in entrata è influenzato dalle pratiche e dalle funzioni relative alla sicurezza dei sistemi che effettuano il collegamento in entrata. Se si richiedono ID utente e parola d'ordine, lo script della finestra di dialogo per il collegamento sul sistema richiedente deve inviare tali ID utente e parola d'ordine. Alcuni sistemi, come ad esempio i server iSeries, forniscono un metodo sicuro per la memorizzazione degli ID utente e delle parole d'ordine. ("Sicurezza e sessioni di collegamento in uscita" a pagina 135 descrive il metodo.) Altri sistemi memorizzano l'ID utente e parola d'ordine nello script che potrebbe essere accessibile a chiunque sappia dove trovare lo script sul sistema.

A causa delle differenti pratiche e funzioni relative alla sicurezza dei propri partner di comunicazioni, si potrebbe voler creare profili di configurazione differenti per ambienti di richiesta differenti. Si utilizza il comando STRTCPPTP per impostare il sistema in modo che accetti una sessione per un profilo di configurazione specifico. E' possibile avviare sessioni per alcuni profili di configurazione solo a determinate ore del giorno, ad esempio. Si potrebbe utilizzare il controllo di sicurezza per registrare l'attività per i profili utente associati.

Prevenzione dell'accesso ad altri sistemi da parte di utenti del collegamento in entrata

In base alla configurazione di rete e di sistema, un utente che avvia un collegamento SLIP potrebbe essere in grado di accedere ad un altro sistema nella rete senza collegarsi al sistema. Ad esempio, un utente potrebbe stabilire un collegamento SLIP ad un sistema. Quindi l'utente potrebbe stabilire un collegamento FTP ad un altro sistema nella stessa rete che non consente collegamento in entrata.

E' possibile impedire ad un utente SLIP di accedere ad altri sistemi nella rete specificando N (No) per il campo *Consentire inoltro datagramma IP* nel profilo di configurazione. Questo impedisce ad un utente di accedere alla rete prima di collegarsi al sistema. Tuttavia, dopo che l'utente è riuscito a collegarsi al sistema, il valore di inoltro del datagramma non ha alcun effetto. Non limita la capacità dell'utente di utilizzare un'applicazione TCP/IP sul sistema iSeries (come ad esempio FTP o TELNET), per stabilire un collegamento ad un altro sistema nella rete.

Controllo di sessioni di collegamento in uscita

Prima che qualcuno possa utilizzare SLIP per stabilire un collegamento in uscita dal sistema, è necessario avviare un profilo di configurazione *DIAL SLIP. Per creare o modificare un profilo di configurazione SLIP, si utilizza il comando WRKTCPPTP. Per avviare un profilo di configurazione, si utilizza il comando Avvio Point-to-Point TCP/IP (STRTCPPTP) o un'opzione dal pannello WRKTCPPTP. Quando viene inviato il sistema, l'autorizzazione pubblica per i comandi STRTCPPTP e ENDTCPPTP è *EXCLUDE. Le opzioni per aggiungere, modificare e cancellare profili di configurazione SLIP sono disponibili solo se si ha l'autorizzazione speciale *IOSYSCFG. Come responsabile della sicurezza, è

possibile utilizzare sia l'autorizzazione al comando che l'autorizzazione speciale per stabilire chi può configurare il sistema in modo da consentire collegamenti in uscita.

Sicurezza e sessioni di collegamento in uscita

Gli utenti sul sistema iSeries potrebbero voler stabilire collegamenti in uscita verso sistemi che richiedono la convalida utente. Lo script di finestra di dialogo per il collegamento sul server iSeries deve inviare un ID utente ed una parola d'ordine al sistema remoto. I server iSeries forniscono un metodo sicuro per memorizzare quella parola d'ordine. La parola d'ordine non deve essere memorizzata nello script di finestra di dialogo per il collegamento.

Note:

1. Anche se il sistema memorizza la parola d'ordine per il collegamento in formato codificato, il sistema decodifica la parola d'ordine prima di inviarla. Le parole d'ordine SLIP, come le parole d'ordine FTP e TELNET, vengono inviate non codificate ("in chiaro"). Tuttavia, a differenza di FTP e TELNET, la parola d'ordine SLIP viene inviata prima che i sistemi stabiliscano la modalità TCP/IP.

   Poiché SLIP utilizza un collegamento point-to-point in modalità asincrona, il rischio per la sicurezza quando si inviano parole d'ordine non codificate è differente dal rischio con le parole d'ordine FTP e TELNET. Parole d'ordine FTP e TELNET non codificate potrebbero essere inviate come traffico IP su una rete e sono, quindi, vulnerabili allo sniffing elettronico. La trasmissione della parola d'ordine SLIP è protetta quanto la connessione telefonica tra i due sistemi.
2. Il file predefinito per la memorizzazione degli script di finestra di dialogo per il collegamento SLIP è QUSRSYS/QATOCPPSCR. L'autorizzazione pubblica per questo file è *USE, che impedisce agli utenti pubblici di modificare gli script di finestra di dialogo per il collegamento predefiniti.

Quando si crea un profilo di collegamento per una sessione remota che richiede convalida, effettuare quanto segue:

__ Passo 1. Assicurarsi che il valore di sistema Conservazione dati sicurezza server (QRETSVRSEC) sia 1 (Sì). Questo valore di sistema determina se sarà consentita la memorizzazione delle parole d'ordine che possono essere decodificate in un'area protetta nel sistema.

__ Passo 2. Utilizzare il comando WRKTCPPTP per creare un profilo di configurazione con le seguenti caratteristiche:

- Come modalità del profilo di configurazione, specificare *DIAL.
- Come *Nome accesso servizio remoto*, specificare l'ID utente previsto dal sistema remoto. Ad esempio, se ci si sta collegando ad un altro server iSeries, specificare il nome profilo utente in quel server iSeries.
- Come *Parola d'ordine accesso servizio remoto*, specificare la parola d'ordine prevista dal sistema remoto per questo ID utente. Nel proprio server iSeries, questa parola d'ordine è memorizzata in un'area protetta in un formato che è possibile decodificare. I nomi e le parole d'ordine che si assegnano per i profili di configurazione sono associati al profilo utente QTCP. I nomi e le parole d'ordine non sono accessibili con alcun comando o interfaccia utente. Solo programmi di sistema registrati possono accedere a queste informazioni sulla parola d'ordine.

  Nota: tenere a mente che le parole d'ordine per i propri profili di collegamento non vengono salvate quando si salvano i file di configurazione TCP/IP. Per salvare le parole d'ordine SLIP, è

necessario utilizzare il comando Salvataggio dati sicurezza (SAVSECDTA) per salvare il profilo utente QTCP.

- Come script di finestra di dialogo per il collegamento, specificare uno script che invia l'ID utente e la parola d'ordine. Il sistema viene consegnato con diversi script di finestra di dialogo di esempio che forniscono questa funzione. Quando il sistema esegue lo script, richiama la parola d'ordine, la decodifica e la invia al sistema remoto.

Considerazioni sulla sicurezza per il protocollo point-to-point

Il protocollo point-to-point (PPP) è disponibile come parte di TCP/IP. PPP è uno standard industriale per i collegamenti point-to-point che fornisce ulteriore funzionalità rispetto a quella disponibile con SLIP.

Con PPP, il server iSeries può avere collegamenti ad alta velocità direttamente ad un Internet Service Provider o ad altri sistemi in un'intranet o extranet. Le LAN remote possono effettuare reali collegamenti in entrata al server iSeries.

Si tenga a mente che PPP, come SLIP, fornisce un collegamento di rete al server iSeries. Un collegamento PPP fondamentalmente accompagna il richiedente alla porta del sistema. Il richiedente ha ancora bisogno di un ID utente e una parola d'ordine per entrare nel sistema e collegarsi ad un server TCP/IP come TELNET o FTP. Quelle che seguono sono considerazioni sulla sicurezza con questa nuova capacità di collegamento:

Nota: si configura PPP utilizzando iSeries Navigator su una stazione di lavoro IBM iSeries Access per Windows.

- PPP fornisce la capacità di avere collegamenti dedicati (dove lo stesso utente ha sempre lo stesso indirizzo IP). Con un indirizzo dedicato, si ha il potenziale per lo spoofing IP (un falso sistema che si spaccia per un sistema garantito con un indirizzo IP noto). Tuttavia, le potenziate capacità di autenticazione che PPP fornisce, sono utili nella protezione contro lo spoofing IP.
- Con PPP, come con SLIP, si creano profili di collegamento che hanno un nome utente ed una parola d'ordine associati. Tuttavia, a differenza di SLIP, l'utente non ha bisogno di avere un profilo utente ed una parola d'ordine validi. Il nome utente e la parola d'ordine non sono associati ad un profilo utente. Invece, si utilizzano elenchi di convalida per l'autenticazione PPP. Inoltre, PPP non richiede uno script per il collegamento. L'autenticazione (interscambio di nome utente e parola d'ordine) fa parte dell'architettura PPP ed avviene ad un livello inferiore rispetto allo SLIP.
- Con PPP, si ha l'opzione per l'utilizzo di CHAP (challenge handshake authentication protocol). Non ci si dovrà più preoccupare di un eventuale utente non autorizzato che ottiene tramite sniffing le parole d'ordine poiché CHAP codifica nomi utente e parole d'ordine.

  Il collegamento PPP utilizza CHAP solo se ambo le parti dispongono di supporto CHAP. Durante lo scambio di segnali per impostare le comunicazioni tra due modem, i due sistemi negoziano. Per esempio, se SYSTEMA supporta CHAP e SYSTEMB no, SYSTEMA può negare la sessione o accettare di utilizzare un nome utente e una parola d'ordine non codificate. L'accettazione dell'utilizzo di nome utente e parola d'ordine non codificati è conosciuta anche come fine negoziazione. La decisione di terminare la negoziazione è un'opzione di configurazione. Sull'intranet, ad esempio, dove è noto che tutti i sistemi hanno capacità CHAP, si dovrebbe configurare il profilo di collegamento in modo che

non metterà fine alla negoziazione. In un collegamento pubblico in cui il sistema sta effettuando un collegamento in uscita, si potrebbe voler porre fine alla negoziazione.

Il profilo del collegamento per PPP fornisce la capacità di specificare indirizzi IP validi. E' possibile, ad esempio, indicare che si prevede un indirizzo specifico o una gamma di indirizzi per uno specifico utente. Questa capacità, insieme alla possibilità di parole d'ordine codificate, fornisce ulteriore protezione contro lo spoofing.

Come ulteriore protezione contro tentativi di falsificazione o sfruttamento dell'identità in una sessione attiva, è possibile configurare PPP perché effettui la rinegoziazione ad intervalli designati. Ad esempio, mentre è attiva una sessione PPP, il server iSeries potrebbe negoziare con l'altro sistema per quanto riguarda utente e parola d'ordine. Effettua questa operazione ogni 15 minuti per assicurare che si tratti dello 'stesso profilo di collegamento'. (L'utente finale non sarà consapevole di questa attività di rinegoziazione. I sistemi scambiano nomi e parole d'ordine al di sotto del livello visualizzato dall'utente finale.)

Con PPP, è realistico prevedere che LAN remote possano stabilire un collegamento in entrata al server iSeries e alla rete estesa. In questo ambiente, l'inoltro IP attivato è probabilmente un requisito. L'inoltro IP ha il potenziale di consentire ad un intruso di navigare nella rete. Tuttavia, PPP ha protezioni più potenti (come ad esempio la codifica di parole d'ordine e la convalida dell'indirizzo IP). Questo rende meno probabile che un intruso possa stabilire un collegamento di rete in primo luogo.

Per ulteriori informazione su PPP, consultare l'iSeries Information Center.

Considerazioni sulla sicurezza per l'utilizzo del server Bootstrap Protocol

BOOTP (Bootstrap Protocol) fornisce un metodo dinamico per l'associazione di stazioni di lavoro a server e l'assegnazione di indirizzi IP della stazione di lavoro e origini IPL (initial program load).

BOOTP è un protocollo TCP/IP utilizzato per consentire ad una stazione di lavoro priva di supporti magnetici (client) di richiedere un file contenente il codice iniziale da un server sulla rete. Il server BOOTP si pone in ascolto sulla ben nota porta server BOOTP 67. Quando si riceve una richiesta client, il server ricerca l'indirizzo IP definito per il client e restituisce una risposta al client con l'indirizzo IP del client ed il nome del file di caricamento. Il cliente quindi avvia una richiesta TFTP al server per il file di caricamento. La corrispondenza tra l'indirizzo hardware del client e l'indirizzo IP è conservata nella tabella BOOTP sul server iSeries.

Prevenzione dell'accesso BOOTP

Se non si dispone di alcun client thin collegato alla rete, non è necessario eseguire il server BOOTP sul sistema. Può essere utilizzato per altre unità, ma la soluzione più opportuna per quelle unità è utilizzare DHCP. Effettuare le seguenti operazioni per impedire l'esecuzione del server BOOTP:

__ Passo 1. Per impedire l'avvio automatico dei lavori del server BOOTP quando si avvia TCP/IP, immettere quanto segue:

```
CHGBPA AUTOSTART(*NO)
```

Note:

1. AUTOSTART(*NO) è il valore predefinito.

2. “Controllo dei server TCP/IP con avvio automatico” a pagina 130 fornisce ulteriori informazioni sul controllo di quali server TCP/IP si avviano automaticamente.

__ Passo 2. Per impedire che qualcuno associ un'applicazione utente, come ad esempio un'applicazione socket, alla porta che il sistema normalmente utilizza per BOOTP, effettuare quanto segue:

Nota: poiché DHCP e BOOTP utilizzano lo stesso numero porta, questo bloccherà anche la porta che viene utilizzata da DHCP. Non limitare la porta se si desidera utilizzare DHCP.

__ Passo a. Immettere `GO CFGTCP` per visualizzare il menu Configurazione TCP/IP.

__ Passo b. Selezionare l'opzione 4 (Gestione limitazioni porta TCP/IP).

__ Passo c. Sul pannello Gestione limitazioni porta TCP/IP, specificare l'opzione 1 (Aggiunta).

__ Passo d. Per il valore inferiore dell'intervallo porta, specificare `67`.

__ Passo e. Per il valore superiore dell'intervallo porta, specificare `*ONLY`.

Note:

1. La limitazione porta diventa effettiva al successivo avvio di TCP/IP. Se TCP/IP è attivo quando si impostano le limitazioni porta, sarebbe opportuno arrestarlo e riavviarlo.
2. RFC1700 fornisce informazioni sulle assegnazioni comuni del numero porta.

__ Passo f. Per il protocollo, specificare `*UDP`.

__ Passo g. Per il campo del profilo utente, specificare un nome profilo utente protetto sul sistema. (Un profilo utente protetto è un profilo utente che non possiede programmi che adottano l'autorizzazione e che non dispone di una parola d'ordine nota ad altri utenti). Limitando la porta a un utente specifico, si escludono automaticamente tutti gli altri utenti.

Protezione del server BOOTP

Il server BOOTP non fornisce accesso diretto al sistema iSeries e quindi rappresenta un rischio limitato per la sicurezza. La principale preoccupazione come responsabile della sicurezza è quella di assicurare che le informazioni corrette siano associate al client thin corretto. In altre parole, un malintenzionato potrebbe modificare la tabella BOOTP e causare il funzionamento non corretto o il mancato funzionamento dei client thin.

Per gestire il server BOOTP e la tabella BOOTP, è necessario disporre dell'autorizzazione speciale *IOSYSCFG. E' necessario controllare con attenzione i profili utente con autorizzazione speciale *IOSYSCFG sul sistema.

Considerazioni sulla sicurezza per l'utilizzo del server DHCP

DHCP (Dynamic host configuration protocol) fornisce una framework per il passaggio delle informazioni sulla configurazione ad host su una rete TCP/IP. Per le stazioni di lavoro client, DHCP può fornire una funzione simile alla configurazione automatica. Un programma abilitato DHCP sulla stazione di lavoro client trasmette una richiesta di informazioni sulla configurazione. Se il server DHCP è in esecuzione sul server iSeries, il server risponde alla richiesta inviando le informazioni di cui la stazione di lavoro client ha bisogno per configurare correttamente TCP/IP.

E' possibile utilizzare DHCP per rendere più semplice agli utenti il primo collegamento al server iSeries. Questo avviene perché l'utente non deve immettere le informazioni sulla configurazione TCP/IP. E' possibile inoltre utilizzare DHCP per ridurre il numero di indirizzi TCP/IP interni necessari in una sottorete. Il server DHCP può temporaneamente assegnare indirizzi IP ad utenti attivi (dal relativo lotto di indirizzi IP).

Per i client thin, è possibile utilizzare DHCP al posto di BOOTP. DHCP fornisce maggiore funzionalità rispetto a BOOTP e può supportare la configurazione dinamica sia dei client thin che dei PC.

Prevenzione accesso DHCP

Se *non* si desidera che alcuno utilizzi il server DHCP sul sistema, effettuare quanto segue:

1. Per impedire l'avvio automatico di lavori server DHCP quando si avvia TCP/IP, immettere quanto segue:

   ```
   CHGDHCPA AUTOSTART(*NO)
   ```

   Note:

   1. AUTOSTART(*NO) è il valore predefinito.
   2. "Controllo dei server TCP/IP con avvio automatico" a pagina 130 fornisce ulteriori informazioni sul controllo di quali server TCP/IP si avviano automaticamente.
2. Per impedire che qualcuno associ un'applicazione utente, come ad esempio un'applicazione socket, alla porta che il sistema normalmente utilizza per DHCP, effettuare quanto segue:
   a. Immettere `GO CFGTCP` per visualizzare il menu Configurazione TCP/IP.
   b. Selezionare l'opzione 4 (Gestione limitazioni porta TCP/IP).
   c. Sul pannello Gestione limitazioni porta TCP/IP, specificare l'opzione 1 (Aggiunta).
   d. Per il valore inferiore dell'intervallo porta, specificare `67`.
   e. Per il valore superiore dell'intervallo porta, specificare `68`.

      Note:

      1. La limitazione porta diventa effettiva al successivo avvio di TCP/IP. Se TCP/IP è attivo quando si impostano le limitazioni porta, sarebbe opportuno arrestarlo e riavviarlo.
      2. RFC1700 fornisce informazioni sulle assegnazioni comuni del numero porta.

   f. Per il protocollo, specificare `*UDP`.
   g. Per il campo del profilo utente, specificare un nome profilo utente protetto sul sistema. (Un profilo utente protetto è un profilo utente che non possiede

programmi che adottano l'autorizzazione e che non dispone di una parola d'ordine nota ad altri utenti). Limitando la porta a un utente specifico, si escludono automaticamente tutti gli altri utenti.

Protezione del server DHCP

Quelle che seguono sono considerazioni sulla sicurezza quando si decide di eseguire DHCP sul sistema iSeries:

- Limitare il numero di utenti con autorizzazione alla gestione di DHCP. La gestione di DHCP richiede la seguente autorizzazione:
  - Autorizzazione speciale *IOSYSCFG
  - Autorizzazione *RW ai seguenti file:

    ```
    /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
    /QIBM/UserData/OS400/DHCP/dhcprd.cfg
    ```
- Valutare l'accessibilità fisica della LAN. Un estraneo potrebbe facilmente penetrare nell'ubicazione con un portatile e collegarlo fisicamente alla LAN? Se questo è un rischio, DHCP fornisce la capacità di creare un elenco di client (indirizzi hardware) che il server DHCP configurerà. Quando si utilizza questa funzione, si annullano alcune dei benefici di produttività che DHCP fornisce agli amministratori di rete. Tuttavia, si impedisce al sistema di configurare stazioni di lavoro sconosciute.
- Se possibile, utilizzare un lotto di indirizzi IP che sia riutilizzabile (non progettato per Internet). Questo serve anche ad impedire che una stazione di lavoro fuori della rete ottenga dal server informazioni sulla configurazione utilizzabili.
- Utilizzare i punti di uscita DHCP se è necessaria ulteriore protezione di sicurezza. La seguente è una panoramica dei punti di uscita e delle relative capacità. L'*iSeries System API Reference* descrive come utilizzare questi punti di uscita.

  Immissione porta
  Il sistema richiama il programma di uscita ogni qualvolta legge un pacchetto di dati dalla porta 67 (la porta DHCP). Il programma di uscita riceve il pacchetto di dati completo. Può decidere se il sistema dovrebbe elaborare o eliminare il pacchetto. E' possibile utilizzare questo punto di uscita quando le funzioni di controllo DHCP esistenti non sono sufficienti per le proprie esigenze.

  Assegnazione indirizzo
  Il sistema richiama il programma di uscita ogni qualvolta DHCP assegna formalmente un indirizzo ad un client.

  Rilascio indirizzo
  Il sistema richiama il programma di uscita ogni qualvolta DHCP rilascia formalmente un indirizzo e lo reinserisce nel lotto di indirizzi.

Considerazioni sulla sicurezza per l'utilizzo del server TFTP

TFTP (Trivial file transfer protocol) fornisce un trasferimento file di base senza autenticazione utente. TFTP funziona con BOOTP (Bootstrap Protocol) o DHCP (Dynamic Host Configuration Protocol).

Il client si collega inizialmente al server BOOTP o al server DHCP. Il server BOOTP o il server DHCP replica con l'indirizzo IP del client ed il nome del file di

caricamento. Il cliente quindi avvia una richiesta TFTP al server per il file di caricamento. Quando il client completa lo scaricamento del file di caricamento, chiude la sessione TFTP.

Prevenzione accesso TFTP

Se non si dispone di alcun client thin collegato alla rete, probabilmente non è necessario eseguire il server TFTP sul sistema. Effettuare le seguenti operazioni per impedire l'esecuzione del server TFTP:

__ Passo 1. Per impedire l'avvio automatico di lavori server TFTP quando si avvia TCP/IP, immettere quanto segue:

```
CHGTFTPA AUTOSTART(*NO)
```

Note:

1. AUTOSTART(*NO) è il valore predefinito.
2. "Controllo dei server TCP/IP con avvio automatico" a pagina 130 fornisce ulteriori informazioni sul controllo di quali server TCP/IP si avviano automaticamente.

__ Passo 2. Per impedire che qualcuno associ un'applicazione utente, come ad esempio un'applicazione socket, alla porta che il sistema normalmente utilizza per TFTP, effettuare quanto segue:

- __ Passo a. Immettere `GO CFGTCP` per visualizzare il menu Configurazione TCP/IP.
- __ Passo b. Selezionare l'opzione 4 (Gestione limitazioni porta TCP/IP).
- __ Passo c. Sul pannello Gestione limitazioni porta TCP/IP, specificare l'opzione 1 (Aggiunta).
- __ Passo d. Per il valore inferiore dell'intervallo porta, specificare `69`.
- __ Passo e. Per il valore superiore dell'intervallo porta, specificare `*ONLY`.

  Note:

  1. La limitazione porta diventa effettiva al successivo avvio di TCP/IP. Se TCP/IP è attivo quando si impostano le limitazioni porta, sarebbe opportuno arrestarlo e riavviarlo.
  2. RFC1700 fornisce informazioni sulle assegnazioni comuni del numero porta.
- __ Passo f. Per il protocollo, specificare `*UDP`.
- __ Passo g. Per il campo del profilo utente, specificare un nome profilo utente protetto sul sistema. (Un profilo utente protetto è un profilo utente che non possiede programmi che adottano l'autorizzazione e che non dispone di una parola d'ordine nota ad altri utenti). Limitando la porta a un utente specifico, si escludono automaticamente tutti gli altri utenti.

Protezione del server TFTP

Per impostazione predefinita, il server TFTP fornisce accesso molto limitato al sistema iSeries. E' specificamente configurato per fornire il codice iniziale per client thin. Come responsabile della sicurezza, si dovrebbero conoscere le seguenti caratteristiche del server TFTP:

- Il server TFTP non richiede autenticazione (un ID utente ed una parola d'ordine). Tutti i lavori TFTP vengono eseguiti tramite il profilo utente QTFTP. Il profilo utente QTFTP non dispone di parola d'ordine. Quindi, non è disponibile per il collegamento interattivo. Il profilo utente QTFTP non ha alcuna autorizzazione speciale, né è esplicitamente autorizzato alle risorse di sistema. Utilizza l'autorizzazione pubblica per accedere alle risorse di cui ha bisogno per i client thin.
- Quando il server TFTP arriva, è configurato per accedere all'indirizzario che contiene le informazioni sul client thin. E' necessario disporre di *PUBLIC o di QTFTP autorizzato alla lettura o alla scrittura per quell'indirizzario. Per scrivere nell'indirizzario è necessario che sia specificato *CREATE nel parametro "Concessione file di scrittura" del comando CHGTFTPA. Per scrivere in un file esistente è necessario avere *REPLACE specificato nel parametro "Concessione file di scrittura" di CHGTFTPA. *CREATE consente di sostituire i file esistenti o crearne di nuovi. *REPLACE consente solo di sostituire i file esistenti.

  Un client TFTP non può accedere ad alcun altro indirizzario a meno che non si definisca esplicitamente l'indirizzario con il comando Modifica attributi TFTP (CHGTFTPA). Quindi, se un utente locale o remoto tenta di avviare una sessione TFTP per il sistema, la capacità dell'utente di accedere ad informazioni o provocare danni è molto limitata.
- Se si sceglie di configurare il server TFTP in modo da fornire altri servizi oltre alla gestione dei client thin, è possibile definire un programma di uscita per valutare ed autorizzare ogni richiesta TFTP. Il server TFTP un'uscita convalida richiesta simile all'uscita disponibile per il server FTP. Per ulteriori informazioni, consultare l'iSeries Information Center—>Rete—>TCP/IP—>TFTP. Consultare "Requisiti necessari e informazioni correlate" a pagina xii per informazioni sull'accesso all'iSeries Information Center.

Considerazioni sulla sicurezza per l'utilizzo del server REXEC

Il server REXEC (Remote EXECution server) riceve ed esegue comandi da un client REXEC. Un client REXEC in genere è un'applicazione PC o UNIX che supporta l'invio di comandi REXEC. Il supporto fornito da questo server è simile alla capacità che è disponibile quando si usa il comando secondario RCMD (Comando remoto) per il server FTP.

Prevenzione dell'accesso REXEC

Se non si desidera che il proprio server iSeries accetti comandi da un client REXEC, effettuare quanto segue per impedire l'esecuzione del server REXEC:

__ Passo 1. Per impedire l'avvio automatico dei lavori del server REXEC quando si avvia TCP/IP, immettere quanto segue:

```
CHGRXCA AUTOSTART(*NO)
```

Note:

1. AUTOSTART(*NO) è il valore predefinito.
2. "Controllo dei server TCP/IP con avvio automatico" a pagina 130 fornisce ulteriori informazioni sul controllo di quali server TCP/IP si avviano automaticamente.

__ Passo 2. Per impedire che qualcuno associ un'applicazione utente, come ad esempio un'applicazione socket, alla porta che il sistema normalmente utilizza per REXEC, effettuare quanto segue:

__ Passo a. Immettere `GO CFGTCP` per visualizzare il menu Configurazione TCP/IP.

__ Passo b. Selezionare l'opzione 4 (Gestione limitazioni porta TCP/IP).

__ Passo c. Sul pannello Gestione limitazioni porta TCP/IP, specificare l'opzione 1 (Aggiunta).

__ Passo d. Per il valore inferiore dell'intervallo porta, specificare 512.

__ Passo e. Per il valore superiore dell'intervallo porta, specificare *ONLY.

__ Passo f. Per il protocollo, specificare *TCP.

__ Passo g. Per il campo del profilo utente, specificare un nome profilo utente protetto sul sistema. (Un profilo utente protetto è un profilo utente che non possiede programmi che adottano l'autorizzazione e che non dispone di una parola d'ordine nota ad altri utenti). Limitando la porta a un utente specifico, si escludono automaticamente tutti gli altri utenti.

Note:

1. La limitazione porta diventa effettiva al successivo avvio di TCP/IP. Se TCP/IP è attivo quando si impostano le limitazioni porta, sarebbe opportuno arrestarlo e riavviarlo.
2. RFC1700 fornisce informazioni sulle assegnazioni comuni del numero porta.

Protezione del server REXEC

Quelle che seguono sono considerazioni utili quando si decide di eseguire il Remote EXECution server sul proprio sistema:

- Una richiesta REXCD include un ID utente, una parola d'ordine ed il comando da eseguire. Si applica il normale controllo di autorizzazione ed autenticazione del server iSeries:
  - La combinazione di profilo utente e parola d'ordine deve essere valida.
  - Il sistema applica il valore *Possibilità limitate* (LMTCPB) per il profilo utente.
  - L'utente deve essere autorizzato al comando e a tutte le risorse che il comando utilizza.
- Il server REXEC fornisce punti di uscita simili ai punti di uscita disponibili per il server FTP. E' possibile utilizzare il punto di uscita Convalida per valutare il comando e decidere se consentirlo. Per ulteriori informazioni, consultare l'iSeries Information Center—>Rete—>TCP/IP—>REXEC. Consultare "Requisiti necessari e informazioni correlate" a pagina xii per informazioni sull'accesso all'iSeries Information Center.
- Quando si decide di eseguire il server REXEC, si effettua l'esecuzione al di fuori di qualsisi controllo accesso menu disponibile sul sistema. E' necessario garantire che lo schema di autorizzazione all'oggetto sia adeguato a proteggere le risorse.

Considerazioni sulla sicurezza per l'utilizzo di RouteD

Il server RouteD (Route Daemon) fornisce supporto per il RIP (Routing Information Protocol) sui server iSeries. RIP è il protocollo di instradamento più diffuso. E' un Interior Gateway Protocol che assiste TCP/IP nell'instradamento di pacchetti IP all'interno di un sistema autonomo.

RouteD è progettato per aumentare l'efficienza del traffico di rete consentendo ai sistemi entro una rete garantita di aggiornarsi reciprocamente con le informazioni

correnti sull'instradamento. Quando si esegue RouteD, il sistema può ricevere aggiornamenti da altri sistemi partecipanti circa la modalità di instradamento delle trasmissioni (pacchetti). Perciò, se il server RouteD è accessibile ad un hacker, l'hacker potrebbe utilizzarlo per reinstradare i pacchetti attraverso un sistema che può eseguire lo sniffing o la modifica di quei pacchetti. Quelli che seguono sono suggerimenti per la sicurezza di RouteD:

- I server iSeries utilizzano RIPv1, che non fornisce alcun metodo di autenticazione dei router. E' progettato per l'utilizzo entro una rete garantita. Se il sistema si trova in una rete con altri sistemi che non vengono "riconosciuti", non si dovrebbe eseguire il server RouteD. Per garantire che il server RouteD non si avvii automaticamente, immettere quanto segue:

  ```
  CHGRTDA AUTOSTART(*NO)
  ```

  Note:

  1. AUTOSTART(*NO) è il valore predefinito.
  2. "Controllo dei server TCP/IP con avvio automatico" a pagina 130 fornisce ulteriori informazioni sul controllo di quali server TCP/IP si avviano automaticamente.
- Assicurarsi di controllare chi può modificare la configurazione RouteD, che richiede l'autorizzazione speciale *IOSYSCFG.
- Se il sistema fa parte di più di una rete (ad esempio, un'intranet ed Internet), è possibile configurare il server RouteD per inviare ed accettare aggiornamenti solo con la rete protetta.

Considerazioni sulla sicurezza per l'utilizzo del server DNS

Il server DNS (Domain Name System) fornisce la conversione di un nome host in indirizzi IP e viceversa. Sui server iSeries, il server DNS ha lo scopo di fornire la conversione indirizzi per la rete protetta, interna (intranet).

Prevenzione dell'accesso DNS

Se *non* si desidera che alcuno utilizzi il server DNS sul sistema, effettuare quanto segue:

1. Per impedire l'avvio automatico di lavori server DNS quando si avvia TCP/IP, immettere quanto segue:

   ```
   CHGDNSA AUTOSTART(*NO)
   ```

   Note:

   1. AUTOSTART(*NO) è il valore predefinito.
   2. "Controllo dei server TCP/IP con avvio automatico" a pagina 130 fornisce ulteriori informazioni sul controllo di quali server TCP/IP si avviano automaticamente.
2. Per impedire che qualcuno associ un'applicazione utente, come ad esempio un'applicazione socket, alla porta che il sistema normalmente utilizza per DNS, effettuare quanto segue:
   a. Immettere `GO CFGTCP` per visualizzare il menu Configurazione TCP/IP.
   b. Selezionare l'opzione 4 (Gestione limitazioni porta TCP/IP).
   c. Sul pannello Gestione limitazioni porta TCP/IP, specificare l'opzione 1 (Aggiunta).
   d. Per il valore inferiore dell'intervallo porta, specificare `53`.
   e. Per il valore superiore dell'intervallo porta, specificare `*ONLY`.

Note:

1. La limitazione porta diventa effettiva al successivo avvio di TCP/IP. Se TCP/IP è attivo quando si impostano le limitazioni porta, sarebbe opportuno arrestarlo e riavviarlo.
2. RFC1700 fornisce informazioni sulle assegnazioni comuni del numero porta.

f. Per il protocollo, specificare `*TCP`.

g. Per il campo del profilo utente, specificare un nome profilo utente protetto sul sistema. (Un profilo utente protetto è un profilo utente che non possiede programmi che adottano l'autorizzazione e che non dispone di una parola d'ordine nota ad altri utenti). Limitando la porta a un utente specifico, si escludono automaticamente tutti gli altri utenti.

h. Ripetere i passi da 2c a 2g per *UDP (User datagram protocol).

Protezione del server DNS

Quelle che seguono sono considerazioni sulla sicurezza quando si decide di eseguire DNS sul sistema iSeries:

- La funzione che il server DNS fornisce è la conversione dell'indirizzo IP e la conversione del nome. Non fornisce alcun accesso agli oggetti nel sistema iSeries. Il rischio quando un estraneo accede al server DNS è che il server fornisca una facile visualizzazione della topologia della rete. Il DNS potrebbe risparmiare ad un hacker un pò di fatica nell'individuare indirizzi di potenziali bersagli. Tuttavia, il DNS non fornisce informazioni che serviranno a penetrare in quei sistemi bersaglio.
- In genere, si utilizza il server DNS iSeries per intranet. Perciò, probabilmente non si ha necessità di limitare la capacità di effettuare query al DNS. Tuttavia, si potrebbero, ad esempio avere diverse sottoreti nell'ambito dell'intranet. Si potrebbe non desiderare che utenti da una sottorete differente siano in grado di effettuare query al DNS nel server iSeries. Un'opzione di sicurezza di DNS consente di limitare l'accesso ad un dominio principale. Utilizzare iSeries Navigator per specificare indirizzi IP a cui il server DNS dovrebbe rispondere.

  Un'altra opzione di sicurezza consente di specificare quali server secondari possono copiare informazioni dal server DNS principale. Quando si utilizza questa opzione, il server accetterà richieste di trasferimento zona (una richiesta di copiare informazioni) solo dai server secondari esplicitamente elencati.
- Accertarsi di limitare con attenzione la capacità di modificare il file di configurazione per il server DNS. I malintenzionati potrebbero, ad esempio, modificare il file DNS in modo che punti ad un indirizzo IP esterno alla rete. Potrebbero simulare un server nella rete e, forse, ottenere accesso ad informazioni riservate da utenti che utilizzano il server.

Considerazioni sulla sicurezza per l'utilizzo del server HTTP per iSeries

Il server HTTP fornisce client browser World Wide Web con accesso ad oggetti multimediali del server iSeries, come ad esempio documenti HTML (Hypertext Markup Language). Supporta anche la specifica *CGI (Common Gateway Interface)*. Programmatori di applicazioni possono scrivere programmi CGI per estendere la funzionalità del server.

L'amministratore può utilizzare Internet Connection Server o IBM HTTP server for iSeries per eseguire più server contemporaneamente sullo stesso server iSeries.

Ogni server in esecuzione è detto **istanza del server**. Ogni istanza del server ha un nome univoco. L'amministratore controlla quali istanze vengono avviate e cosa può fare ogni istanza.

Nota: è necessario che l'istanza *ADMIN del server HTTP sia in esecuzione quando si utilizza un browser web per configurare o gestire uno qualsiasi dei seguenti elementi:

- Firewall per iSeries
- Internet Connection Server
- Internet Connection Secure Server
- IBM HTTP Server for iSeries

Un utente (visitatore del sito Web) non visualizza mai il pannello Collegamento di un server iSeries. Tuttavia, l'amministratore del server iSeries deve autorizzare esplicitamente tutti i documenti HTML ed i programmi CGI definendoli nelle direttive HTTP. Inoltre, l'amministratore può impostare la sicurezza della risorsa e l'autenticazione utente (ID utente e parola d'ordine) per alcune o per tutte le richieste.

Un attacco da parte di un hacker potrebbe dare come risultato una negazione del servizio al proprio server Web. Il server può individuare un attacco negazione-del-servizio misurando il supero tempo delle richieste di certi client. Se il server non riceve una richiesta dal client, stabilisce che è in corso un attacco di negazione-del-servizio. Questo si verifica dopo aver effettuato il collegamento iniziale del client al server. Il valore predefinito del server è quello di eseguire la rilevazione e la neutralizzazione dell'attacco.

Prevenzione dell'accesso HTTP

Se *non* si desidera che alcuno utilizzi il programma per accedere al sistema, si dovrebbe impedire l'esecuzione del server HTTP. Effettuare le seguenti operazioni.

__ Passo 1. Per impedire l'avvio automatico di lavori server HTTP quando si avvia TCP/IP, immettere quanto segue:

```
CHGHTTPA AUTOSTART(*NO)
```

Note:

1. AUTOSTART(*NO) è il valore predefinito.
2. "Controllo dei server TCP/IP con avvio automatico" a pagina 130 fornisce ulteriori informazioni sul controllo di quali server TCP/IP si avviano automaticamente.

__ Passo 2. Per impostazione predefinita, il lavoro server HTTP utilizza il profilo utente QTMHHTTP. Per impedire l'avvio del server HTTP, impostare lo stato del profilo utente QTMHHTTP su *DISABLED.

Controllo dell'accesso al server HTTP

Lo scopo principale dell'esecuzione di un server HTTP è quello di fornire ai visitatori accesso ad un sito Web sul sistema iSeries. Si può pensare a chi visita il sito Web come a chi legge un annuncio pubblicitario su un giornale commerciale. Il visitatore non è consapevole dell'hardware e del software che consentono l'esecuzione del sito Web, come ad esempio che tipo di server si sta utilizzando e dove è ubicato fisicamente. Di solito, si preferisce non porre alcuna barriera (come ad esempio un pannello Collegamento) tra un potenziale visitatore ed il proprio sito Web. Tuttavia, è possibile che si voglia limitare l'accesso ad alcuni dei documenti o programmi CGI forniti dal proprio sito Web.

E' possibile anche che si desideri che un singolo sistema iSeries fornisca più siti Web logici. Ad esempio, il sistema iSeries può supportare rami differenti della propria attività aziendale che hanno gruppi di clienti differenti. Per ognuno di questi rami dell'attività aziendale, si desidera un sito Web univoco che viene visualizzato in modo totalmente indipendente dal visitatore. Inoltre, potrebbe essere opportuno fornire siti Web interni (un'intranet) con informazioni confidenziali sull'attività aziendale.

Come responsabile della sicurezza, è necessario proteggere il contenuto del sito Web mentre, nello stesso tempo, è necessario accertarsi che le pratiche di sicurezza non influenzino negativamente il valore del sito Web. Inoltre, è necessario assicurarsi che l'attività HTTP non metta a rischio l'integrità del sistema o della rete. Gli argomenti che seguono forniscono suggerimenti per la sicurezza quando si utilizza il programma.

Considerazioni sulla gestione

Quelle che seguono sono alcune considerazioni di sicurezza per la gestione del server Internet.

- Si eseguono funzioni di impostazione e configurazione utilizzando un browser Web e l'istanza *ADMIN. Per alcune funzioni, come ad esempio la creazione di ulteriori istanze sul server, si *deve* utilizzare il server *ADMIN.
- L'URL predefinito per la home page di gestione (l'home page per il server *ADMIN) è pubblicato nella documentazione per prodotti che forniscono funzioni di gestione browser. Perciò, l'URL predefinito probabilmente sarà noto agli hacker e pubblicato nei forum degli hacker, così come sono note e pubblicate le parole d'ordine predefinite per i profili utente fornite da IBM. E' possibile proteggersi da questo rischio in diversi modi:
  - Eseguire l'istanza *ADMIN del server HTTP solo quando è necessario eseguire funzioni di gestione. Non mantenere continuamente in esecuzione l'istanza *ADMIN.
  - Attivare il supporto SSL per l'istanza *ADMIN (utilizzando Digital Certificate Manager). L'istanza *ADMIN utilizza le direttiva di protezione HTTP per richiedere un ID utente ed una parola d'ordine. Quando si utilizza SSL, l'ID utente e la parola d'ordine sono codificati (insieme a tutte le altre informazioni sulla configurazione che vengono visualizzate nei modulo di gestione).
  - Utilizzare un firewall sia per impedire l'accesso al server *ADMIN da Internet che per nascondere i nomi di dominio e sistema, che sono parte dell'URL.
- Quando si eseguono funzioni di gestione, è necessario collegarsi con un profilo utente che abbia l'autorizzazione speciale *IOSYSCFG. Potrebbe essere anche necessaria l'autorizzazione ad oggetti specifici nel sistema, come ad esempio i seguenti:
  - Le librerie o indirizzari che contengono i documenti HTML ed i programmi CGI.
  - Qualsiasi profilo utente a cui si intende passare all'interno delle direttive per il server.
  - Gli ACL (Access Control List) per qualsiasi indirizzario utilizzato dalle direttive.
  - Un oggetto elenco di convalida per la creazione e la manutenzione di ID utente e parole d'ordine.

  Sia con il server *ADMIN che TELNET, si ha la capacità di eseguire funzioni di gestione in remoto, forse tramite un collegamento Internet. Si tenga presente che se si eseguono operazioni di gestione tramite un collegamento pubblico

(Internet), si potrebbero esporre ID utente e parola d'ordine molto significativi al rischio di sniffing. Lo ″sniffer″ può quindi utilizzare questo ID utente e questa parola d'ordine per tentare l'accesso al sistema utilizzando, ad esempio, TELNET o FTP.

Note:

1. Con TELNET, il pannello Collegamento viene considerato alla stregua di qualsiasi altro pannello. Sebbene la parola d'ordine non venga visualizzata quando la si immette, il sistema la trasmette senza alcuna crittografia o codifica.
2. Con il server *ADMIN, la parola d'ordine viene codificata non crittografata. Lo schema di codifica è uno standard industriale e di conseguenza è comunemente noto nella comunità degli hacker. Anche se la codifica non viene facilmente compresa da uno ″sniffer″ non esperto, uno sniffer di provata esperienza probabilmente ha gli strumenti idonei a tentare la decodifica della parola d'ordine.

Suggerimento sulla sicurezza

Se si intende eseguire la gestione remota su Internet, si dovrebbe utilizzare l'istanza *ADMIN con SSL, in modo che le trasmissioni siano crittografate. Non utilizzare un'applicazione non protetta, come ad esempio la versione precedente a V4R4 di TELNET (TELNET supporta SSL ad iniziare dalla V4R4). Se si sta utilizzando il server *ADMIN attraverso un'intranet di utenti *garantiti*, è possibile probabilmente utilizzarlo in modo sicuro per la gestione.

- Le direttive HTTP forniscono le basi per tutte le attività del server. La configurazione inviata fornisce la capacità di offrire una Pagina di benvenuto predefinita. Un client non può visualizzare alcun documento tranne la Pagina di benvenuto fino a quando l'amministratore del server non definisce le direttive per il server. Per definire le direttive, utilizzare un browser Web ed il server *ADMIN oppure il comando Gestione configurazione HTTP (WRKHTTPCFG). Entrambi i metodi richiedono l'autorizzazione speciale *IOSYSCFG. Quando si collega il server iSeries ad Internet, diventa ancora più importante valutare e controllare il numero di utenti nell'organizzazione che dispongono dell'autorizzazione speciale *IOSYSCFG.

Protezione delle risorse

L'IBM HTTP server for iSeries include direttive HTTP che possono fornire un controllo dettagliato delle risorse di informazioni utilizzate dal server. E' possibile utilizzare direttive per controllare da quali indirizzari il server Web fornisce URL sia per i file HTML che per i programmi CGI, per passare ad altri profili utente e per richiedere l'autenticazione per alcune risorse.

Nota: la documentazione contenuta in ″Server Web″ nell'Information Center fornisce descrizioni complete delle direttive HTTP disponibili e della loro modalità di utilizzo. Quelli che seguono sono alcuni suggerimenti e considerazioni per utilizzare questo supporto:

- Il server HTTP parte dalle basi di un'″autorizzazione esplicita.″ Il server non accetta una richiesta a meno che tale richiesta non sia esplicitamente definita nelle direttive. In altre parole, il server immediatamente rigetta qualsiasi richiesta per un URL a meno che tale URL non sia definito nelle direttive (per nome o in modo generico).
- E' possibile utilizzare le direttive di protezione per richiedere un ID utente e una parola d'ordine prima di accettare una richiesta per alcune o tutte le risorse.

– Quando un utente (client) ha bisogno di una risorsa protetta, il server richiede al browser un ID utente ed una parola d'ordine. Il browser richiede all'utente di immettere un ID utente ed una parola d'ordine e quindi invia l'informazione al server. Alcuni browser memorizzano ID utente e parola d'ordine e li inviano automaticamente con le successive richieste. Questo libera l'utente dall'impegno di immettere ripetutamente gli stessi ID utente e parola d'ordine in ogni richiesta.

  Poiché alcuni browser memorizzano l'ID utente e la parola d'ordine si hanno le stesse attività di istruzione dell'utente che si hanno quando gli utenti entrano nel sistema tramite il pannello di collegamento del server iSeries o tramite un router. Una sessione browser non presidiata rappresenta un potenziale rischio per la sicurezza.
– Si hanno tre opzioni per quanto riguarda la modalità di gestione degli ID utente e delle parole d'ordine da parte del sistema (specificate nelle direttive di protezione):
  1. E' possibile utilizzare una normale convalida di profilo utente e parola d'ordine server iSeries . Questa opzione è più comunemente utilizzata per proteggere risorse in un'intranet (rete protetta).
  2. E' possibile creare ″utenti Internet″: utenti che possono essere convalidati ma non hanno un profilo utente nel server iSeries. Gli utenti Internet sono implementati tramite un oggetto server iSeries denominato ″elenco di convalida″. Gli oggetti elenco di convalida contengono elenchi di utenti e parole d'ordine specificamente definiti per l'utilizzo con una particolare applicazione.

     Si decide il modo in cui vengono forniti ID utente e parole d'ordine Internet (ad esempio tramite un'applicazione o tramite un amministratore in risposta ad una richiesta e-mail), ed anche il modo di gestire gli utenti Internet. Utilizzare l'interfaccia basata sul browser del server HTTP per queste impostazioni.

     Per reti non protette (Internet), l'utilizzo di utenti Internet fornisce una migliore protezione generale rispetto all'utilizzo di normali profili utente e parole d'ordine. La serie univoca di ID utente e parole d'ordine crea una limitazione incorporata alle possibili azioni di tali utenti. Gli ID utente e le parole d'ordine non sono disponibili per il collegamento normale (ad esempio con TELNET o FTP). Inoltre, non si espongono ID utente e parole d'ordine normali allo sniffing.
  3. LDAP (Lightweight directory access protocol) è un protocollo di servizio indirizzario che fornisce accesso ad un indirizzario tramite un TCP (Transmission Control Protocol). Consente di memorizzare informazioni in tale servizio indirizzario e di eseguire query su di esso. LDAP ora è supportato come opzione per l'autenticazione utente.

Note:

1. Quando il browser invia l'ID utente e la parola d'ordine (per un profilo utente o un utente Internet), sono codificati, non crittografati. Lo schema di codifica è uno standard industriale e di conseguenza è comunemente noto nella comunità degli hacker. Anche se la codifica non viene facilmente compresa da uno ″sniffer″ non esperto, uno sniffer di provata esperienza probabilmente ha gli strumenti idonei a tentare la loro decodifica.
2. Il server iSeries memorizza l'oggetto di convalida in un'area di sistema protetta. E' possibile accedervi solo tramite interfacce di sistema definite (API) ed appropriata autorizzazione.

- E' possibile utilizzare DCM (Digital Certificate Manager) per creare la propria Autorità di certificazione intranet. Digital Certificate associa automaticamente un certificato al profilo utente del proprietario. Il certificato dispone delle stesse autorizzazioni e degli stessi permessi del profilo associato.

- Quando il server accetta una richiesta, subentra la normale sicurezza risorsa del server iSeries. Il profilo utente che richiede la risorsa deve disporre dell'autorizzazione alla risorsa (come ad esempio la cartella o il file fisico origine che contiene il documento HTML). Per impostazione predefinita, i lavori vengono eseguiti tramite il profilo utente QTMHHTTP. E' possibile utilizzare una direttiva per passare ad un profilo utente differente. Il sistema quindi utilizza l'autorizzazione di quel profilo utente per accedere agli oggetti. Quelle che seguono sono alcune considerazioni relative a questo supporto:
  - Lo scambio dei profili utente può essere particolarmente utile quando il server fornisce più di un sito Web logico. E' possibile associare un profilo utente differente alle direttive per ogni sito Web e quindi utilizzare la normale sicurezza risorsa del server iSeries per proteggere i documenti per ogni sito.
  - E' possibile utilizzare la capacità di scambiare profili utente in combinazione con l'oggetto convalida. Il server utilizza un ID utente ed una parola d'ordine univoci (separati dall'ID utente e la parola d'ordine normali) per valutare la richiesta iniziale. Dopo che il server ha autenticato l'utente, il sistema quindi passa ad un profilo utente differente e si avvantaggia della sicurezza risorsa. L'utente non è, quindi, consapevole del vero nome profilo utente e non può tentare di utilizzarlo in altri modi (come ad esempio FTP).
- Alcune richieste server HTTP devono eseguire un programma sul server HTTP. Ad esempio, un programma potrebbe accedere ai dati sul sistema. Prima che il programma possa essere eseguito, l'amministratore server deve mettere in corrispondenza la richiesta (URL) con uno specifico programma definito dall'utente conforme agli standard interfaccia utente CGI. Quelle che seguono sono alcune considerazioni relative ai programmi CGI:
  - E' possibile utilizzare le direttive di protezione per programmi CGI esattamente come si farebbe per documenti HTML. Quindi, è possibile richiedere un ID utente ed una parola d'ordine prima di eseguire il programma.
  - Per impostazione predefinita, i programmi CGI si eseguono tramite il profilo utente QTMHHTP1. E' possibile passare ad un profilo utente differente prima di eseguire il programma. Perciò, è possibile impostare la normale sicurezza risorsa del server iSeries per le risorse a cui accedono i programmi CGI.
  - Come responsabile della sicurezza, si dovrebbe eseguire un esame della sicurezza prima di autorizzare l'uso di qualsiasi programma CGI sul sistema. Si dovrebbe conoscere la provenienza del programma e quali funzioni il programma CGI esegue. Si dovrebbero anche monitorare le capacità dei profili utente tramite i quali si eseguono programmi CGI. Si dovrebbero anche effettuare verifiche con i programmi CGI per stabilire, ad esempio, se è possibile ottenere l'accesso ad una riga comandi. Si trattino i programmi CGI con la stessa attenzione riservata ai programmi che adottano l'autorizzazione.
  - Inoltre, assicurarsi di valutare quali oggetti critici potrebbero avere un'autorizzazione pubblica inappropriata. Un programma CGI con una progettazione inadeguata potrebbe, in rari casi, fare sì che un utente esperto, malintenzionato, tenti il roaming del sistema.
  - Utilizzare una libreria utenti specifica, come ad esempio CGILIB, per conservare tutti i programmi CGI. Utilizzare l'autorizzazione oggetto per controllare sia chi può inserire nuovi oggetti in questa libreria e chi può

eseguire programmi in questa libreria. Utilizzare le direttive per limitare il server HTTP all'esecuzione di programmi CGI che si trovano in questa libreria.

Nota: se il server fornisce più siti Web logici, potrebbe essere opportuno impostare una libreria separata per i programmi CGI per ogni sito.

Altre considerazioni sulla sicurezza

Quelle che seguono sono ulteriori considerazioni sulla sicurezza:

- HTTP fornisce accesso di sola lettura al sistema iSeries. Le richieste del server HTTP non possono aggiornare o cancellare dati sul sistema direttamente. Tuttavia, si potrebbero avere programmi CGI che aggiornano i dati. Inoltre, è possibile abilitare il programma CGI Net.Data per accedere al database server iSeries. Questo sistema utilizza uno script (che è simile ad un programma di uscita) per valutare richieste al programma Net.Data. Perciò, l'amministratore di sistema può controllare quali azioni potrà intraprendere il programma Net.Data.
- Il server HTTP fornisce una registrazione accessi che è possibile utilizzare per monitorare sia gli accessi che gli accessi tentati tramite il server.

Considerazioni sulla sicurezza per l'utilizzo di SSL con IBM HTTP Server per iSeries

IBM HTTP Server per iSeries può fornire collegamenti Web protetti al server iSeries. Un **sito web protetto** implica che le trasmissioni tra il client ed il server (in entrambe le direzioni) sono crittografate. Queste trasmissioni crittografate sono protette dall'esame di sniffer e da chi tenta di catturare o modificare le trasmissioni.

Nota: tenere a mente che un sito Web protetto si applica esclusivamente alla sicurezza delle informazioni che passano tra client e server. L'intento di ciò non è quello di ridurre la vulnerabilità del proprio server agli attacchi degli hacker. Tuttavia, si limitano certamente le informazioni che un possibile hacker può facilmente ottenere tramite sniffing.

Gli argomenti relativi all'SSL e a Webserving (HTTP) nell'information center forniscono informazioni complete per l'installazione, la configurazione e la gestione del processo di crittografia. Questi argomenti forniscono sia una panoramica delle funzioni del server che alcune considerazioni per l'utilizzo del server.

Internet Connection Server fornisce supporto HTTP e HTTPS quando è installato uno dei seguenti programmi su licenza:

- 5722–NC1
- 5722–NCE

Quando queste opzioni sono installate, al prodotto ci si riferisce come Internet Connection Secure Server.

IBM HTTP Server for iSeries (5722–DG1) fornisce sia il supporto http che https. E' necessario installare uno dei seguenti prodotti crittografici per abilitare SSL:

- 5722–AC2
- 5722–AC3

La sicurezza che si basa sulla crittografia ha diversi requisiti:

- Sia l'inviante che il ricevente (server e client) devono ″conoscere″ il meccanismo della crittografia ed essere in grado di crittografare e decrittografare. Il server

HTTP richiede un client abilitato SSL. (I più diffusi browser Web sono abilitati SSL.) I programmi su licenza di crittografia iSeries supportano diversi metodi di crittografia standard industriali. Quando un cliente tenta di stabilire una sessione protetta, il server ed il client negoziano per trovare il metodo di crittografia più sicuro supportato da entrambi.

- Un utente non autorizzato non deve essere in grado di decrittografare la trasmissione. Perciò, i metodi di crittografia richiedono che entrambe le parti abbiano una **chiave privata** per crittografare/decrittografare nota solo a loro. Se si desidera avere un sito Web *esterno* protetto, si dovrebbe utilizzare un'autorità di certificazione (AC) indipendente per creare ed emettere certificati digitali per utenti e server. L'autorità di certificazione è nota come parte garantita.

La crittografia protegge la segretezza delle informazioni trasmesse. Tuttavia, per informazioni critiche, come ad esempio informazioni finanziarie, si desidera l'integrità e l'autenticità oltre alla segretezza. In altre parole, il client e (facoltativamente) il server devono riconoscere la parte all'altra estremità (tramite un riferimento indipendente) e devono essere certi che la trasmissione non sia stata modificata. La firma digitale fornita da un'autorità di certificazione (AC) fornisce queste garanzie di autenticità ed integrità. Il protocollo SSL fornisce l'autenticazione verificando la firma digitale del certificato del server (e facoltativamente del certificato del client).

Crittografare e decrittografare richiede tempo di elaborazione e influenzerà le prestazioni delle proprie trasmissioni. Perciò, i server iSeries forniscono la capacità per eseguire contemporaneamente sia programmi per l'utilizzo protetto che non protetto del server. E' possibile utilizzare il server HTTP non protetto per fornire documenti che non richiedono sicurezza, come ad esempio il catalogo dei prodotti. Questi documenti avranno un URL che inizia con `http://`. E' possibile utilizzare un server HTTP protetto per informazioni critiche come ad esempio il modulo nel quale il cliente immette le informazioni sulla carta di credito. Il programma può fornire documenti il cui URL inizia con `http://` o con `https://`.

Pro memoria

E' buona consuetudine in Internet informare i client quando le trasmissioni sono protette e non protette, particolarmente quando il sito Web utilizza un server protetto solo per alcuni documenti.

Tenere a mente che la crittografia richiede sia un client protetto che un server protetto. I browser protetti (client HTTP) sono divenuti alquanto comuni.

Considerazioni sulla sicurezza per LDAP

Le funzioni di sicurezza LDAP (Lightweight Directory Access Protocol) include la codifica parola d'ordine CRAM-MD5, gli ACL e SSL (Secure Sockets Layer). In V5R1, i collegamenti Kerberos e il supporto di Controllo sicurezza sono stati aggiunti per migliorare la sicurezza LDAP.

Per ulteriori informazioni su tali argomenti, fare riferimento ad iSeries Information Center—>Rete–>TCP/IP–>Servizi indirizzario (LDAP). Consultare "Requisiti necessari e informazioni correlate" a pagina xii per informazioni sull'accesso all'iSeries Information Center.

Considerazioni sulla sicurezza per LPD

LPD (line printer daemon) fornisce la capacità di distribuire l'emissione di stampa al sistema. Il sistema non esegue alcuna procedura di collegamento per LPD.

Prevenzione dell'accesso LPD

Se *non* si desidera che alcuno utilizzi LPD per accedere al sistema, si dovrebbe impedire l'esecuzione del server LPD. Effettuare le seguenti operazioni.

__ Passo 1. Per impedire l'avvio automatico di lavori server LPD quando si avvia TCP/IP, immettere quanto segue:

```
CHGLPDA AUTOSTART(*NO)
```

Note:

1. AUTOSTART(*YES) è il valore predefinito.
2. "Controllo dei server TCP/IP con avvio automatico" a pagina 130 fornisce ulteriori informazioni sul controllo di quali server TCP/IP si avviano automaticamente.

__ Passo 2. Per impedire che qualcuno associ un'applicazione utente, come ad esempio un'applicazione socket, alla porta che il sistema normalmente utilizza per LPD, effettuare quanto segue:

__ Passo a. Immettere `GO CFGTCP` per visualizzare il menu Configurazione TCP/IP.

__ Passo b. Selezionare l'opzione 4 (Gestione limitazioni porta TCP/IP).

__ Passo c. Sul pannello Gestione limitazioni porta TCP/IP, specificare l'opzione 1 (Aggiunta).

__ Passo d. Per il valore inferiore dell'intervallo porta, specificare `515`.

__ Passo e. Per il valore superiore dell'intervallo porta, specificare `*ONLY`.

Note:

1. La limitazione porta diventa effettiva al successivo avvio di TCP/IP. Se TCP/IP è attivo quando si impostano le limitazioni porta, sarebbe opportuno arrestarlo e riavviarlo.
2. RFC1700 fornisce informazioni sulle assegnazioni comuni del numero porta.

__ Passo f. Per il protocollo, specificare `*TCP`.

__ Passo g. Per il campo del profilo utente, specificare un nome profilo utente protetto sul sistema. (Un profilo utente protetto è un profilo utente che non possiede programmi che adottano l'autorizzazione e che non dispone di una parola d'ordine nota ad altri utenti). Limitando la porta a un utente specifico, si escludono automaticamente tutti gli altri utenti.

__ Passo h. Ripetere i passi da 2c a 2g per il protocollo *UDP.

Controllo accesso LPD

Se si desidera consentire ai client LPD di accedere al sistema, tenere presenti le seguenti questioni di sicurezza:

- Per impedire che un utente riempia il sistema di oggetti non desiderati, accertarsi di aver impostato limiti di soglia adeguati per i propri ASP (auxiliary storage pool). E' possibile visualizzare ed impostare le soglie per gli ASP utilizzando SST (system service tools) o DST (dedicated service tools). Il manuale *Copia di riserva e ripristino* fornisce ulteriori informazioni sulle soglie ASP.
- E' possibile utilizzare l'autorizzazione alle code di emissione per limitare il numero di chi può inviare file di spool al sistema. Utenti LPD senza un ID utente utilizzano il profilo utente QTMPLPD. E' possibile assegnare a questo profilo utente accesso solo a poche code di emissione.

Considerazioni sulla sicurezza per SNMP

Il server iSeries può agire come agent SNMP (simple network management protocol) in una rete. SNMP fornisce un mezzo per la gestione di gateway, router e host in un ambiente di rete. Un agent SNMP raccoglie informazioni sul sistema ed esegue funzioni richieste dai gestori di rete SNMP remoti.

Prevenzione accesso SNMP

Se *non* si desidera che alcuno utilizzi SNMP per accedere al sistema, si dovrebbe impedire l'esecuzione del server SNMP. Effettuare le seguenti operazioni.

__ Passo 1. Per impedire l'avvio automatico di lavori server SNMP quando si avvia TCP/IP, immettere quanto segue:

```
CHGSNMPA AUTOSTART(*NO)
```

Note:

1. AUTOSTART(*YES) è il valore predefinito.
2. "Controllo dei server TCP/IP con avvio automatico" a pagina 130 fornisce ulteriori informazioni sul controllo di quali server TCP/IP si avviano automaticamente.

__ Passo 2. Per impedire che qualcuno associ un'applicazione utente, come ad esempio un'applicazione socket, alla porta che il sistema normalmente utilizza per SNMP, effettuare quanto segue:

__ Passo a. Immettere `GO CFGTCP` per visualizzare il menu Configurazione TCP/IP.

__ Passo b. Selezionare l'opzione 4 (Gestione limitazioni porta TCP/IP).

__ Passo c. Sul pannello Gestione limitazioni porta TCP/IP, specificare l'opzione 1 (Aggiunta).

__ Passo d. Per il valore inferiore dell'intervallo porta, specificare `161`.

__ Passo e. Per il valore superiore dell'intervallo porta, specificare `*ONLY`.

Note:

1. La limitazione porta diventa effettiva al successivo avvio di TCP/IP. Se TCP/IP è attivo quando si impostano le limitazioni porta, sarebbe opportuno arrestarlo e riavviarlo.
2. RFC1700 fornisce informazioni sulle assegnazioni comuni del numero porta.

__ Passo f. Per il protocollo, specificare `*TCP`.

__ Passo g. Per il campo del profilo utente, specificare un nome profilo utente protetto sul sistema. (Un profilo utente protetto è un profilo utente che non possiede programmi che adottano l'autorizzazione e che non dispone di una parola d'ordine nota ad altri utenti). Limitando la porta a un utente specifico, si escludono automaticamente tutti gli altri utenti.

__ Passo h. Ripetere i passi da 2c a 2g per il protocollo *UDP.

Controllo accesso SNMP

Se si desidera consentire ai gestori SNMP di accedere al sistema, tenere presenti le seguenti questioni di sicurezza:

- Chi può accedere alla rete tramite SNMP può raccogliere informazioni sulla rete. Informazioni che sono state nascoste utilizzando alias ed un server nome dominio diventano disponibili per l'eventuale intruso tramite SNMP. Inoltre, un intruso potrebbe utilizzare SNMP per modificare la configurazione di rete e interrompere le comunicazioni.
- SNMP si basa su un nome comunità per l'accesso. Come concetto, il nome comunità è simile ad una parola d'ordine. Il nome comunità non è codificato. Perciò, è passibile di sniffing. Utilizzare il comando Aggiunta comunità per SNMP (ADDCOMSNMP) per impostare il parametro indirizzo internet gestore (INTNETADR) su uno o più indirizzi IP specifici invece di *ANY. E' possibile impostare anche il parametro OBJACC dei comandi ADDCOMSNMP o CHGCOMSNMP su *NONE per impedire che i gestori in una comunità accedano a qualsiasi oggetto MIB. Si intende che questo viene fatto solo temporaneamente per negare l'accesso ai gestori in una comunità senza eliminare la comunità.

Considerazioni sulla sicurezza per il server INETD

A differenza della maggioranza dei server TCP/IP, il server INETD non fornisce un singolo servizio ai client. Invece, fornisce una varietà di servizi diversificati che gli amministratori possono personalizzare. Per tale ragione, il server INETD viene talvolta denominato ″il super server″. Il server INETD ha i seguenti servizi incorporati:

- ora
- ora del giorno
- reinvio
- eliminazione
- modificato

Questi servizi sono supportati sia per TCP che per UDP. Per UDP, i servizi di reinvio, dell'ora, dell'ora del giorno e modificato ricevono pacchetti UDP, quindi rinviano i pacchetti al mittente. Il server di reinvio rimanda i pacchetti che riceve, i server dell'ora e dell'ora del giorno generano l'ora in uno specifico formato e la inviano di nuovo ed il server modificato genera un pacchetto di caratteri ASCII stampabili e lo reinvia.

La natura di questi servizi UDP rende un sistema vulnerabile ad un attacco tipo negazione del servizio . Ad esempio, presumiamo che l'utente abbia due server iSeries: SYSTEMA e SYSTEMB. Un programmatore malintenzionato potrebbe creare l'intestazione IP e l'intestazione UDP con un indirizzo origine di SYSTEMA ed un numero porta UDP del server dell'ora. Egli può quindi inviare quel pacchetto al server dell'ora su SYSTEMB, che invierà l'ora a SYSTEMA, che rimanderà la

risposta a SYSTEMB e così via, generando un loop continuo e consumando risorse CPU su entrambi i sistemi ed anche l'ampiezza banda di rete.

Perciò, si dovrebbe prendere in considerazione il rischio di un tale attacco sul proprio sistema iSeries ed eseguire questi servizi solo su una rete protetta. Il server INETD viene fornito senza l'avvio automatico quando si avvia TCP/IP. E' possibile configurare o meno l'avvio dei servizi quando si avvia INETD. Per impostazione predefinita, i server dell'ora ed i server dell'ora del giorno TCP e UDP sono entrambi avviati quando si avvia il server INETD.

Esistono due file di configurazione per il server INETD:

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

Questi file determinano quali programmi avviare quando si avvia il server INETD. Stabiliscono anche in base a quale profilo utente si eseguono questi programmi quando INETD li avvia.

Nota: il file di configurazione in proddata non dovrebbe mai essere modificato. Viene sostituito ogni volta che si ricarica il sistema. Le modifiche alla configurazione del cliente dovrebbero essere inserite solo nel file, nell'albero indirizzario dati utente, poiché questo file **non** viene aggiornato durante gli aggiornamenti del release.

Se un programmatore malintenzionato ottiene l'accesso a questi file, potrebbe configurarli in modo da avviare qualsiasi programma all'avvio di INETD. Quindi è di estrema importanza proteggere questi file. Per impostazione predefinita richiedono l'autorizzazione QSECOFR per apportare modifiche. Non si dovrebbe ridurre l'autorizzazione richiesta per l'accesso ad essi.

Nota: non modificare il file di configurazione nell'indirizzario ProdData. Tale file viene sostituito ogni volta che si ricarica il sistema. Le modifiche alla configurazione del cliente dovrebbero essere inserite solo nel file nell'albero indirizzario Dati utente, poiché tale file non viene aggiornato durante gli aggiornamenti del release.

Considerazioni sulla sicurezza per limitare il roaming TCP/IP

Se il sistema è collegato ad una rete, potrebbe sembrare opportuno limitare la capacità degli utenti di navigare attraverso la rete con applicazioni TCP/IP. Un modo per farlo è limitare l'accesso ai seguenti comandi TCP/IP del client:

Nota: questi comandi potrebbero essere in diverse librerie nel sistema. Come minimo, si trovano sia nella libreria QSYS che nella libreria QTCP. Accertarsi di localizzare e proteggere tutte le ricorrenze.

- STRTCPFTP
- FTP
- STRTCPTELN
- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD (client REXEC)

Le possibili destinazioni degli utenti sono determinate dai seguenti fattori:

- Voci nella tabella host TCP/IP.

- Voce *DFTROUTE nella tabella di instradamento TCP/IP. Questo consente agli utenti di immettere l'indirizzo IP del sistema hop-successivo quando la relativa destinazione è una rete sconosciuta. Un utente può raggiungere o contattare una rete remota utilizzando l'instradamento predefinito.
- Configurazione server dei nomi remoto. Questo supporto consente ad un altro server nella rete di localizzare i nomi host per gli utenti.
- Tabella sistema remoto.

E' necessario controllare chi può aggiungere voci a queste tabelle e modificare la configurazione. E' anche necessario comprendere le implicazioni delle proprie voci di tabella e della propria configurazione.

Tenere presente che un utente esperto con accesso ad un compilatore ILE C può creare un programma socket che può collegarsi ad una porta TCP o UDP. E' possibile rendere il tutto più difficile limitando l'accesso ai seguenti file interfaccia socket nella libreria QSYSINC:
- SYS
- NETINET
- H
- ARPA
- socket ed SSL

Per programmi di servizio, è possibile limitare l'uso di applicazioni socket ed SSL già compilate limitando l'uso di questi programmi di servizio:
- QSOSRV1
- QSOSRV2
- QSOSKIT(SSL)
- QSOSSLSR(SSL)

I programmi di servizio vengono inviati con l'autorizzazione pubblica *USE, ma l'autorizzazione può essere modificata in *EXCLUDE (o un altro valore in base alle necessità).

Capitolo 14. Accesso sicuro a una stazione di lavoro

Molti utenti del sistema dispongono di PC sulle loro scrivanie come stazioni di lavoro. Utilizzano programmi da eseguire sul PC e utilizzano un PC per collegarsi al server iSeries.

La maggior parte dei metodi per collegare un PC ai server iSeries fornisce ulteriori funzioni rispetto all'emulazione della stazione di lavoro. Il PC può apparire come un pannello per iSeries e fornire all'utente sessioni di collegamento interattive. Inoltre è possibile che il PC appaia ai server iSeries come un altro computer e fornisca funzioni come il trasferimento file e la chiamata procedura remota.

Come responsabile della sicurezza del server iSeries, è necessario essere consapevole di quanto segue:

- Funzioni disponibili per utenti PC collegati al sistema
- Risorse del server iSeries a cui gli utenti PC possono accedere.

E' possibile che si desideri impedire le funzioni PC avanzate (come il trasferimento file e la chiamata procedura remota) se lo schema di sicurezza server iSeries non è ancora preparato a tali funzioni. Probabilmente, l'obiettivo a lungo raggio è consentire le funzioni PC avanzate mentre ancora si proteggono le informazioni sul sistema. I seguenti argomenti discutono alcune delle questioni sulla sicurezza associate all'accesso al PC.

Prevenzione dei virus di una stazione di lavoro

Queste informazioni suggeriscono delle strategie che i responsabili della sicurezza possono mettere in atto contro i virus PC.

Accesso sicuro ai dati di una stazione di lavoro

Alcuni software client PC utilizzano delle cartelle condivise per memorizzare le informazioni sul server. Per accedere ai file di database iSeries, l'utente del PC ha una serie limitata, ben definita di interfacce. Con la funzione di trasferimento file che fa parte della maggioranza dei software client/server, l'utente del PC può copiare i file tra il server e il PC. Con la funzione di accesso al database, come un file DDM, un SQL remoto o un'unità di controllo ODBC, l'utente del PC può accedere ai dati sul server.

In questo ambiente, è possibile creare dei programmi per individuare e valutare le richieste di un utente PC per accedere alle risorse del server. Quando le richieste utilizzano un file DDM, si specifica il programma di uscita nell'attributo di rete DDMACC (distributed data management access). Per alcuni metodi di trasferimento file PC, si specifica il programma di uscita nell'attributo di rete (PCSACC) accesso di richiesta client. O, è possibile specificare PCSACC (*REGFAC) per utilizzare la funzione di registrazione. Quando le richieste utilizzano altre funzioni server per accedere ai dati, è possibile utilizzare il comando WRKREGINF per registrare i programmi di uscita per tali funzioni server.

© Copyright IBM Corp. 1996, 2004

I programmi di uscita, tuttavia, possono essere di difficile progettazione e sono raramente immuni dagli errori. Essi non sono una sostituzione per l'autorizzazione all'oggetto, che è pensata per proteggere gli oggetti da un accesso non autorizzato da qualsiasi origine.

Alcuni software client, come ad esempio IBM iSeries Access per Windows, utilizzano l'IFS (integrated file system) per memorizzare e accedere ai dati sui server iSeries. Con l'IFS (integrated file system), l'intero server diventa più facilmente disponibile per utenti del PC. L'autorizzazione all'oggetto diventa ancor più essenziale. Attraverso l'IFS (integrated file system), un utente con sufficiente autorizzazione può visualizzare una libreria server come se fosse un indirizzario PC. I semplici comandi di copia e spostamento possono spostare i dati all'istante da una libreria server iSeries su un indirizzario PC o viceversa. Il sistema apporta automaticamente le modifiche appropriate al formato dei dati.

Note:

1. E' possibile utilizzare un elenco di autorizzazioni per controllare l'utilizzo di oggetti nel file system QSYS.LIB. Consultare "Limitazione dell'accesso al file system QSYS.LIB" a pagina 107 per ulteriori informazioni.
2. Il Capitolo 11, "Utilizzo di IFS (Integrated File System) per proteggere i file", a pagina 101 fornisce ulteriori informazioni sulle questioni di sicurezza con l'IFS (integrated file system).

La forza dell'IFS (integrated file system) risiede nella sua semplicità per utenti e sviluppatori. Con una singola interfaccia, l'utente può gestire oggetti in più ambienti. L'utente del PC non ha bisogno di un software speciale o di API per accedere agli oggetti. Al contrario, può utilizzare i comandi PC che gli sono familiari o "puntare e fare clic" per gestire gli oggetti direttamente.

Per tutti i sistemi con PC collegati, ma in modo particolare per sistemi con un software client che utilizza l'IFS (integrated file system), un buono schema di autorizzazione all'oggetto è di fondamentale importanza. Dal momento che la sicurezza è integrata nel prodotto OS/400, qualsiasi richiesta per accedere ai dati deve passare per il processo di verifica autorizzazione. Tale verifica si applica alle richieste da qualsiasi origine e all'accesso dati che utilizza qualsiasi metodo.

Autorizzazione all'oggetto con accesso a una stazione di lavoro

Quando si imposta l'autorizzazione per gli oggetti, è necessario valutare quali possibilità fornisce tale autorizzazione per l'utente del PC. Ad esempio, quando un utente ha un'autorizzazione *USE a un file, l'utente può visualizzare o stampare i dati nel file. L'utente non può modificare le informazioni nel file o cancellare il file. Per l'utente del PC, la visualizzazione è uguale alla "lettura", che fornisce sufficiente autorizzazione per consentire all'utente di copiare un file sul PC. E' possibile che non si voglia questo.

Per alcuni file critici, è possibile che sia necessario impostare l'autorizzazione pubblica su *EXCLUDE per impedire lo scaricamento. E' quindi possibile fornire un altro metodo per "visualizzare" il file sul server, come ad esempio utilizzando un menu e dei programmi che adottano l'autorizzazione.

Un'altra opzione per impedire lo scaricamento è utilizzare un programma di uscita che viene eseguito ogni qualvolta un utente del PC avvia una funzione server (diversa da un collegamento interattivo). E' possibile specificare un programma di uscita nell'attributo di rete PCSACC utilizzando il comando Modifica attributi di

rete (CHGNETA). Oppure, è possibile registrare i programmi di uscita utilizzando il comando Gestione informazioni di registrazione (WRKREGINF). Il metodo utilizzato dipende dal modo in cui i PC accedono ai dati sul sistema e quale programma client utilizzano i PC. Il programma di uscita (QIBM_QPWFS_FILE_SERV) si applica all'accesso iSeries Access e Net Server all'IFS. Ciò non impedisce l'accesso da un PC con altri meccanismi, come ad esempio FTP o ODBC.

Un software PC fornisce normalmente anche la funzione di caricamento, quindi un utente può copiare i dati dal PC a un file di database del server. Se non si è impostato correttamente lo schema di autorizzazione, è possibile che un utente del PC sostituisca tutti i dati in un file con i dati provenienti da un PC. E' necessario assegnare l'autorizzazione *CHANGE con cautela. Esaminare l'Appendice D nel manuale *Riferimenti alla sicurezza iSeries* per comprendere quale autorizzazione è richiesta per le operazioni file.

L'iSeries Information Center fornisce ulteriori informazioni sull'autorizzazione per le funzioni PC e sull'utilizzo dei programmi di uscita. Consultare "Requisiti necessari e informazioni correlate" a pagina xii per dettagli.

Gestione applicazione

Gestione applicazione è un componente installabile in modo facoltativo di iSeries Navigator, la GUI (graphical user interface) per il server iSeries. Gestione applicazione consente ai responsabili di sistema di controllare le funzioni o le applicazioni disponibili per utenti e gruppi su un server specifico. Ciò include il controllo delle funzioni disponibili per utenti che accedono al server tramite i client. A questo punto è importante notare che, se si accede al server da un client Windows, è l'utente del server iSeries e non l'utente Windows che stabilisce quali funzioni sono disponibili per la gestione.

Per una documentazione completa su Gestione applicazione di iSeries Navigator, consultare iSeries Information Center–>Collegamento a iSeries—>Cosa collegare con—>iSeries Navigator (../html/as400/v5r2/ic2924/info/rzaj3/rzaj3overview.htm).

Gestione normativa

Le normative sono uno strumento che gli amministratori possono utilizzare al momento della configurazione del software sui PC client. Le normative possono limitare le relative funzioni e applicazioni a cui un utente ha accesso sul PC. Le normative possono inoltre suggerire o imporre configurazioni che devono essere utilizzate da alcuni utenti o PC.

Nota: le normative non forniscono il controllo sulle risorse del server. Le normative non sostituiscono la sicurezza del server. Esse possono essere utilizzate per influenzare la modalità di accesso al server di iSeries Access da un particolare PC tramite un particolare utente. Tuttavia, non modificano la modalità di accesso alle risorse server tramite altri meccanismi.

Le normative sono memorizzate su un server dei file. Ogni qualvolta l'utente si collega a una stazione di lavoro Windows, le normative che si applicano a tale utente Windows vengono scaricate dal server dei file. Le normative vengono applicate al registro prima di qualsiasi operazione dell'utente sulla stazione di lavoro.

Normative Microsoft rispetto a gestione applicazione

iSeries Access Express supporta due differenti strategie per implementare il controllo di gestione all'interno della rete: normative di sistema Microsoft e Gestione applicazione di iSeries Navigator. Considerare quanto segue al momento di decidere la strategia che si adatta maggiormente alle proprie esigenze.

Normative di sistema Microsoft

Le normative sono vincolate al PC, non dipendono da specifici release OS/400. Esse possono essere applicate sia ai PC che agli utenti Windows. Ciò indica che gli utenti fanno riferimento al profilo utente Windows, non al profilo utente del server. E' possibile utilizzare le normative sia per "configurare" che per limitare. Esse offrono maggiore granularità rispetto a Gestione applicazione e possono offrire una maggiore gamma di funzioni. Ciò dipende dal fatto che non è necessario un collegamento al server per stabilire se l'utente può utilizzare o meno la funzione. L'implementazione di normative è più complicata dell'implementazione di Gestione applicazione poiché è necessario utilizzare l'editor della normativa di sistema Microsoft ed è inoltre necessario configurare i PC singolarmente per scaricare le normative.

Gestione applicazione di **Gestione applicazione di iSeries Navigator**

Gestione applicazione associa i dati con il profilo utente, invece che con il profilo Windows associato alle normative di sistema Microsoft. Mentre i server iSeries che eseguono V4R3 o versioni successive del prodotto OS/400 sono necessari per utilizzare Gestione applicazione, alcune funzioni sono disponibili soltanto in V4R4 o successive. Gestione applicazione utilizza la GUI (graphical user interface) di iSeries Navigator per le sue operazioni, che è molto più semplice da utilizzare rispetto all'editor della normativa. Le informazioni di Gestione applicazione si applica all'utente indipendentemente da quale PC effettua il collegamento. E' possibile limitare particolari funzioni all'interno di iSeries Navigator. Gestione applicazione è preferibile se tutte le funzioni che si desidera limitare sono abilitate a tale strumento e se la versione di OS/400 utilizzata lo supporta.

Utilizzo di SSL con iSeries Access per Windows

Per informazioni sull'utilizzo di iSeries Access Express con SSL, consultare gli argomenti iSeries Information Center *Gestione SSL (Secure Sockets Layer), Protezione di iSeries Access Express e iSeries Navigator, iSeries Developer Kit per Java e iSeries Java Toolbox* sotto l'argomento principale Java. E' inoltre possibile consultare tali informazioni sul CD fornito con il sistema.

Sicurezza iSeries Navigator

iSeries Navigator fornisce un'interfaccia al server di semplice utilizzo per utenti che dispongono di iSeries Access. Con ogni nuovo release del prodotto OS/400, diventano disponibili più funzioni server tramite iSeries Navigator. Un'interfaccia di semplice utilizzo fornisce numerosi vantaggi, inclusi i costi ridotti di assistenza tecnica e un'immagine migliorata per il sistema. Comporta anche problematiche per la sicurezza.

Come responsabile della sicurezza, non è più possibile affidarsi all'ignoranza degli utenti per proteggere le risorse. iSeries Navigator rende molte funzioni semplici e visibili per gli utenti. E' necessario accertarsi di avere progettato e implementato le normative di sicurezza per i profili utente e per la sicurezza dell'oggetto in modo che corrispondano alle proprie esigenze di sicurezza.

V4R4 e le versioni successive di IBM e(logo)server iSeries Access per Windows forniscono i seguenti metodi per controllare le funzioni che gli utenti possono eseguire tramite iSeries Navigator:

- Installazione selettiva
- Gestione applicazione
- Supporto della normativa di sistema Windows NT

iSeries Navigator è composto da più componenti che è possibile installare separatamente. Ciò consente di installare soltanto le funzioni richieste. Gestione applicazione consente a un amministratore di controllare le funzioni a cui un utente o un gruppo può accedere tramite iSeries Navigator. Gestione applicazione organizza le applicazioni nelle seguenti categorie:

iSeries Navigator
Include iSeries Navigator e i moduli di collegamento.

Applicazioni client
Include tutte le applicazioni client, incluso iSeries Access, che fornisce le funzioni sui client gestiti tramite Gestione applicazione.

Applicazioni host
Include tutte le applicazioni che si trovano esclusivamente sul server e fornisce funzioni gestite tramite Gestione applicazioni.

E' possibile utilizzare l'installazione selettiva, la gestione applicazione e le normative per limitare le funzioni di iSeries Navigator a cui un utente può accedere. Nessuna di queste, tuttavia, dovrebbe essere utilizzata per la sicurezza delle risorse.

A partire da V4R4, IBM e(logo)server iSeries Access per Windows supporta anche l'utilizzo dell'Editor della normativa di sistema Windows NT per controllare quali funzioni è possibile eseguire da un particolare client PC, indipendentemente da quale utente utilizza tale PC.

Consultare l'iSeries Information Center per ulteriori informazioni sull'installazione selettiva, sulla Gestione applicazione e Gestione normativa. La sezione "Limitazione dell'accesso a una funzione del programma" a pagina 5 del presente manuale contiene inoltre ulteriori informazioni sulla gestione applicazione.

Prevenzione accesso ODBC

ODBC (Open database connectivity) è uno strumento che le applicazioni PC possono utilizzare per accedere a dati iSeries come se fossero dati PC. Il programmatore ODBC può rendere l'ubicazione fisica dei dati evidente per l'utente dell'applicazione PC. Per ulteriori informazioni riguardo le considerazioni sulla sicurezza ODBC, andare alle informazioni "iSeries Access for Windows ODBC security" (/rzaii/rzaiiodbc09.HTM), reperibili nell'iSeries Information Center.

Considerazioni sulla sicurezza per le parole d'ordine della sessione di una stazione di lavoro

Normalmente, quando un utente PC avvia il software di collegamento, come ad esempio iSeries Access, l'utente immette una volta l'ID utente e la parola d'ordine per il server. La parola d'ordine viene codificata e memorizzata nella memoria del PC. Ogni qualvolta l'utente stabilisce una nuova sessione sullo stesso server, il PC invia l'ID utente e la parola d'ordine automaticamente.

Alcuni software client/server forniscono l'opzione di saltare il pannello di collegamento per le sessioni interattive. Il software invierà l'ID utente e la parola d'ordine codificata quando l'utente avvia una sessione interattiva (emulazione 5250). Per supportare tale opzione, è necessario impostare il valore di sistema QRMTSIGN sul server su *VERIFY.

Quando si decide di consentire che venga saltato il pannello di collegamento, è necessario considerare delle compensazioni per la sicurezza.

Rischio della sicurezza: per l'emulazione 5250 o per qualsiasi altro tipo di sessione interattiva, il pannello di collegamento è uguale a qualsiasi altro pannello. Sebbene la parola d'ordine non venga visualizzata sul pannello al momento dell'immissione, la parola d'ordine viene inviata sul collegamento in formato decodificato esattamente come qualsiasi altro campo dati. Per alcuni tipi di collegamenti, questo potrebbe dare l'opportunità ad un potenziale intruso di monitorare il collegamento e individuare un ID utente e una parola d'ordine. Il monitoraggio di un collegamento utilizzando apparecchiature elettroniche viene spesso definito come **sniffing**. A partire da V4R4, è possibile utilizzare SSL (secure sockets layer) per codificare la comunicazione tra iSeries Access e il server iSeries. Ciò protegge i dati, incluse le parole d'ordine, dallo sniffing.

Quando si sceglie l'opzione per saltare il pannello di collegamento, il PC codifica la parola d'ordine prima che venga inviata. La codifica evita la possibilità che dei potenziali intrusi si impossessino della parola d'ordine tramite lo sniffing. Tuttavia, è necessario accertarsi che gli utenti di PC pratichino una sicurezza operativa. Un PC non presidiato con una sessione attiva sul sistema iSeries consente a chiunque di avviare un'altra sessione senza conoscere ID utente e parola d'ordine. Sarebbe opportuno impostare un blocco sui PC quando il sistema è inattivo per un periodo prolungato e configurare il PC in modo che, per riprendere la sessione, sia necessario inserire una parola d'ordine.

Anche se non si sceglie di saltare il pannello di collegamento, un PC non presidiato con una sessione attiva rappresenta un rischio per la sicurezza. Utilizzando un software PC, chiunque può avviare una sessione server e accedere ai dati, ancora una volta senza conoscere ID utente e parola d'ordine. Il rischio con l'emulazione 5250 è in qualche modo maggiore poiché richiede meno conoscenze per avviare una sessione e iniziare ad accedere ai dati.

E' inoltre necessario informare gli utenti sull'effetto provocato dallo scollegamento della sessione iSeries Access. Molti utenti presuppongono (in modo logico ma non corretto) che l'opzione di scollegamento arresti completamente il collegamento al server. In effetti, quando un utente seleziona l'opzione di scollegamento, il server rende la sessione dell'utente (licenza) disponibile per un altro utente. Tuttavia, il collegamento del client al server è ancora attivo. Un altro utente potrebbe accedere al PC incustodito e alle risorse del server senza immettere mai ID utente e parola d'ordine.

E' possibile suggerire due opzioni agli utenti che hanno necessità di scollegare le sessioni:

- Accertarsi che i PC abbiano una funzione di blocco che richieda una parola d'ordine. Ciò rende il PC non presidiato non disponibile a chi non conosca la parola d'ordine.
- Per scollegare completamente una sessione, scollegare Windows o riavviare (eseguire il reboot) il PC. In questo modo si termina la sessione su iSeries.

E' inoltre necessario informare gli utenti su un potenziale rischio per la sicurezza quando utilizzano iSeries Access per Windows. Quando un utente specifica un'UNC (universal naming convention) per identificare una risorsa iSeries, il client Win95 o NT crea un collegamento di rete per collegarsi al server. Dal momento che l'utente specifica un'UNC, non visualizza questo come unità di rete correlata. Spesso, l'utente non è neanche consapevole del collegamento di rete. Tuttavia, tale collegamento di rete rappresenta un rischio per la sicurezza su un PC non presidiato poiché il server viene visualizzato nell'albero indirizzario sul PC. Se la sessione di un utente ha un profilo utente potente, le risorse del server potrebbero essere a rischio su un PC non presidiato. Come avviene nel precedente esempio, il rimedio è di accertarsi sia che gli utenti comprendano il rischio sia che utilizzano la funzione di blocco del PC.

Protezione del server dalle procedure e dai comandi remoti

Un utente PC esperto con un software quale iSeries Access può eseguire i comandi sul server senza passare per il pannello di collegamento. Di seguito vengono riportati numerosi metodi disponibili affinché gli utenti del PC possano eseguire i comandi del server. Il software client/server stabilisce i metodi disponibili per gli utenti del PC.

- Un utente può aprire un file DDM e utilizzare la funzione del comando remoto per eseguire un comando.
- Alcuni software, come ad esempio i client ottimizzati di iSeries Access, forniscono la funzione del comando remoto tramite le API DPC (Distributed Program Call), senza l'utilizzo di DDM.
- Alcuni software, come ad esempio SQL remoto e ODBC, forniscono una funzione del comando remoto senza DDM o DPC.

Per un software client/server che utilizza DDM per il supporto del comando remoto, è possibile utilizzare l'attributo di rete DDMACC per impedire completamente i comandi remoti . Per un software client/server che utilizza un altro supporto server, è possibile registrare i programmi di uscita per il server. Se si desidera consentire i comandi remoti, è necessario assicurarsi che lo schema di autorizzazione oggetto protegga i dati in modo adeguato. La funzione di un comando remoto equivale a fornire a un utente una riga comandi. Inoltre, quando iSeries riceve un comando remoto tramite DDM, il sistema non applica l'impostazione Possibilità limitate (LMTCPB) dei profili utente.

Protezione delle stazioni di lavoro dalle procedure e dai comandi remoti

IBM iSeries Access per Windows fornisce la funzione di ricezione comandi remoti sul PC. E' possibile utilizzare il comando Esecuzione comando remoto (RUNRMTCMD) sul server per eseguire una procedura su un PC collegato. La funzione RUNRMTCMD è uno strumento valido per i responsabili di sistema e per il personale dell'help-desk. Tuttavia, dà anche la possibilità di danneggiare i dati del PC, deliberatamente o accidentalmente.

I PC non hanno le stesse funzioni di autorizzazione oggetto dei server iSeries. La migliore protezione contro i problemi con il comando RUNRMTCMD è limitare attentamente gli utenti di sistema che hanno accesso al comando. IBM iSeries Access per Windows fornisce la funzione di registrazione degli utenti che possono eseguire comandi remoti su un PC specifico. Quando il collegamento avviene tramite TCP/IP, è possibile utilizzare il pannello di controllo delle proprietà sul client per controllare l'accesso ai comandi remoti. E' possibile autorizzare gli utenti

tramite ID utente o tramite nome sistema remoto. Quando il collegamento avviene tramite SNA, qualche software client fornisce la funzione di impostazione della sicurezza relativa alla conversazione. Con un altro software client, si sceglie semplicemente se impostare o meno la funzione del comando in entrata.

Per ciascuna combinazione di software client e tipo di collegamento (come ad esempio TCP/IP o SNA), è necessario esaminare il potenziale per i comandi in entrata nei PC collegati. Consultare la documentazione client ricercando un "comando in entrata" o "RUNRMTCMD". Prepararsi ad avvisare gli utenti del PC e gli amministratori di rete sulla modalità corretta (sicura) di configurare i client in modo da consentire o impedire tale funzione.

Server gateway

E' possibile che il sistema faccia parte di una rete con un server gateway o intermedio tra il sistema iSeries e i PC. Ad esempio, è possibile che il sistema iSeries sia collegato a una LAN con un server PC che ha dei PC collegati al server. Le questioni sulla sicurezza in questa situazione dipendono dalle funzioni del software in esecuzione sul server gateway. La Figura 13 visualizza un esempio di una configurazione server gateway.

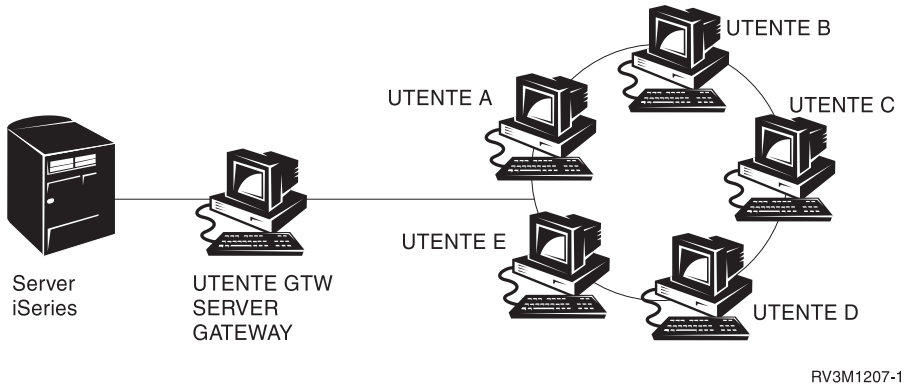

Figura 13. Sistema iSeries con un server gateway

Con alcuni software, il sistema iSeries non sarà a conoscenza degli utenti (come ad esempio UTENTE A o UTENTE C) che si trovano ad un'estremità rispetto al server gateway. Il server si collegherà al sistema come singolo utente (UTENTE GTW). Esso utilizzerà l'ID utente UTENTE GTW per gestire tutte le richieste che provengono dagli utenti da quell'estremità. Una richiesta da UTENTE A sarà considerata dal server alla stregua di una richiesta dall'utente UTENTE GTW.

In questo caso, è necessario affidarsi al server gateway per l'applicazione della sicurezza. E' necessario comprendere e gestire le funzioni di sicurezza del server gateway. Dalla prospettiva di un server iSeries, ciascun utente ha la stessa autorizzazione dell'ID utente che il server gateway utilizza per avviare la sessione. E' possibile pensare tale situazione come all'esecuzione di un programma che adotta l'autorizzazione e fornisce una riga comandi.

Con un altro software, il server gateway passa le richieste da singoli utenti ai server iSeries. Il server iSeries riconosce che UTENTE A sta richiedendo l'accesso a un oggetto particolare. Il gateway è praticamente trasparente per il sistema.

Se il sistema si trova su una rete che dispone di server gateway, è necessario valutare quale livello di autorizzazione fornire agli ID utente utilizzati dai server gateway. E' inoltre necessario comprendere quanto segue:

- I meccanismi di sicurezza che i server gateway applicano.
- In che modo gli utenti all'estremità opposta verranno considerati nel sistema iSeries.

Comunicazioni LAN wireless

Alcuni client potrebbero utilizzare la LAN wireless iSeries per comunicare con il sistema senza l'uso di cavi. La LAN wireless iSeries utilizza la tecnologia delle comunicazioni in frequenza radio. Come responsabile della sicurezza, bisognerebbe tenere presenti le seguenti caratteristiche di sicurezza dei prodotti LAN wireless iSeries:

- Questi prodotti LAN wireless utilizzano tecnologia ad ampio spettro. Questa stessa tecnologia è stata utilizzata dal governo in passato per proteggere le trasmissioni radio. A qualcuno che tenta il monitoraggio elettronico delle trasmissioni di dati, le trasmissioni si presentano come un rumore piuttosto che un'effettiva trasmissione.
- Il collegamento wireless ha tre parametri di configurazione rilevanti per la sicurezza:
  - Velocità dei dati (due possibili velocità di dati)
  - Frequenza (cinque possibili frequenze)
  - Identificativo di sistema (8 milioni di possibili identificativi)

  Questi elementi di configurazione si combinano per fornire 80 milioni di possibili configurazioni, che rendono infinitesimale la probabilità che un hacker indovini la configurazione corretta.
- Proprio come altri metodi di comunicazione, la sicurezza delle comunicazioni wireless è influenzata dalla sicurezza dell'unità del client. Le informazioni sull'ID di sistema e su altri parametri di configurazione si trovano in un file sull'unità client e dovrebbero essere protette.
- Se si perde un'unità wireless o viene rubata, le normali misure di sicurezza del server, come ad esempio le parole d'ordine di collegamento e la sicurezza dell'oggetto, forniscono protezione quando un utente non autorizzato tenta di utilizzare l'unità persa o rubata per accedere al sistema.
- Se un'unità client wireless viene persa o rubata, si dovrebbe considerare la modifica delle informazioni sull'ID di sistema per tutti gli utenti, i punti di accesso ed i sistemi. Equivale a cambiare le serrature delle porte se ci viene rubata una serie di chiavi.
- Si potrebbe voler eseguire la partizione del server in gruppi di client con ID sistema univoci. In questo modo si limita l'impatto della perdita o del furto dell'unità. Questo metodo funziona solo se è possibile confinare un gruppo di utenti in una parte specifica dell'installazione.
- A differenza della tecnologia LAN wired, la tecnologia LAN wireless è proprietaria. Perciò, non sono pubblicamente disponibili sniffer elettronici per questi prodotti LAN wireless. Uno sniffer è un dispositivo elettronico che esegue il monitoraggio non autorizzato di una trasmissione.

Capitolo 15. Programmi di uscita sicurezza

Alcune funzioni del server iSeries forniscono un'uscita in modo che il sistema possa eseguire un programma creato dall'utente per eseguire una convalida e un controllo aggiuntivi. Ad esempio, è possibile impostare il sistema in modo che esegua un programma di uscita ogni qualvolta qualcuno tenti di aprire un file DDM (distributed data management) sul sistema. E' possibile utilizzare la funzione di registrazione per specificare i programmi di uscita che vengono eseguiti in alcune condizioni.

Numerose pubblicazioni iSeries contengono esempi di programmi di uscita che eseguono funzioni di sicurezza. La Tabella 24 fornisce un elenco di tali programmi di uscita e origini per i programmi di esempio.

Tabella 24. Origini di programmi di uscita di esempio

Tipo di programma di uscita	**Scopo**	**Contesto in cui ricercare gli esempi**
Convalida della parola d'ordine	Il valore di sistema QPWDVLDPGM può specificare un nome programma o indicare che i programmi di convalida registrati per il punto di uscita QIBM_QSY_VLD_PASSWRD vengano utilizzati per controllare una nuova parola d'ordine per requisiti aggiuntivi che non vengono gestiti dai valori di sistema QPWDxxx. E' necessario monitorare attentamente l'utilizzo di tale programma poiché riceve delle parole d'ordine non codificate. Tale programma **non dovrebbe** memorizzare le parole d'ordine in un file o passarle a un altro programma.	• *An Implementation Guide for iSeries Security and Auditing, GG24–4200* • *Riferimenti alla sicurezza iSeries*, SC13-3195-07
Accesso PC Support/400 o Client Access[1]	E' possibile specificare questo nome programma nel parametro (PCSACC) accesso di richiesta client degli attributi di rete per controllare le seguenti funzioni: • Funzione stampante virtuale • Funzione trasferimento file • Funzione cartelle condivise di tipo 2 • Funzione messaggio Client access • Code dati • Funzione SQL remoto	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
Accesso DDM (Distributed Data Management)	E' possibile specificare questo nome programma nel parametro (DDMACC) accesso di richiesta DDM degli attributi di rete per controllare le seguenti funzioni: • Funzione cartelle condivise di tipo 0 e 1 • Funzione inoltro comando remoto	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
Collegamento remoto	E' possibile specificare un programma nel valore di sistema QRMTSIGN per controllare quali utenti possono collegarsi automaticamente da quali ubicazioni (pass-through.)	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*

© Copyright IBM Corp. 1996, 2004

Tabella 24. Origini di programmi di uscita di esempio (Continua)

Tipo di programma di uscita	Scopo	Contesto in cui ricercare gli esempi
ODBC (Open Database Connectivity) con iSeries Access[1]	Controllare le seguenti funzioni di ODBC: • Se ODBC è sempre consentito. • Quali funzioni sono consentite per i file di database iSeries. • Quali istruzioni SQL sono consentite. • Quali informazioni è possibile richiamare relative agli oggetti del server database. • Quali funzioni del catalogo SQL sono consentite.	Nessuno disponibile.
Programma di gestione interruzione QSYSMSG	E' possibile creare un programma per monitorare la coda messaggi QSYSMSG e intraprendere l'azione appropriata (come la notifica al responsabile della sicurezza) a seconda del tipo di messaggio.	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
TCP/IP	Diversi server TCP/IP (come FTP, TFTP, TELNET e REXEC) forniscono dei punti di uscita. E' possibile aggiungere dei programmi di uscita per gestire il collegamento e per convalidare le richieste utente, come le richieste per richiamare o inserire un file specifico. E' inoltre possibile utilizzare tali uscite per fornire FTP anonimo sul sistema.	"TCP/IP User Exits nel manuale *iSeries System API Reference*"
Modifiche profilo utente	E' possibile creare dei programmi di uscita per i seguenti comandi del profilo utente: CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• *Riferimenti alla sicurezza iSeries*, SC13-3195-07 • "TCP/IP User Exits nel manuale *iSeries System API Reference*"

Note:

1. Per informazioni aggiuntive su tale argomento, consultare l'iSeries Information Center. Consultare "Requisiti necessari e informazioni correlate" a pagina xii per ulteriori dettagli.

Capitolo 16. Considerazioni sulla sicurezza per browser Internet

Molti utenti di PC nell'azienda dispongono di browser sulle stazioni di lavoro. Possono collegarsi a Internet. Possono anche collegarsi al server. Di seguito vengono riportate considerazioni sulla sicurezza sia per i PC che per il server.

Rischio: danni alla stazione di lavoro

Una pagina web visitata dall'utente può avere un ″programma″ associato come un'applet Java, un controllo Active-X o un altro tipo di modulo aggiuntivo. Sebbene sia raro, questo tipo di ″programma″, quando viene eseguito su un PC, ha il potenziale di danneggiare le informazioni sul PC. Come responsabile della sicurezza, considerare quanto segue per proteggere i PC nella propria azienda:

- Conoscere le opzioni di sicurezza dei differenti browser di cui dispongono gli utenti. Ad esempio, con alcuni browser, è possibile controllare l'accesso delle applet Java al di fuori del browser (l'ambiente operativo limitato di Java è denominato *sandbox*). Ciò può impedire il danneggiamento dei dati PC da parte delle applet.

  Nota: il concetto di sandbox e le relative limitazioni di sicurezza associate non esistono per Active-X e per altri moduli aggiuntivi.
- Consigliare gli utenti relativamente alle impostazioni del browser. Probabilmente non si ha a disposizione né tempo né risorse per accertarsi che gli utenti seguano i consigli del responsabile della sicurezza. Quindi, è necessario che questi li istruisca sui potenziali rischi di impostazioni improprie.
- Considerare la standardizzazione dei browser web che forniscono le opzioni di sicurezza necessarie.
- Fare in modo che gli utenti avvertano il responsabile della sicurezza di eventuali funzionalità o sintomi sospetti che potrebbero essere associati a particolari siti web.

Rischio: accesso agli indirizzari iSeries tramite unità collegate

Supponiamo che un PC sia collegato al server con una sessione IBM iSeries Access per Windows. La sessione ha impostato delle unità collegate per collegarsi ad iSeries IFS (integrated file system). Ad esempio, l'unità **G** del PC potrebbe essere correlata all'IFS (integrated file system) del server SYSTEM1 nella rete.

Supponiamo che lo stesso utente PC disponga di un browser e possa accedere a Internet. L'utente richiede una pagina Web che esegue un ″programma virus″ come ad esempio un'applet Java o un controllo Active-X. Plausibilmente, il programma potrebbe tentare di cancellare tutto il contenuto dell'unità G del PC.

L'utente ha a disposizione diverse protezioni per evitare danni alle unità collegate:

- La protezione più importante è la sicurezza delle risorse sul server. L'applet Java o il controllo Active-X concepisce il server come l'utente che ha stabilito la sessione PC. E' necessario gestire attentamente ciò che gli utenti PC sono autorizzati ad eseguire sul server.

© Copyright IBM Corp. 1996, 2004

- Consigliare agli utenti PC di impostare i browser per impedire tentativi di accesso alle unità collegate. Ciò funziona per le applet Java ma non per i controlli Active-X, che non dispongono del concetto di sandbox.
- Informare gli utenti sui pericoli dei collegamenti al server e a Internet nella stessa sessione. Inoltre, accertarsi che gli utenti del PC (con client Windows 95, ad esempio) comprendano che le unità rimangono correlate anche quando sembra che la sessione di iSeries Access sia terminata.

Rischio: applet firmate garantite

E' possibile che gli utenti abbiano seguito i consigli del responsabile della sicurezza e abbiano impostato i browser per impedire alle applet la scrittura su qualsiasi unità PC. Tuttavia, è possibile che gli utenti del PC siano consapevoli del fatto che un'*applet firmata* può sostituire l'impostazione per il browser.

Un'applet firmata ha una firma digitale associata per stabilirne l'autenticità. Quando un utente accede a una pagina web che presenta un'applet firmata, viene visualizzato un messaggio. Il messaggio indica la firma dell'applet (l'utente che l'ha firmata e il momento in cui ciò è avvenuto). Quando l'utente accetta l'applet, concede ad essa una sostituzione delle impostazioni di sicurezza per il browser. L'applet firmata può scrivere sulle unità locali del PC, anche se l'impostazione predefinita per il browser lo impedisce. L'applet firmata può anche scrivere sulle unità collegate del server poiché compaiono sul PC come unità locali.

Per le applet Java che derivano dal server, è possibile che sia necessario utilizzare le applet firmate. Tuttavia, sarebbe opportuno avvertire gli utenti in generale di non accettare applet firmate da origini ignote.

Capitolo 17. Informazioni correlate

Manuali

- *APPC Programming*, SC41-5443-00 descrive il supporto APPC (advanced program-to-program communications) per il sistema iSeries. Questo manuale guida l'utente nello sviluppo dei programmi delle applicazioni che utilizzano APPC e nella definizione degli ambienti di comunicazioni per le comunicazioni APPC. Esso include considerazioni sul programma dell'applicazione, comandi e requisiti della configurazione, gestione problemi per APPC e considerazioni generali sulla rete. Consultare il CD-ROM dell'iSeries Information Center.
- *AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet* Redbook, SG24-4929 discute i problemi relativi alla severità e i rischi associati al collegamento di iSeries con Internet. Fornisce esempi, consigli, suggerimenti e tecniche per le applicazioni TCP/IP.
- *Copia di riserva e ripristino*, SC13-3047-07 fornisce informazioni sulla pianificazione di una strategia di copia di riserva e ripristino, sul salvataggio delle informazioni dal sistema e sul ripristino del sistema. Consultare iSeries Information Center. E' inoltre possibile individuare ulteriori informazioni su tali argomenti nell'iSeries Information Center. Consultare "Requisiti necessari e informazioni correlate" a pagina xii per ulteriori dettagli.
- *CL Programming*, SC41-5721-06, fornisce descrizioni dettagliate per la codifica di DDS (data description specification) per file che è possibile descrivere esternamente. Tali file sono file fisici, logici, di visualizzazione, stampa e ICF (intersystem communication function). Consultare iSeries Information Center.
- L'argomento CL nell'Information Center (consultare "Requisiti necessari e informazioni correlate" a pagina xii per ulteriori dettagli) fornisce una descrizione di tutti i comandi iSeries CL (control language) e dei relativi comandi OS/400. I comandi OS/400 vengono utilizzati per richiedere funzioni del programma su licenza Operating System/400 (5722-SS1). Tutti i comandi CL non OS/400--quelli associati agli altri programmi su licenza, incluse tutte le varie lingue e i programmi di utilità--vengono descritti in altri manuali che supportano tali programmi su licenza.
- *Implementing iSeries Security, 3rd Edition* di Wayne Madden e Carol Woodbury. Loveland, Colorado: 29th Street Press, una divisione di Duke Communications International, 1998. Fornisce supporto e suggerimenti pratici per la pianificazione, l'impostazione e la gestione della sicurezza iSeries.

  Numero ordine ISBN:

  1-882419-78-2
- Per ulteriori informazioni sul server HTTP, consultare l'URL seguente:

  `http://www.ibm.com/eserver/iseries/software/http/docs/doc.htm`
- *Riferimenti alla sicurezza iSeries*, SC13-3195-07, fornisce informazioni complete sui valori di sistema della sicurezza, sui profili utente, sulla sicurezza delle risorse e sul controllo sicurezza. Il presente manuale non descrive la riservatezza per programmi su licenza specifici, lingue e programmi di utilità. Consultare iSeries Information Center.
- L'argomento "Operazioni di base del sistema" nell'Information Center fornisce informazioni su alcuni dei concetti chiave e delle attività richieste per le operazioni di base di iSeries. Consultare "Requisiti necessari e informazioni correlate" a pagina xii per ulteriori dettagli.

© Copyright IBM Corp. 1996, 2004

- L'Information Center descrive come utilizzare e configurare TCP/IP e le numerose applicazioni TCP/IP, come ad esempio FTP, SMTP e TELNET. Consultare "Requisiti necessari e informazioni correlate" a pagina xii per ulteriori dettagli.
- *TCP/IP File Server Support for OS/400 Installation and User's Guide*, SC41-0125, fornisce informazioni introduttive, istruzioni di installazione e procedure di configurazione per l'offerta del programma su licenza Supporto server dei file. Spiega le funzioni disponibili con il prodotto e include esempi e suggerimenti per l'utilizzo di tale prodotto con altri sistemi.
- *Trusted Computer Systems Evaluation Criteria* DoD 5200.28.STD, descrive i criteri per i livelli di sicurezza per i sistemi di computer. TCSEC è una pubblicazione del governo degli Stati Uniti. Per ottenere delle copie, rivolgersi a:

  Office of Standards and Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 USA
  All'attenzione del: Capo degli standard di sicurezza
- L'Information Center contiene numerosi argomenti relativi a System Management e Work Management su iSeries. Alcuni di tali argomenti includono raccolta di dati delle prestazioni, gestione dei valori di sistema e gestione della memoria. Per dettagli sull'accesso dell'Information Center, consultare "Requisiti necessari e informazioni correlate" a pagina xii. Work Management, SC41-5306-03, fornisce informazioni su come creare e modificare un ambiente di gestione lavoro. Consultare iSeries Information Center.

In aggiunta a tali argomenti dell'Information Center e ai Manuali supplementari, è possibile utilizzare le seguenti risorse per assistenza:

- **IBM SecureWay**
  IBM SecureWay fornisce un marchio comune per l'esteso portafoglio IBM di offerte sulla sicurezza; hardware, software, consulenza e servizi per aiutare i clienti a proteggere le risorse IT. Sia nel caso si rivolgano a soddisfare esigenze del singolo o a creare una soluzione globale per l'azienda, le offerte IBM SecureWay forniscono l'esperienza necessaria per pianificare, progettare, implementare ed eseguire soluzioni sicure per le aziende. Per ulteriori informazioni sulle offerte IBM SecureWay, visitare la home page di IBM SecureWay:

  `http://www.ibm.com/secureway`
- **Offerte di servizi**
  L'installazione di un nuovo hardware o software può migliorare notevolmente l'efficienza e le operazioni dell'azienda. Ma pone anche la minaccia di interruzione delle attività aziendali e di guasti e può mettere alla prova le preziose risorse interne. IBM Global Services fornisce servizi correlati alla sicurezza iSeries. Il seguente sito web consente di ricercare degli elenchi completi di servizi per il proprio iSeries:

  `http://www.as.ibm.com/asus`

Informazioni particolari

Queste informazioni sono state progettate per prodotti e servizi offerti negli Stati Uniti.

L'IBM potrebbe non fornire in altri paesi prodotti, servizi o funzioni discussi in questo documento. Contattare il rappresentante IBM per informazioni sui prodotti e servizi correntemente disponibili nella propria area. Qualsiasi riferimento ad un prodotto, programma o servizio IBM non implica che sia possibile utilizzare soltanto tali prodotti, programmi o servizi IBM. In sostituzione a quanto fornito dall'IBM, è possibile utilizzare qualsiasi prodotto, programma o servizio funzionalmente equivalente che non violi alcun diritto di proprietà intellettuale dell'IBM. Tuttavia la valutazione e la verifica dell'uso di prodotti o servizi non IBM ricadono esclusivamente sotto la responsabilità dell'utente.

L'IBM può avere brevetti o domande di brevetto in corso relativi a quanto trattato nel presente documento. La fornitura di questa pubblicazione non implica la concessione di alcuna licenza su tali brevetti. Chi desiderasse ricevere informazioni relative a licenze può rivolgersi per iscritto a:

IBM Director of Licensing
IBM Corporation
Schoenaicher Str. 220
D 7030 Boeblingen
Deutschland.

Le disposizioni contenute nel seguente paragrafo non si applicano al Regno Unito o ad altri paesi nei quali tali disposizioni non siano congruenti con le leggi locali: L'IBM FORNISCE QUESTA PUBBLICAZIONE "COSI' COM'E'" SENZA ALCUNA GARANZIA, ESPLICITA O IMPLICITA, IVI INCLUSE EVENTUALI GARANZIE DI COMMERCIABILITA' ED IDONEITA' AD UNO SCOPO PARTICOLARE. Alcuni stati non consentono la recessione da garanzie implicite o esplicite in alcune transazioni, quindi questa specifica potrebbe non essere applicabile in determinati casi.

Queste informazioni potrebbero contenere imprecisioni tecniche o errori tipografici. Si effettuano periodicamente modifiche alle informazioni qui accluse; queste modifiche saranno inserite in nuove edizioni della pubblicazione. L'IBM può apportare perfezionamenti e/o modifiche nel(i) prodotto(i) e/o nel(i) programma(i) descritto(i) in questa pubblicazione in qualsiasi momento senza preavviso.

Qualsiasi riferimento a siti Web non IBM, contenuto in queste informazioni, viene fornito solo per comodità e non implica in alcun modo l'approvazione di tali siti. Le informazioni reperibili nei siti Web non sono parte integrante delle informazioni relative a questo prodotto IBM, pertanto il loro utilizzo ricade sotto la responsabilità dell'utente.

L'IBM può utilizzare o distribuire le informazioni fornite in qualsiasi modo ritenga appropriato senza obblighi verso l'utente.

Sarebbe opportuno che coloro che hanno la licenza per questo programma e desiderano avere informazioni su di esso allo scopo di consentire: (i) lo scambio di informazioni tra programmi creati in maniera indipendente e non (compreso questo), (ii) l'uso reciproco di tali informazioni, contattassero:

© Copyright IBM Corp. 1996, 2004

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Tali informazioni possono essere disponibili, soggette a termini e condizioni appropriate, compreso in alcuni casi il pagamento di una tariffa.

Il programma su licenza descritto in questa pubblicazione e tutto il relativo materiale disponibile viene fornito dall'IBM nei termini dell'IBM Customer Agreement, IBM International Program License Agreement o qualsiasi altro accordo equivalente tra le parti.

Qualsiasi dato sulle prestazioni contenuto in questa pubblicazione è stato stabilito in un ambiente controllato. Quindi i risultati ottenuti in altri ambienti operativi potrebbero variare in modo significativo. E' possibile che alcune misurazioni siano state effettuate su sistemi a livello di sviluppo e non esiste alcuna garanzia che tali misurazioni siano le stesse su sistemi generalmente disponibili. Inoltre, alcune misurazioni possono essere state valutate per estrapolazione. I risultati effettivi possono variare. Sarebbe opportuno che gli utenti di questa pubblicazione verificassero i dati applicabili per il relativo ambiente specifico.

Le informazioni riguardanti prodotti non IBM sono ottenute dai fornitori di tali prodotti, dai loro annunci pubblicati o da altre fonti pubblicamente reperibili. L'IBM non ha testato tali prodotti e non può confermare l'inadeguatezza delle prestazioni, della compatibilità o di altre richieste relative a prodotti non IBM. Domande inerenti alle prestazioni di prodotti non IBM dovrebbero essere indirizzate ai fornitori di tali prodotti.

Tutte le specifiche relative alle direttive o intenti futuri dell'IBM sono soggetti a modifiche o a revoche senza notifica e rappresentano soltanto scopi ed obiettivi.

Queste informazioni sono solo per scopi di pianificazione. Le presenti informazioni sono soggette a modifiche prima che i prodotti descritti siano resi disponibili.

Queste informazioni contengono esempi di dati e report utilizzati in quotidiane operazioni aziendali. Per illustrarle nel modo più completo possibile, gli esempi includono i nomi di individui, società, marchi e prodotti. Tutti questi nomi sono fittizi e qualsiasi somiglianza con nomi ed indirizzi utilizzati da gruppi aziendali realmente esistenti è puramente casuale.

LICENZA DI COPYRIGHT:

Queste informazioni contengono programmi di applicazione di esempio nella lingua di origine, che illustrano le tecniche di programmazione su varie piattaforme operative. E' possibile copiare, modificare e distribuire questi programmi di esempio in qualsiasi formato senza pagare all'IBM, allo scopo di sviluppare, utilizzare, commercializzare o distribuire i programmi dell'applicazione conformi all'interfaccia di programmazione dell'applicazione per la piattaforma operativa per cui i programmi di esempio vengono scritti. Questi esempi non sono stati interamente testati in tutte le condizioni. IBM, perciò, non fornisce nessun tipo di garanzia o affidabilità implicita, rispetto alla funzionalità o alle funzioni di questi programmi. E' possibile copiare, modificare e distribuire questi programmi di esempio in qualsiasi formato senza pagare all'IBM allo scopo di sviluppare,

utilizzare, commercializzare o distribuire i programmi dell'applicazione conformi alle interfacce di programmazione dell'applicazione IBM.

Se si sta utilizzando la versione in formato elettronico di questo manuale, le fotografie e le illustrazioni a colori potrebbero non essere visualizzate.

Marchi

I seguenti termini sono marchi dell'IBM Corporation negli Stati Uniti e/o negli altri Paesi:

Advanced Peer-to-Peer Networking
APPN
AS/400
DB2
DRDA
e (logo)
IBM
iSeriesNet.Data
Operating System/400
OS/400
PowerPC
SecureWay
System/36
System/38
400

ActionMedia, LANDesk, MMX, Pentium e ProShare sono marchi o marchi registrati di Intel Corporation negli Stati Uniti, in altri paesi o in entrambi.

Microsoft, Windows, Windows NT e il logo Windows sono marchi registrati di Microsoft Corporation negli Stati Uniti, in altri paesi o in entrambi.

Java e i logo basati su Java sono marchi registrati di Sun Microsystems, Inc. negli Stati Uniti, in altri paesi o in entrambi.

UNIX è un marchio registrato di The Open Group negli Stati Uniti e in altri paesi.

Altri nomi di aziende, prodotti o servizi riportati in questa pubblicazione sono marchi di altre società.

Indice analitico

Caratteri speciali

(SNMP), simple network management protocol 154

A

abilitazione
  profilo utente
    automaticamente 30
accesso
  controllo 47
Accesso ad altri sistemi da parte di utenti del collegamento in entrata, Prevenzione 134
Accesso agli indirizzari iSeries 400 tramite unità collegate 171
Accesso al file system QSYS.LIB, limitazione 107
advanced program-to-program communications (APPC)
  Vedere APPC (advanced program-to-program communication)
Advisor, Sicurezza 13
ambiente utente
  monitoraggio 66
analisi
  autorizzazione oggetto 55
  errore del programma 56
  profili utente 53
  profilo utente
    tramite autorizzazioni speciali 34
    tramite classe utente 34
API, Creazione di un file di flusso con open() o creat() 110
API, Creazione di un indirizzario 110
API QHFRGFS
  programma di uscita 83
API QSYSCHID (Modifica uid) 112
API QTNADDCR
  programma di uscita 83
APPC (advanced program-to-program communications)
  assegnazione profilo utente 117
  avvio di un lavoro di pass-through 118
  comando remoto 121
    limitazione con voce PGMEVOKE 121
  descrizione linea 125
    campo AUTOANS (risposta automatica) 125
    campo AUTODIAL (composizione automatica) 125
    parametri rilevanti per la sicurezza 125
  descrizione unità
    limitazione con autorizzazione all'oggetto 114
APPC (advanced program-to-program communications) *(Continua)*
  descrizione unità *(Continua)*
    parametri rilevanti per la sicurezza 121
    parametro APPN (Supporto-APPN) 123
    parametro avvio programma SNUF 123
    parametro LOCPWD (parola d'ordine di ubicazione) 114
    parametro PREESTSSN (sessione pre-stabilita) 123
    parametro SECURELOC (ubicazione protetta) 114, 117
    parametro SNGSSN (sessione singola) 123
    parametro ubicazione protetta (SECURELOC) 122
    protezione con APPN 115
    ruolo nella sicurezza 114
  descrizione unità di controllo
    parametri rilevanti per la sicurezza 124
    parametro AUTOCRTDEV (creazione automatica unità) 124
    parametro CPSSN (sessioni control-point) 124
    parametro tempificatore scollegamento 124
  distribuzione della responsabilità di sicurezza 117
  elementi di base 114
  identificazione di un utente 115
  limitazione di sessioni 114
  sessione 114
  suggerimenti sulla sicurezza 113
  terminologia 113
  valori di sicurezza pianificati
    con il parametro SECURELOC (ubicazione protetta) 117
    descrizione 115
    esempi dell'applicazione 116
  valutazione configurazione 121, 125
Applet firmate, garanzia 172
assegnazione
  profilo utente per lavoro APPC 117
Atti illeciti, prevenzione e rilevazione 89
attivazione
  profilo utente 24, 30
attributi sicurezza
  stampa 8
attributo di rete
  accesso di richiesta client (PCSACC)
    limitazione dell'accesso dati PC 159
    origine per programma di uscita sicurezza 169
    utilizzo di un programma di uscita 83
attributo di rete *(Continua)*
  accesso di richiesta DDM (DDMACC)
    limitazione dei comandi remoti 165
    limitazione dell'accesso dati PC 159
    origine per programma di uscita sicurezza 169
    utilizzo di un programma di uscita 83, 120
  comando per impostazione 39
  JOBACN (azione del lavoro di rete) 120
  stampa rilevante per la sicurezza 8, 34
attributo di rete (JOBACN) relativo all'azione del lavoro di rete 120
attributo di rete (PCSACC) accesso di richiesta client
  limitazione dell'accesso dati PC 159
  origine per programma di uscita sicurezza 169
  utilizzo di un programma di uscita 83
attributo di rete accesso di richiesta client (PCSACC)
  limitazione dell'accesso dati PC 159
  origine per programma di uscita sicurezza 169
  utilizzo di un programma di uscita 83
attributo di rete accesso di richiesta DDM (DDMACC)
  limitazione dei comandi remoti 165
  limitazione dell'accesso dati PC 159
  origine per programma di uscita sicurezza 169
  utilizzo di un programma di uscita 83, 120
attributo di rete JOBACN (azione del lavoro di rete) 120
autorizzazione
  accesso ai comandi di ripristino 87
  accesso ai comandi di salvataggio 87
  accesso dati da parte di utenti PC 160
  ad un livello di sicurezza 10 o 20 47
  adottata 79
    limitazione 80
    modifica 56
    monitoraggio 79
  ambiente di transizione 49
  autorizzazione speciale *SAVSYS (salvataggio del sistema) 86
    controllo 86
  code di emissione 64
  code lavori 64
  comandi strumento di sicurezza 29
  gestione 59
  integrazione controllo accesso menu 49

© Copyright IBM Corp. 1996, 2004

autorizzazione *(Continua)*
introduzione 5, 49
lingue nazionali 52
monitoraggio 59, 63
nuovi oggetti 60
panoramica 47
pubblica 59
quando si applica 47
sicurezza libreria 51
speciale 64
autorizzazione, oggetto
Vedere autorizzazione oggetto
autorizzazione adottata
limitazione 80
monitoraggio dell'utilizzo 79
stampa elenco di oggetti 34
autorizzazione oggetto
accesso ai comandi di ripristino 87
accesso ai comandi di salvataggio 87
accesso dati da parte di utenti PC 160
ad un livello di sicurezza 10 o 20 47
adottata 79
limitazione 80
monitoraggio 79
ambiente di transizione 49
analisi 55
autorizzazione speciale *SAVSYS (salvataggio del sistema) 86
controllo 86
code di emissione 64
code lavori 64
comandi strumento di sicurezza 29
gestione 59
integrazione controllo accesso menu 49
introduzione 5, 49
lingue nazionali 52
monitoraggio 59, 63
nuovi oggetti 60
panoramica 47
pubblica 59
quando si applica 47
sicurezza libreria 51
speciale 64
visualizzazione 55
autorizzazione privata
monitoraggio 63
autorizzazione pubblica
monitoraggio 59
revoca 39
revoca tramite il comando RVKPUBAUT 42
stampa 36
autorizzazione pubblica all'indirizzario principale 105
autorizzazione speciale
*SAVSYS (salvataggio del sistema)
controllo 86
analisi assegnazione 34
elenco utenti 54
mancata corrispondenza con la classe utente 65
monitoraggio 64
autorizzazione speciale (*IOSYSCFG) alla configurazione del sistema
richiesta per i comandi di configurazione APPC 115
autorizzazione speciale *IOSYSCFG (configurazione del sistema)
richiesta per i comandi di configurazione APPC 115
autorizzazione speciale *SAVSYS (salvataggio del sistema)
controllo 86
avvio
lavoro di pass-through 118
azioni, controllo 56
azioni di controllo 56

B

bibliografia 173
BOOTP (Bootstrap Protocol)
limitazione porta 138
suggerimenti sulla sicurezza 137
Bootstrap Protocol (BOOTP)
limitazione porta 138
suggerimenti sulla sicurezza 137
Browser, considerazioni sulla sicurezza 171

C

campo AUTOANS (risposta automatica) 125
campo AUTODIAL (composizione automatica) 125
campo composizione automatica (AUTODIAL) 125
campo risposta automatica (AUTOANS) 125
capacità di ripristino
monitoraggio 78
capacità di salvataggio
monitoraggio 78
caricamento
richiesta autorizzazione 161
chiamata non qualificata 87
classe utente
analisi assegnazione 34
mancata corrispondenza con l'autorizzazione speciale 65
coda di emissione
monitoraggio accesso 64
stampa di parametri rilevanti per la sicurezza 37
stampa per profili utente 66
coda lavori
monitoraggio accesso 64
stampa di parametri rilevanti per la sicurezza 37
coda messaggi messaggio di sistema (QSYSMSG)
origine per programma di uscita sicurezza 169
utilizzo suggerito 97
coda messaggi QSYSMSG (messaggio di sistema)
origine per programma di uscita sicurezza 169
utilizzo suggerito 97
codifica
parola d'ordine
sessioni PC 163
codifica a senso unico 27
Collegamenti, Controllo SLIP in entrata 132
collegamento
come evitare 164
controllo 15
impostazione dei valori sistema 23
monitoraggio tentativi 27
collegamento sicuro 114
comando
revoca autorizzazione pubblica 39
comando, CL
ADDPFRCOL (Aggiunta raccolta prestazioni)
programma di uscita 83
ANZDFTPWD (Analisi parole d'ordine predefinite)
descrizione 30
utilizzo suggerito 27
ANZPRFACT (Analisi attività profilo)
creazione di utenti esenti 30
descrizione 30
utilizzo suggerito 25
Avvio TCP/IP (STRTCP)
limitazione 127
CHGACTPRFL (Modifica elenco profili attivi)
descrizione 30
utilizzo suggerito 26
CHGACTSCDE (Modifica voce Scd di attivazione)
descrizione 30
utilizzo suggerito 24
CHGEXPSCDE (Modifica scadenza voce di pianificazione)
descrizione 30
CHGEXPSCDE (Modifica voce SCD di scadenza)
utilizzo suggerito 26
CHGMSGD (Modifica descrizione messaggio)
programma di uscita 83
CHGPFRCOL (Modifica raccolta prestazioni)
programma di uscita 83
CHGSECAUD (Modifica controllo riservatezza)
descrizione 32
utilizzo suggerito 97
CHGSYSLIBL (Modifica lista librerie sistema)
limitazione dell'accesso 87
CHKOBJITG (Controllo integrità oggetto)
utilizzo suggerito 78
comando PRTPUBAUT (Stampa oggetti autorizzati pubblicamente)
descrizione 34
utilizzo suggerito 115

comando, CL *(Continua)*
comando Visualizzazione libreria (DSPLIB) 55
Configurazione riservatezza sistema (CFGSYSSEC)
descrizione 39
utilizzo suggerito 15
Controllo integrità oggetto (CHKOBJITG)
descrizione 34, 55
Creazione caricamento prodotto (CRTPRDLOD)
programma di uscita 83
DSPACTPRFL (Visualizzazione elenco profili attivi)
descrizione 30
DSPACTSCD (Visualizzazione pianificazione attivazione)
descrizione 30
DSPAUTUSR (Visualizzazione utenti autorizzati)
modifica 53
DSPEXPSCD (Visualizzazione pianificazione di scadenza)
descrizione 30
utilizzo suggerito 26
DSPSECAUD (Visualizzazione controllo riservatezza)
descrizione 32
DSPUSRPRF (Visualizzazione profilo utente)
utilizzo del file di emissione 54
ENDPFRMON (Fine monitoraggio prestazioni)
programma di uscita 83
Esecuzione comando remoto (RUNRMTCMD)
limitazione 165
Gestione descrizione sottosistema (WRKSBSD) 91
Gestione informazioni registrazione (WRKREGINF)
programma di uscita 85
Inoltro comando remoto (SBMRMTCMD)
limitazione 120
Invio voce di giornale (SNDJRNE) 57
Modifica copie riserva (CHGBCKUP)
programma di uscita 83
pianificazione attivazione 30
PRTADPOBJ (Stampa oggetti di adozione)
descrizione 34
PRTCMNSEC (Stampa riservatezza di comunicazione)
esempio 121, 125
PRTPVTAUT (Stampa autorizzazioni private)
descrizione 36
elenco di autorizzazioni 34, 60
utilizzo suggerito 115
PRTSYSSECA (Stampa attributi riservatezza di sistema)
descrizione 34
emissione esempio 8
utilizzo suggerito 15
comando, CL *(Continua)*
PRTUSROBJ (Stampa oggetti utenti)
utilizzo suggerito 87
PRTUSRPRF (Stampa profilo utente)
descrizione 34
esempio autorizzazioni speciali 65
esempio di mancata corrispondenza 65
esempio informazioni sull'ambiente 66
informazioni sulla parola d'ordine 25, 27
RCVJRNE (Ricezione voce di giornale)
programma di uscita 83
Revoca autorizzazione pubblica (RVKPUBAUT)
descrizione 39
utilizzo suggerito 91
RVKPUBAUT (Revoca autorizzazione pubblica)
dettagli 42
SETATNPGM (Impostazione programma attenzione)
programma di uscita 83
Stampa autorizzazione coda (PRTQAUT)
descrizione 37
Stampa autorizzazione descrizione lavoro (PRTJOBDAUT)
descrizione 34
utilizzo suggerito 94
Stampa descrizione sottosistema (PRTSBSDAUT)
descrizione 34
utilizzo suggerito 118
Stampa oggetti utente (PRTUSROBJ)
descrizione 34
Stampa programmi trigger (PRTTRGPGM)
descrizione 34
Stampa riservatezza di comunicazioni (PRTCMNSEC)
descrizione 34
STREML3270 (Avvio emulazione pannello 3270)
programma di uscita 83
STRPFRMON (Avvio monitoraggio prestazioni)
programma di uscita 83
strumenti di sicurezza 30
Traccia di un lavoro (TRCJOB)
programma di uscita 83
Visualizzazione adozione programma (DSPPGMADP)
controllo 56
Visualizzazione autorizzazione oggetto (DSPOBJAU) 55
Visualizzazione autorizzazione oggetto (DSPOBJAUT) 55
Visualizzazione descrizione oggetto (DSPOBJD)
utilizzo del file di emissione 54
Visualizzazione libreria (DSPLIB) 55
Visualizzazione profilo utente (DSPUSRPRF)
utilizzo del file di emissione 54
comando, CL *(Continua)*
Visualizzazione utenti autorizzati (DSPAUTUSR)
modifica 53
Visualizzazione voci giornale di controllo (DSPAUDJRNE)
descrizione 34
utilizzo suggerito 97
Comando, iSeries 400 Creazione indirizzario 110
comando (PRTPUBAUT), Stampa oggetti autorizzati pubblicamente 107
comando (PRTPVTAUT), Stampa autorizzazioni private 106
comando, Stampa autorizzazioni private (PRTPVTAUT) 106
comando, Stampa oggetti autorizzati pubblicamente (PRTPUBAUT) 107
comando ADDPFRCOL (Aggiunta raccolta prestazioni)
programma di uscita 83
comando Aggiunta raccolta prestazioni (ADDPFRCOL)
programma di uscita 83
comando Analisi attività profilo (ANZPRFACT)
creazione di utenti esenti 30
descrizione 30
utilizzo suggerito 25
comando Analisi parole d'ordine predefinite (ANZDFTPWD)
descrizione 30
utilizzo suggerito 27
comando ANZDFTPWD (Analisi parole d'ordine predefinite)
descrizione 30
utilizzo suggerito 27
comando ANZPRFACT (Analisi attività profilo)
creazione di utenti esenti 30
descrizione 30
utilizzo suggerito 25
comando autorizzazioni private (PRTPVTAUT), Stampa 106
comando Avvio emulazione pannello 3270 (STREML3270)
programma di uscita 83
comando Avvio monitoraggio prestazioni (STRPFRMON)
programma di uscita 83
comando Avvio TC/IP (STRTCP)
limitazione 127
comando Avvio TCP/IP (STRTCP)
limitazione 127
comando CHGACTPRFL (Modifica elenco profili attivi)
descrizione 30
utilizzo suggerito 26
comando CHGEXPSCDE (Modifica scadenza voce di pianificazione)
descrizione 30
comando CHGEXPSCDE (Modifica voce SCD di scadenza)
utilizzo suggerito 26
comando CHGMSGD (Modifica descrizione messaggio)
programma di uscita 83

comando CHGPFRCOL (Modifica raccolta prestazioni)
programma di uscita 83
Comando CHGSYSLIBL (Modifica lista librerie sistema)
limitazione dell'accesso 87
comando CHKOBJITG (Controllo integrità oggetto)
utilizzo suggerito 78
comando Configurazione riservatezza sistema (CFGSYSSEC)
descrizione 39
utilizzo suggerito 15
comando Controllo integrità oggetto (CHKOBJITG)
descrizione 34, 55
utilizzo suggerito 78
comando Creazione caricamento prodotto (CRTPRDLOD)
programma di uscita 83
comando di ripristino
limitazione dell'accesso 87
comando di salvataggio
limitazione dell'accesso 87
comando DSPACTPRFL (Visualizzazione elenco profili attivi)
descrizione 30
comando DSPACTSCD (Visualizzazione pianificazione attivazione)
descrizione 30
comando DSPAUTUSR (Visualizzazione utenti autorizzati)
modifica 53
comando DSPEXPSCD (Visualizzazione pianificazione di scadenza)
descrizione 30
utilizzo suggerito 26
comando DSPUSRPRF (Visualizzazione profilo utente)
utilizzo del file di emissione 54
comando ENDPFRMON (Fine monitoraggio prestazioni)
programma di uscita 83
comando Esecuzione comando remoto (RUNRMTCMD)
limitazione 165
comando Fine monitoraggio prestazioni (ENDPFRMON)
programma di uscita 83
comando Gestione descrizione sottosistema (WRKSBSD) 91
comando Gestione informazioni registrazione (WRKREGINF)
programma di uscita 85
comando Impostazione programma attenzione (SETATNPGM)
programma di uscita 83
comando Inoltro comando remoto (SBMRMTCMD)
limitazione 120
comando Invio voce di giornale (SNDJRNE) 57
comando Modifica controllo riservatezza (CHGSECAUD)
descrizione 32
utilizzo suggerito 97
comando Modifica copie riserva (CHGBCKUP)
programma di uscita 83
Comando Modifica descrizione messaggio (CHGMSGD)
programma di uscita 83
comando Modifica elenco profili attivi (CHGACTPRFL)
descrizione 30
utilizzo suggerito 26
comando Modifica lista librerie sistema (CHGSYSLIBL)
limitazione dell'accesso 87
comando Modifica raccolta prestazioni (CHGPFRCOL)
programma di uscita 83
comando Modifica scadenza voce di pianificazione (CHGEXPSCDE)
descrizione 30
comando Modifica voce Scd di attivazione (CHGACTSCDE)
descrizione 30
utilizzo suggerito 24
comando Modifica voce SCD di scadenza (CHGEXPSCDE)
utilizzo suggerito 26
comando oggetti autorizzati pubblicamente (PRTPUBAUT), Stampa 107
comando PRTADPOBJ (Stampa oggetti di adozione)
descrizione 34
comando PRTCMNSEC (Stampa riservatezza di comunicazione)
esempio 121, 125
comando PRTPUBAUT (Stampa oggetti autorizzati pubblicamente)
descrizione 34
utilizzo suggerito 115
comando PRTPVTAUT (Stampa autorizzazioni private)
descrizione 36
elenco di autorizzazioni 34, 60
utilizzo suggerito 115
comando PRTSYSSECA (Stampa attributi riservatezza di sistema)
descrizione 34
emissione esempio 8
utilizzo suggerito 15
comando PRTUSROBJ (Stampa oggetti utente)
utilizzo suggerito 87
comando PRTUSRPRF (Stampa profilo utente)
descrizione 34
esempio autorizzazioni speciali 65
esempio di mancata corrispondenza 65
esempio informazioni sull'ambiente 66
informazioni sulla parola d'ordine 25, 27
comando remoto
limitazione con voce PGMEVOKE 121
prevenzione 120, 165
comando Revoca autorizzazione pubblica (RVKPUBAUT)
descrizione 39
dettagli 42
utilizzo suggerito 91
comando RVKPUBAUT (Revoca autorizzazione pubblica)
dettagli 42
comando SETATNPGM (Impostazione programma attenzione)
programma di uscita 83
comando Stampa attributi riservatezza di sistema (PRTSYSSECA)
descrizione 34
emissione esempio 8
utilizzo suggerito 15
comando Stampa autorizzazione coda (PRTQAUT)
descrizione 37
comando Stampa autorizzazione descrizione lavoro (PRTJOBDAUT)
descrizione 34
utilizzo suggerito 94
comando Stampa autorizzazioni private (PRTPVTAUT) 106
descrizione 36
elenco di autorizzazioni 34, 60
utilizzo suggerito 115
comando Stampa descrizione sottosistema (PRTSBSDAUT)
descrizione 34
utilizzo suggerito 118
comando Stampa oggetti autorizzati pubblicamente (PRTPUBAUT) 107
descrizione 36
utilizzo suggerito 115
comando Stampa oggetti di adozione (PRTADPOBJ)
descrizione 34
comando Stampa oggetti utente (PRTUSROBJ)
descrizione 34
utilizzo suggerito 87
comando Stampa profilo utente (PRTUSRPRF)
descrizione 34
esempio autorizzazioni speciali 65
esempio di mancata corrispondenza 65
esempio informazioni sull'ambiente 66
informazioni sulla parola d'ordine 25, 27
comando Stampa programmi trigger (PRTTRGPGM)
descrizione 34
comando Stampa riservatezza di comunicazione (PRTCMNSEC)
esempio 121, 125
comando Stampa riservatezza di comunicazioni (PRTCMNSEC)
descrizione 34
comando STRPFRMON (Avvio monitoraggio prestazioni)
programma di uscita 83
comando Traccia di un lavoro (TRCJOB)
programma di uscita 83

comando Visualizzazione adozione programma (DSPPGMADP)
controllo 56
modifica 56
comando Visualizzazione autorizzazione oggetto (DSPOBJAUT) 55
utilizzo 55
comando Visualizzazione controllo riservatezza (DSPSECAUD)
descrizione 32
comando Visualizzazione descrizione oggetto (DSPOBJD)
utilizzo del file di emissione 54
comando Visualizzazione libreria (DSPLIB) 55
utilizzo 55
comando Visualizzazione pianificazione attivazione (DSPACTSCD)
descrizione 30
comando Visualizzazione pianificazione di scadenza (DSPEXPSCD)
descrizione 30
utilizzo suggerito 26
comando Visualizzazione profilo utente (DSPUSRPRF)
utilizzo del file di emissione 54
comando Visualizzazione utenti autorizzati (DSPAUTUSR)
modifica 53
comando Visualizzazione voci giornale di controllo (DSPAUDJRNE)
descrizione 34
utilizzo suggerito 97
come evitare il collegamento
implicazioni sulla sicurezza 164
completo
ricevitore del giornale (QAUDJRN) di controllo 57
comunicazioni, APPC
Vedere APPC (advanced program-to-program communication')
Comunicazioni, Elementi di base di APPC 114
Comunicazioni, protezione di APPC 113
comunicazioni, TCP/IP
Vedere comunicazioni TCP/IP
Comunicazioni APPC, Elementi di base 114
Comunicazioni APPC protette 113
comunicazioni TCP/IP
BOOTP (Bootstrap Protocol)
limitazione porta 138
suggerimenti sulla sicurezza 137
come impedire una voce 127
DHCP (dynamic host configuration protocol)
limitazione porta 139
suggerimenti sulla sicurezza 139
DNS (domain name system)
limitazione porta 144
suggerimenti sulla sicurezza 144
FTP (file transfer protocol)
origine per programma di uscita sicurezza 169
comunicazioni TCP/IP *(Continua)*
Internet Connection Secure Server (ICSS)
descrizione 151
suggerimenti sulla sicurezza 151
Internet Connection Server (ICS)
descrizione 145
prevenzione avvio automatico del server 146
suggerimenti sulla sicurezza 145
limitazione
comando STRTCP 127
file di configurazione 129
parametro indirizzo Internet gestore (INTNETADR) 155
roaming 156
uscite 156
LPD (line printer daemon)
descrizione 153
limitazione porta 153
prevenzione avvio automatico del server 153
suggerimenti sulla sicurezza 153
protezione applicazioni porta 129
REXECD (Remote EXECution server)
limitazione porta 142
suggerimenti sulla sicurezza 142
RouteD (Route Daemon)
suggerimenti sulla sicurezza 143
SLIP (Serial Interface Line Protocol)
controllo 132
descrizione 132
protezione collegamento in entrata 133
protezione collegamento in uscita 134
SNMP (simple network management protocol)
limitazione porta 154
prevenzione avvio automatico del server 154
suggerimenti sulla sicurezza 154, 155
suggerimenti per la protezione 127
TFTP (trivial file transfer protocol)
limitazione porta 141
suggerimenti sulla sicurezza 140
comunicazioni wireless 167
Considerazioni sulla sicurezza per browser 171
consiglio
valori di sistema della parola d'ordine 15
valori di sistema di collegamento 23
contenuto
strumenti di sicurezza 30
controllo
accesso
ai comandi di ripristino 87
ai comandi di salvataggio 87
alle informazioni 47
accesso dati dai PC 159
autorizzazione adottata 79, 80
autorizzazione speciale *SAVSYS (salvataggio del sistema) 86
collegamento 15
comandi remoti 120, 165
controllo *(Continua)*
descrizione unità APPC 114
descrizioni sottosistema 91
funzione di ripristino 86
funzione di salvataggio 86
integrità oggetto 34, 78
descrizione 55
modifiche all'elenco librerie 87
oggetti modificati 55
open database connectivity (ODBC) 163
parametro indirizzo Internet gestore (INTNETADR) 155
parole d'ordine 15
parole d'ordine predefinite 30
PC (personal computer) 159
programmi di uscita 83
programmi nascosti 83
programmi pianificati 86
programmi trigger 82
sessioni APPC 114
TCP/IP
file di configurazione 129
uscite 156
voce 127
TPN (transaction program name) della struttura 94
trasferimento file System/36 52
controllo, sicurezza
suggerimenti per l'utilizzo
livello di controllo *PGMADP 80
modifica oggetto 127
panoramica 97
valore *PGMFAIL 78
valore *SAVRST 78
valore *SECURITY 78
voce del giornale CP (Modifica profilo) 25, 26
voce di giornale SV (valore di sistema) 87
Controllo automatico dell'avvio dei server TCP/IP 130
Controllo collegamenti SLIP in entrata 132
Controllo dei server TCP/IP con avvio automatico 130
controllo della sicurezza
impostazione 32
introduzione 7
operazioni di ripristino 87
suggerimenti per l'utilizzo
livello di controllo *PGMADP 80
modifica oggetto 127
panoramica 97
valore *PGMFAIL 78
valore *SAVRST 78
valore *SECURITY 78
voce del giornale CP (Modifica profilo) 25, 26
voce di giornale SV (valore di sistema) 87
visualizzazione 32
Controllo funzioni di sicurezza 52
controllo sicurezza
introduzione 52
Creazione di un file di flusso con l'API open() o creat() 110

Creazione di un indirizzario con un'API 110
Creazione di un oggetto utilizzando un'interfaccia del PC 110
Creazione indirizzario comando 110

D

Dedicated Service Tools (DST)
  parole d'ordine 23
descrizione lavoro
  stampa di parametri rilevanti per la sicurezza 34
  stampa per profili utente 66
  suggerimenti sulla sicurezza 93
descrizione sottosistema
  monitoraggio dei valori rilevanti per la sicurezza 91
  stampa di parametri rilevanti per la sicurezza 34
  suggerimenti sulla sicurezza
    nome voce di una stazione di lavoro 92
    nome voce ubicazione remota 93
    tipo di voce di una stazione di lavoro 92
    voce coda lavori 92
    voce di avvio automatico lavoro 92
    voce di comunicazione 93
    voce di instradamento 92
    voce di preavvio lavoro 93
  valori rilevanti per la sicurezza 91
  voce di comunicazione
    modalità 118
    utente predefinito 118
  voce di instradamento
    rimozione voce PGMEVOKE 121
descrizione unità
  stampa di parametri rilevanti per la sicurezza 34
descrizione unità, APPC
  Vedere descrizione unità APPC
descrizione unità di controllo
  stampa di parametri rilevanti per la sicurezza 34
descrizione unità stampante
  programma di uscita per pagine separatore 83
DHCP (dynamic host configuration protocol)
  limitazione porta 139
  suggerimenti sulla sicurezza 139
disabilitazione
  profilo utente
    automaticamente 25, 30
    impatto 27
disattivazione
  profilo utente 24
Distribuzione delle API di chiamata programma 165
DNS (domain name system)
  limitazione porta 144
  suggerimenti sulla sicurezza 144
Documenti visualizzazione oggetti elenco autorizzazioni 61
domain name system (DNS)
  limitazione porta 144
  suggerimenti sulla sicurezza 144
DST (Dedicated Service Tools)
  parole d'ordine 23
dynamic host configuration protocol (DHCP)
  limitazione porta 139
  suggerimenti sulla sicurezza 139

E

elementi di base della sicurezza 3
Elementi di base delle comunicazioni APPC 114
Elementi di base di una sessione APPC 114
elenco
  contenuto della libreria 55
  profili utente selezionati 54
  tutte le librerie 55
elenco copie di riserva
  programma di uscita 83
elenco di autorizzazioni
  controllo utilizzo-autorizzazione-adottata 81
  monitoraggio 60
  stampa delle informazioni sugli utenti con autorizzazione 60
  stampa informazioni sull'autorizzazione 34
elenco librerie
  implicazioni di sicurezza 87
elenco profili attivi
  modifica 30
emulazione unità 3270
  programma di uscita 83
errore del programma
  modifica 56
eServer Security Planner 11, 13
evitare
  conflitti di file strumento di sicurezza 29

F

file
  strumenti di sicurezza 29
file di configurazione, TCP/IP
  limitazione dell'accesso 129
file di database
  programma di uscita per informazioni sull'utilizzo 83
  protezione dall'accesso al PC 159
file logico
  programma di uscita per selezione formato record 83
File System, Integrated 101
File system, limitazione dell'accesso a QSYS.LIB 107
File System, principali (/), QOpenSys e definiti dall'utente 103
File System, QFileSvr.400 111
File System, rete 111
File System, Sicurezza per principali (/), QOpenSys e definiti dall'utente 105
File system di rete 111
File system principali (/), QOpenSys e definiti dall'utente 103
File system QFileSvr.400 111
File system QSYS.LIB, limitazione dell'accesso a 107
file transfer protocol (FTP)
  origine per programma di uscita sicurezza 169
firma oggetti 90
firma oggetto
  introduzione 90
firme digitali
  introduzione 90
forzatura
  creazione programma 78
FTP (file transfer protocol)
  origine per programma di uscita sicurezza 169
funzione di ripristino
  controllo 86
funzione di salvataggio
  controllo 86
funzione file system
  programma di uscita 83
Funzioni, Controllo sicurezza 52
Funzioni di sicurezza, Controllo 52

G

Garanzia di applet firmate 172
gestione
  ambiente utente 66
  autorizzazione 59
  autorizzazione adottata 79, 80
  autorizzazione per nuovi oggetti 60
  autorizzazione privata 63
  autorizzazione pubblica 59
  autorizzazione speciale 64
  capacità di ripristino 78
  capacità di salvataggio 78
  code di emissione 64
  code lavori 64
  descrizione sottosistema 91
  elenco di autorizzazioni 60
  funzione di ripristino 86
  funzione di salvataggio 86
  giornale di controllo 56
  programmi pianificati 86
  programmi trigger 82
giornale di controllo
  stampa voci 34
giornale di controllo danneggiato 57
giornale di controllo sicurezza
  stampa voci 34
giornale QAUDJRN (controllo)
  danneggiato 57
  gestione 56
  soglia di memoria del ricevitore 57
  voci del sistema 57

I

ICS (Internet Connection Server)
  descrizione 145

ICS (Internet Connection Server) *(Continua)*
prevenzione avvio automatico del server 146
suggerimenti sulla sicurezza 145
ICSS (Internet Connection Secure Server)
descrizione 151
suggerimenti sulla sicurezza 151
identificazione
utente APPC 115
IFS (integrated file system)
implicazioni sulla sicurezza 160
impostazione
attributi di rete 39
controllo della sicurezza 32
valori di sicurezza 39
valori di sistema 39
impostazioni globali 4
inattivo
utente
elenco 54
Indirizzari, protezione 109
Indirizzari iSeries 400 tramite unità collegate, Accesso 171
indirizzario principale, autorizzazione pubblica 105
INETD 155
Informazioni particolari 175
inoltro
prospetti sicurezza 33
instradamento nodo intermedio 123
Integrated File System 101
Integrated File System, sicurezza 101
integrità
controllo
descrizione 55
integrità oggetto
modifica 55
Internet Connection Secure Server (ICSS)
descrizione 151
suggerimenti sulla sicurezza 151
Internet Connection Server (ICS)
descrizione 145
prevenzione avvio automatico del server 146
suggerimenti sulla sicurezza 145
invio
voce giornale 57
iSeries 400 Comando Creazione indirizzario 110
iSeries Access
autorizzazione oggetto 160
codifica parola d'ordine 163
come evitare il collegamento 164
controllo accesso dati 159
implicazioni di IFS (integrated file system) 160
implicazioni sulla sicurezza 159
limitazione dei comandi remoti 165
metodi di accesso dati 159
prevenzione dei virus sul PC 159
protezione dai comandi remoti 165
server gateway 166
trasferimento file 159
virus sui PC 159
iSeries Access Express, Utilizzo di SSL 162
iSeries Access per Windows
utilizzo di SSL con 162
iSeries Navigator, Sicurezza 162

L

lavoro, APPC
assegnazione profilo utente 117
lavoro di pass-through
avvio 118
lavoro remoto
prevenzione 120
LDAP (Lightweight Directory Access Protocol)
funzioni di sicurezza 152
libreria
elenco
contenuto 55
tutte le librerie 55
libreria protetta
controllo degli oggetti utente 87
libreria QSYS38 (System/38)
limitazione comandi 52
libreria System/38 (QSYS38)
limitazione comandi 52
limitazione
Vedere anche controllo
adottata 80
Limitazione dell'accesso al file system QSYS.LIB 107
Limitazione delle sessioni APPC 114
limite
possibilità
elenco utenti 54
line printer daemon (LDP)
descrizione 153
limitazione porta 153
prevenzione avvio automatico del server 153
suggerimenti sulla sicurezza 153
livelli parola d'ordine
impostazione 16
introduzione 16
modifica 17, 18, 19, 20, 21
pianificazione 17
livello di controllo (*PGMADP) adozione programma 80
livello di controllo *PGMADP (adozione programma) 80
livello di sicurezza 10
autorizzazione oggetto 47
migrazione da 47
livello di sicurezza 20
autorizzazione oggetto 47
migrazione da 47
LPD (line printer daemon)
descrizione 153
limitazione porta 153
prevenzione avvio automatico del server 153
suggerimenti sulla sicurezza 153

M

management protocol (SNMP), simple network 154
massima
dimensione
ricevitore del giornale (QAUDJRN) di controllo 57
memoria
soglia
ricevitore del giornale (QAUDJRN) di controllo 57
memorizzazione
parole d'ordine 28
menu
strumenti di sicurezza 30
menu controllo di accesso
ambiente di transizione 49
descrizione 48
integrazione con autorizzazione all'oggetto 49
limitazioni accesso menu 48
parametri profilo utente 48
menu SECBATCH (Inoltro prospetti batch)
inoltro prospetti 33
menu sicurezza
ambiente di transizione 49
descrizione 48
integrazione con autorizzazione all'oggetto 49
limitazioni accesso menu 48
parametri profilo utente 48
messaggio
CPF1107 24
CPF1120 24
programma di uscita 83
messaggio CPF1107 24
messaggio CPF1120 24
Metodi del sistema per inviare le informazioni relative a un utente 115
modalità
voce di comunicazione 118
modifica
autorizzazione oggetto 55
controllo della sicurezza 32
elenco profili attivi 30
errore del programma 56
integrità oggetto 55
messaggi di errore del collegamento 24
parole d'ordine conosciute 21
parole d'ordine fornite dall'IBM 21
uid 112
monitoraggio
ambiente utente 66
attività della parola d'ordine 27
attività di collegamento 27
autorizzazione 59
autorizzazione adottata 79, 80
autorizzazione oggetto 55
autorizzazione per nuovi oggetti 60
autorizzazione privata 63
autorizzazione pubblica 59
autorizzazione speciale 64
capacità di ripristino 78
capacità di salvataggio 78
code di emissione 64
code lavori 64
descrizione sottosistema 91
elenco di autorizzazioni 60

monitoraggio *(Continua)*
errore del programma 56
funzione di ripristino 86
funzione di salvataggio 86
integrità oggetto 55
profilo utente
modifiche 89
programmi pianificati 86
programmi trigger 82

N

NLS (national language support)
autorizzazione oggetto 52
nome voce di una stazione di lavoro
suggerimenti sulla sicurezza 92
nome voce ubicazione remota
suggerimenti sulla sicurezza 93
Nuovi oggetti, sicurezza 109
nuovo oggetto
gestione autorizzazione 60

O

ODBC (open database connectivity)
controllo accesso 163
origine per programma di uscita sicurezza 169
Oggetti, sicurezza per nuovi 109
oggetto
gestione autorizzazione al nuovo 60
modificato
controllo 55
origine autorizzazione
stampa elenco 60
stampa
autorizzazione adottata 34
non IBM 34
origine autorizzazione 34
oggetto utente
in librerie protette 87
open database connectivity (ODBC)
controllo accesso 163
origine per programma di uscita sicurezza 169
Operations Console
autenticazione unità 74
autenticazione utente 74
connettività diretta 74, 75
connettività LAN 74, 75
console remota 73
crittografia 73
integrità dei dati 75
profili utente 73
profili utente programmi di manutenzione 73
riservatezza dei dati 74
utilizzo 73
wizard di configurazione 76
Operations Console con connettività LAN
modifica parola d'ordine 75
utilizzo 75
wizard di configurazione
parola d'ordine profilo unità programmi di manutenzione 76
Operations Console con connettività LAN *(Continua)*
wizard di configurazione *(Continua)*
profilo unità programmi di manutenzione 76
operazione di commit
programma di uscita 83
operazione di rolback
programma di uscita 83
origine
programmi di uscita sicurezza 169

P

pagina separatore
programma di uscita 83
pannello di collegamento
modifica messaggi di errore 24
pannello Visualizzazione utenti autorizzati (DSPAUTUSR) 53
parametro (FMTSLR) programma di selezione formato record 83
parametro AUTOCRTCTL (creazione automatica unità di controllo) 124
parametro avvio programma SNUF 123
parametro coda messaggi (MSGQ) 66
parametro CPSSN (sessioni control-point) 124
parametro creazione automatica unità di controllo (AUTOCRTCTL) 124
parametro FMTSLR (programma di selezione formato record) 83
parametro forzatura creazione (FRCCRT) 78
parametro FRCCRT (forzatura creazione) 78
parametro indirizzo Internet gestore (INTNETADR)
limitazione 155
parametro INTNETADR (indirizzo Internet gestore)
limitazione 155
parametro libreria corrente (CURLIB) 66
parametro LOCPWD (parola d'ordine di ubicazione) 114
parametro menu iniziale (INLMNU) 66
parametro parola d'ordine di ubicazione (LOCPWD) 114
parametro PREESTSSN (sessione pre-stabilita) 123
parametro programma iniziale (INLPGM) 66
parametro SECURELOC (ubicazione protetta) 122
descrizione 117
diagramma 114
valore *VFYENCPWD (verifica parola d'ordine codificata) 117
Valore *VFYENCPWD (verifica parola d'ordine codificata) 122
parametro sessione pre-stabilita (PREESTSSN) 123
parametro sessione singola (SNGSSN) 123
parametro sessioni control-point (CPSSN) 124
parametro SNGSSN (sessione singola) 123
parametro Supporto-APPN (ANN) 123
parametro tempificatore scollegamento 124
parametro ubicazione protetta (SECURELOC) 122
descrizione 117
diagramma 114
valore *VFYENCPWD (verifica parola d'ordine codificata) 117, 122
parametro USEADPAUT (utilizzo autorizzazione adottata) 80
parametro utilizzo autorizzazione adottata (USEADPAUT) 80
parola d'ordine
attività di monitoraggio 27
codifica
sessioni PC 163
codifica a senso unico 27
controllo predefinito 30
impostazione predefinita 27
impostazione regole 15
memorizzazione 28
modifica fornite dall'IBM 21
profilo utente QPGMR (programmatore) 41
profilo utente QSRV (servizio) 41
profilo utente QSRVBAS (servizio base) 41
profilo utente QSYSOPR (operatore di sistema) 41
profilo utente QUSER (utente) 41
valore di sistema (QPWDEXPITV) intervallo di scadenza
impostazione consigliata 15
valore di sistema (QPWDLMTAJC) caratteri adiacenti limitati
impostazione consigliata 15
valore di sistema (QPWDLMTCHR) caratteri limitati
impostazione consigliata 15
valore di sistema (QPWDLMTREP) caratteri ripetuti limitati
impostazione consigliata 15
valore di sistema (QPWDMAXLEN) lunghezza massima
impostazione consigliata 15
valore di sistema (QPWDMINLEN) lunghezza minima
impostazione consigliata 15
valore di sistema (QPWDPOSDIF) differenza di posizione richiesta
impostazione consigliata 15
valore di sistema (QPWDRQDDGT) carattere numerico richiesto
impostazione consigliata 15
valore di sistema (QPWDRQDDIF) differenza richiesta
impostazione consigliata 15
valore di sistema (QPWDVLDPGM) programma di convalida
impostazione consigliata 15
valore di sistema carattere numerico richiesto (QPWDRQDDGT)
valore impostato dal comando CFGSYSSEC 40

parola d'ordine *(Continua)*
valore di sistema caratteri adiacenti limitati (QPWDLMTAJC)
valore impostato dal comando CFGSYSSEC 40
valore di sistema caratteri limitati (QPWDLMTCHR)
valore impostato dal comando CFGSYSSEC 40
valore di sistema caratteri ripetuti limitati (QPWDLMTREP)
valore impostato dal comando CFGSYSSEC 40
valore di sistema differenza di posizione richiesta (QPWDPOSDIF)
valore impostato dal comando CFGSYSSEC 40
valore di sistema differenza richiesta (QPWDRQDDIF)
valore impostato dal comando CFGSYSSEC 40
valore di sistema intervallo scadenza (QPWDEXPITV)
valore impostato dal comando CFGSYSSEC 40
valore di sistema lunghezza massima (QPWDMAXLEN)
valore impostato dal comando CFGSYSSEC 40
valore di sistema lunghezza minima (QPWDMINLEN)
valore impostato dal comando CFGSYSSEC 40
valore di sistema programma di convalida (QPWDVLDPGM)
valore impostato dal comando CFGSYSSEC 40
parola d'ordine conosciuta
modifica 21
parola d'ordine dell'ubicazione APPN 115
parole d'ordine
modifica 21
partizioni, logiche 70
partizioni logiche, sicurezza 70
PC (personal computer)
autorizzazione oggetto 160
codifica parola d'ordine 163
come evitare il collegamento 164
controllo accesso dati 159
implicazioni di IFS (integrated file system) 160
implicazioni sulla sicurezza 159
limitazione dei comandi remoti 165
metodi di accesso dati 159
prevenzione dei virus sul PC 159
protezione dai comandi remoti 165
server gateway 166
trasferimento file 159
virus sui PC 159
personal computer
Vedere PC (personal computer)
personalizzazione
valori di sicurezza 39
pianificazione
profilo utente
attivazione 24, 30
pianificazione *(Continua)*
profilo utente *(Continua)*
disattivazione 24
scadenza 26, 30
pianificazione modifiche al livello di una parola d'ordine
aumento livello della parola d'ordine 17, 18
diminuzione livelli parole d'ordine 20, 21
modifica livelli parole d'ordine pianificazione modifiche al livello 17, 18
modifica livelli parole d'ordine (da 0 a 1) 17
modifica livelli parole d'ordine (da 0 a 2) 18
modifica livelli parole d'ordine (da 1 a 2) 18
modifica livelli parole d'ordine (da 2 a 3) 19
modifica livello parola d'ordine da 1 a 0 21
modifica livello parola d'ordine da 2 a 0 21
modifica livello parola d'ordine da 2 a 1 20
modifica livello parola d'ordine da 3 a 0 20
modifica livello parola d'ordine da 3 a 1 20
modifica livello parola d'ordine da 3 a 2 20
modifiche QPWDLVL 17, 18
possibilità di immissione comandi
elenco utenti 54
prevenzione
voce TCP/IP 127
Prevenzione dell'accesso ad altri sistemi da parte di utenti del collegamento in entrata 134
Prevenzione e rilevazione di atti illeciti 89
profili utente programmi di manutenzione
gestione DST 67
profili utente programmi di manutenzione (DST) 67
profilo
analisi con query 53
utente 53
ampie dimensioni, esame 54
elenco di inattivi 54
elenco di utenti con autorizzazioni speciali 54
elenco di utenti con possibilità di immissione comandi 54
elenco selezionato 54
profilo, gruppo
Vedere profilo di gruppo
profilo, utente
Vedere profilo utente
profilo di gruppo
introduzione 5
profilo fornito dall'IBM
modifica parola d'ordine 21
profilo unità programmi di manutenzione
attributi
console 75
modifica parola d'ordine 75
parola d'ordine 75
parola d'ordine predefinita 75
protezione 76
profilo utente
ampie dimensioni, esame 54
analisi
tramite autorizzazioni speciali 34
tramite classe utente 34
analisi con query 53
assegnazione per lavoro APPC 117
controllo accesso menu 48
controllo parole d'ordine predefinite 30
disabilitazione
automaticamente 25
elaborazione inattivi 25
elenco
inattivo 54
selezionato 54
utenti con autorizzazioni speciali 54
utenti con possibilità di immissione comandi 54
elenco di attivi in modo permanente
modifica 30
introduzione 5
mancata corrispondenza tra autorizzazioni speciali e classe utente 65
modifica
utenti autorizzati 53
monitoraggio 89
monitoraggio autorizzazioni speciali 64
monitoraggio classe utente 65
monitoraggio impostazioni ambiente 66
parola d'ordine predefinita 27
pianificazione attivazione 24
pianificazione disattivazione 24
pianificazione scadenza 26
prevenzione della disabilitazione 26
rimozione automatica 26
rimozione inattivi 25
stampa
Vedere anche elenco
ambiente 66
autorizzazioni speciali 64
stato (*DISABLED) disabilitato 27
visualizzazione pianificazione scadenza 26
profilo utente di ampie dimensioni 54
profilo utente QPGMR (programmatore)
parola d'ordine impostata dal comando CFGSYSSEC 41
profilo utente QSRV (servizio)
parola d'ordine impostata dal comando CFGSYSSEC 41
profilo utente QSRVBAS (servizio base)
parola d'ordine impostata dal comando CFGSYSSEC 41

profilo utente QSYSOPR (operatore di sistema)
parola d'ordine impostata dal comando CFGSYSSEC 41
profilo utente QUSER (utente)
parola d'ordine impostata dal comando CFGSYSSEC 41
programma
Vedere anche programma trigger
forzatura creazione 78
funzione per adottare un'autorizzazione
modifica 56
nascosto
controllo 83
pianificato
valutazione 86
programma di attenzione
programma di uscita 83
stampa per profili utente 66
Programma di pianificazione lavoro
valutazione programmi 86
programma di uscita
API QHFRGFS 83
API QTNADDCR 83
attributo di rete (DDMACC) accesso di richiesta DDM 83, 169
attributo di rete (PCSACC) accesso di richiesta client 83, 169
comando RCVJRNE 83
comando SETATNPGM (Impostazione programma attenzione) 83
comando STREML3270 (Avvio emulazione pannello 3270) 83
comando Traccia di un lavoro (TRCJOB) 83
Creazione caricamento prodotto (comando CRTPRDLOD) 83
descrizione messaggio 83
descrizione unità stampante 83
elenco copie di riserva (comando CHGBCKUP) 83
funzione di registrazione 85
funzioni file system 83
Modifica descrizione messaggio (comando CHGMSGD) 83
open database connectivity (ODBC) 169
operazione di commit 83
operazione di rollback 83
origini 169
pagine separatore 83
programma di attenzione 83
programma QUSCLSXT 83
raccolta prestazioni 83
ricezione voci di giornale 83
ripulitura automatica (QEZUSRCLNP) 83
selezione formato 83
selezione formato file logico 83
tasto funzionale emulazione 3270 83
utilizzo file di database 83
valore di sistema (QPWDVLDPGM) programma di convalida parola d'ordine 83, 169
programma di uscita *(Continua)*
valore di sistema Consentire collegamento remoto (QRMTSIGN) 83, 169
valore di sistema QATNPGM (programma di attenzione) 83
valutazione 83
programma di uscita QEZUSRCLNP 83
programma nascosto
controllo 83
programma QUSCLSXT 83
programma scansione virus 78
programma trigger
elencare tutto 34
monitoraggio dell'utilizzo 82
valutazione uso 83
Programmi, Utilizzo uscita sicurezza 169
programmi che adottano l'autorizzazione
limitazione 80
monitoraggio dell'utilizzo 79
programmi di adozione
visualizzazione 56
programmi di manutenzione
profili utente (programmi di manutenzione) 67
Programmi di uscita sicurezza, Utilizzo 169
Programmi sospetti, Rilevazione 77
proprietà, oggetti 52
proprietà oggetto 52
protezione
applicazioni porta TCP/IP 129
comunicazioni TCP/IP 127
contro virus del computer 77
strumenti di sicurezza 29
protezione di integrità
livello di sicurezza (QSECURITY) 40 3
Protezione indirizzari 109
protezione integrità avanzata
livello di sicurezza (QSECURITY) 50 4
Protezione per nuovi oggetti 109
protocol (SNMP), simple network management 154
protocollo point-to-point (PPP)
considerazioni sulla sicurezza 136
pubblicazioni
correlate 173
pubblicazioni correlate 173

Q

QCONSOLE
parola d'ordine predefinita 75
QMAXSIGN (numero massimo di tentativi di collegamento)
impostazione consigliata 23
QPWFSERVER 108

R

raccolta prestazioni
programma di uscita 83
RCVJRNE (Ricezione voce di giornale)
programma di uscita 83
regolazione
Vedere controllo
Remote EXECution server (REXECD)
limitazione porta 142
suggerimenti sulla sicurezza 142
revoca
autorizzazione pubblica 39
REXECD (Remote EXECution server)
limitazione porta 142
suggerimenti sulla sicurezza 142
ricevitore di giornale
soglia di memoria 57
Ricezione voce di giornale (RCVJRNE)
programma di uscita 83
ricezione voci di giornale
programma di uscita 83
Rilevazione programmi sospetti 77
rimozione
profili utente inattivi 25
profilo utente automaticamente 26, 30
voci di instradamento PGMEVOKE 121
ripristino
giornale di controllo danneggiato 57
ripulitura, automatica
programma di uscita 83
ripulitura automatica
programma di uscita 83
roaming, TCP/IP
limitazione 156
Route Daemon (RouteD)
suggerimenti sulla sicurezza 143
RouteD (Route Daemon)
suggerimenti sulla sicurezza 143

S

salvataggio
strumenti di sicurezza 30
scadenza
profilo utente
impostazione pianificazione 26, 30
visualizzazione pianificazione 30
scansione
modifiche oggetto 55
scaricamento
richiesta autorizzazione 160
SECURE(NONE)
descrizione 116
SECURE(PROGRAM)
descrizione 116
SECURE(SAME)
descrizione 116
SECURITY(NONE)
con il valore *FRCSIGNON per il valore di sistema QRMTSIGN 116
Serial Interface Line Protocol (SLIP)
controllo 132
descrizione 132
protezione collegamento in entrata 133
protezione collegamento in uscita 134

server
definizione 113
server gateway
questioni di sicurezza 166
Sessione, Elementi di base di APPC 114
Sessioni APPC, Limitazione 114
sfruttamento-identità 123
Sicurezza, approccio dell'Integrated File System 101
sicurezza, fisica 89
Sicurezza, LP 69
sicurezza delle risorse
definizione 3
limitazione dell'accesso
introduzione 5
sicurezza di collegamento
definizione 3
Sicurezza e iSeries Navigator 162
sicurezza fisica 89
sicurezza libreria 51
Sicurezza LP 69
Sicurezza per file system principali (/), QOpenSys e definiti dall'utente 105
sicurezza risorse
introduzione 5
simple network management protocol (SNMP) 154
limitazione porta 154
prevenzione avvio automatico del server 154
suggerimenti sulla sicurezza 154, 155
Sistema, file di rete 111
Sistema, file QFileSvr.400 111
Sistema, limitazione dell'accesso al file QSYS.LIB 107
Sistema, Sicurezza per file principali (/), QOpenSys e definiti dall'utente 105
sistema basato sull'oggetto
implicazioni di sicurezza 47
protezione contro i virus del computer 77
sistema client
definizione 113
sistema di destinazione
definizione 113
sistema di origine
definizione 113
sistema di valore operazione ripristino unità (QDEVRCYACN)
valore impostato dal comando CFGSYSSEC 40
sistema locale
definizione 113
sistema remoto
definizione 113
sito Web protetto 151
SLIP (Serial Interface Line Protocol)
controllo 132
descrizione 132
protezione collegamento in entrata 133
protezione collegamento in uscita 134
sniffing 164
SNMP (simple network management protocol)
limitazione porta 154
SNMP (simple network management protocol) *(Continua)*
prevenzione avvio automatico del server 154
suggerimenti sulla sicurezza 154, 155
SSL
utilizzo con iSeries Access per Windows 162
SSL (secure sockets layer)
utilizzo con iSeries Access per Windows 162
stampa
attributi di rete 34
attributi sicurezza di sistema 8
controllo voci giornale 34
elenco di oggetti non IBM 34
impostazioni delle comunicazioni rilevanti per la sicurezza 34
informazioni sull'elenco di autorizzazioni 34, 60
informazioni sull'oggetto adottato 34
oggetti autorizzati pubblicamente 36
parametri coda di emissione rilevanti per la sicurezza 37
parametri coda lavori rilevanti per la sicurezza 37
programmi trigger 34
valori di sistema 34
stampare
valori di descrizione sottosistema rilevanti per la sicurezza 34
strumenti di sicurezza
autorizzazione per i comandi 29
comandi 30
conflitti di file 29
contenuto 30
file 29
menu 30
protezione 29
protezione emissione 29
salvataggio 30
STS (Service Tools Server)
partizioni logiche 70
supporto di gestione del giornale di modifica sistema 57

T

TCP/IP
protocollo point-to-point (PPP)
considerazioni sulla sicurezza 136
TFTP (trivial file transfer protocol)
limitazione porta 141
suggerimenti sulla sicurezza 140
tipo di voce di una stazione di lavoro
suggerimenti sulla sicurezza 92
TPN (transaction program name) della struttura
suggerimenti sulla sicurezza 94
TPN (transaction program name) strutturati
elenco fornito dall'IBM 95
trasferimento file
limitazione 52
PC (personal computer) 159
trasferimento file System/36
limitazione 52
trivial file transfer protocol (TFTP)
limitazione porta 141
suggerimenti sulla sicurezza 140
Trojan horse (Cavallo di Troia)
controllo 83
descrizione 82
eredità dell'autorizzazione adottata 81

U

uid
modifica 112
Unità collegate, accesso agli indirizzari iSeries 400 tramite 171
uscita registrata
valutazione 85
utente
lavoro APPC 115
Utente, Metodi che il sistema utilizza per inviare informazioni relative a 115
Utente APPC ottiene l'accesso al sistema di destinazione 115
utente predefinito
per TPN della struttura 94
voce di comunicazione
possibili valori 118
utente pubblico
definizione 59
Utilizzo di SSL con iSeries Access Express 162
utilizzo file
programma di uscita 83

V

valore *VFYENCPWD (verifica parola d'ordine codificata) 117, 122
valore di convalida 78
valore di convalida del programma 78
valore di sicurezza
impostazione 39
valore di sicurezza, pianificati
con il parametro SECURELOC (ubicazione protetta) 117
descrizione 115
esempi dell'applicazione 116
valore di sistema
collegamento
consigli 23
comando per impostazione 39
consentire collegamento remoto (QRMTSIGN)
influenza del valore *FRCSIGNON 116
origine per programma di uscita sicurezza 169
utilizzo di un programma di uscita 83
Conservazione dati sicurezza server (QRETSVRSEC)
descrizione 28
introduzione 4
Programma di convalida parola d'ordine (QPWDVLDPGM)
impostazione consigliata 15

valore di sistema *(Continua)*
Programma di convalida parola d'ordine (QPWDVLDPGM) *(Continua)*
origine per programma di uscita sicurezza 169
utilizzo di un programma di uscita 83
QALWOBJRST (consentire ripristino oggetto)
valore impostato dal comando CFGSYSSEC 40
QALWOBJRST (Consentire ripristino oggetto)
utilizzo suggerito 87
QAUDCTL (controllo)
modifica 32
visualizzazione 32
QAUDLVL (livello di controllo)
modifica 32
visualizzazione 32
QAUTOCFG (configurazione automatica)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
QAUTOVRT (configurazione automatica unità virtuale)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
QDEVRCYACN (operazione di ripristino unità)
come evitare rischi per la sicurezza 120
impostazione consigliata 23
QDEVRCYACN (operazione ripristino unità)
valore impostato dal comando CFGSYSSEC 40
QDSCJOBITV (intervallo supero tempo lavori scollegati)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
QDSPSGNINF (visualizzazione informazioni di collegamento)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
QINACTITV (intervallo di supero tempo lavoro inattivo)
impostazione consigliata 23
QINACTITV (intervallo supero tempo lavoro inattivo)
valore impostato dal comando CFGSYSSEC 40
QINACTMSGQ (coda messaggi lavoro inattivo)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
QLMTSECOFR (limitazione responsabile riservatezza)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
valore di sistema *(Continua)*
QMAXSGNACN (operazione quando si raggiunge il numero massimo di tentativi di collegamento)
valore impostato dal comando CFGSYSSEC 40
QMAXSIGN (numero massimo di tentativi di collegamento)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
QPWDEXPITV (intervallo scadenza parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
QPWDLMTAJC (caratteri adiacenti limitati parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
QPWDLMTCHR (caratteri limitati parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
QPWDLMTREP (caratteri ripetuti limitati parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
QPWDLMTREP (differenza di posizione richiesta nella parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
QPWDLVL (livello parola d'ordine)
impostazione consigliata 15
QPWDMAXLEN (lunghezza massima parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
QPWDMINLEN (lunghezza minima parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
QPWDRQDDGT (carattere numerico richiesto nella parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
QPWDRQDDIF (differenza richiesta nella parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
QPWDVLDPGM (programma di convalida parola d'ordine)
valore impostato dal comando CFGSYSSEC 40
QRETSVRSEC (Conservazione dati sicurezza server)
utilizzo per collegamento in uscita SLIP 135
valore di sistema *(Continua)*
QRMTSIGN (consentire collegamento remoto)
valore impostato dal comando CFGSYSSEC 40
QSECURITY (livello sicurezza)
descrizione 3
valore impostato dal comando CFGSYSSEC 40
QSYSLIBL (elenco librerie di sistema)
protezione 87
QUSEADPAUT (utilizzo autorizzazione adottata) 81
sicurezza
impostazione 39
stampa rilevante per la sicurezza 8, 34
valore di sistema (QAUTOCFG)
configurazione automatica
impostazione consigliata 23
valore di sistema (QAUTOVRT)
configurazione automatica unità virtuale
impostazione consigliata 23
valore di sistema (QINACTITV) intervallo supero tempo lavoro inattivo
impostazione consigliata 23
valore di sistema (QINACTMSGQ) coda messaggi lavoro inattivo
impostazione consigliata 23
valore di sistema (QMAXSIGN) numero massimo di tentativi di collegamento
impostazione consigliata 23
valore di sistema (QPWDVLDPGM) programma di convalida parola d'ordine
impostazione consigliata 15
origine per programma di uscita sicurezza 169
utilizzo di un programma di uscita 83
valore di sistema (QSYSLIBL) elenco librerie di sistema
protezione 87
valore di sistema (QVFYOBJRST) verifica degli oggetti al ripristino
firma digitale 79
valori di sistema ripristino
valori di sistema di ripristino (QVFYOBJRST) 79
valore di sistema coda messaggi lavoro inattivo (QINACTMSGQ)
valore impostato dal comando CFGSYSSEC 40
valore di sistema configurazione automatica (QAUTOCFG)
valore impostato dal comando CFGSYSSEC 40
valore di sistema configurazione automatica unità virtuale (QAUTOVRT)
valore impostato dal comando CFGSYSSEC 40
valore di sistema consentire collegamento remoto (QRMTSIGN)
valore impostato dal comando CFGSYSSEC 40

valore di sistema Consentire collegamento remoto (QRMTSIGN)
influenza del valore *FRCSIGNON 116
origine per programma di uscita sicurezza 169
utilizzo di un programma di uscita 83
valore di sistema consentire ripristino oggetto (QALWOBJRST)
valore impostato dal comando CFGSYSSEC 40
valore di sistema Consentire ripristino oggetto (QALWOBJRST)
utilizzo suggerito 87
valore di sistema Conservazione dati sicurezza server (QRETSVRSEC)
descrizione 28
utilizzo per collegamento in uscita SLIP 135
Valore di sistema differenza richiesta nella parola d'ordine (QPWDRQDDIF)
valore impostato dal comando CFGSYSSEC 40
valore di sistema intervallo supero tempo lavori scollegati (QDSCJOBITV)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
valore di sistema intervallo supero tempo lavoro inattivo (QINACTITV)
valore impostato dal comando CFGSYSSEC 40
valore di sistema limitazione responsabile riservatezza (QLMTSECOFR)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
valore di sistema livello sicurezza (QSECURITY)
descrizione 3
valore impostato dal comando CFGSYSSEC 40
Valore di sistema numero massimo di tentativi di collegamento (QMAXSIGN)
valore impostato dal comando CFGSYSSEC 40
valore di sistema operazione di ripristino unità (QDEVRCYACN)
come evitare rischi per la sicurezza 120
impostazione consigliata 23
valore di sistema operazione quando si raggiunge il numero massimo di tentativi di collegamento (QMAXSGNACN)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
valore di sistema QALWOBJRST (consentire ripristino oggetto)
valore impostato dal comando CFGSYSSEC 40
valore di sistema QAUDCTL (controllo)
modifica 32
visualizzazione 32
valore di sistema QAUDLVL (livello di controllo)
modifica 32
visualizzazione 32
valore di sistema QAUTOCFG (configurazione automatica)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
valore di sistema QAUTOVRT (configurazione automatica unità virtuale)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
valore di sistema QDEVRCYACN (operazione ripristino unità)
come evitare rischi per la sicurezza 120
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
valore di sistema QDSCJOBITV (intervallo supero tempo lavori scollegati)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
valore di sistema QDSPSGNINF (visualizzazione informazioni di collegamento)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
valore di sistema QINACTITV (intervallo supero tempo lavoro inattivo)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
valore di sistema QINACTMSGQ (coda messaggi lavoro inattivo)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
valore di sistema QLMTSECOFR (limitazione responsabile riservatezza)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
valore di sistema QMAXSGNACN (operazione quando si raggiunge il numero massimo di tentativi di collegamento)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
Valore di sistema QMAXSIGN (numero massimo di tentativi di collegamento)
valore impostato dal comando CFGSYSSEC 40
valore di sistema QPWDEXPITV (intervallo scadenza parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
valore di sistema QPWDLMTAJC (caratteri adiacenti limitati parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
valore di sistema QPWDLMTCHR (caratteri limitati parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
valore di sistema QPWDMAXLEN (lunghezza massima parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
valore di sistema QPWDMINLEN (lunghezza minima parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
valore di sistema QPWDPOSDIF (differenza di posizione richiesta nella parola d'ordine)
impostazione consigliata 15
Valore di sistema QPWDPOSDIF (differenza di posizione richiesta nella parola d'ordine)
valore impostato dal comando CFGSYSSEC 40
valore di sistema QPWDRQDDGT (carattere numerico richiesto nella parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
valore di sistema QPWDRQDDIF (differenza richiesta nella parola d'ordine)
impostazione consigliata 15
valore impostato dal comando CFGSYSSEC 40
valore di sistema QPWDVLDPGM (programma di convalida parola d'ordine)
valore impostato dal comando CFGSYSSEC 40
valore di sistema QRETSVRSEC (Conservazione dati sicurezza server)
descrizione 28
utilizzo per collegamento in uscita SLIP 135
valore di sistema QRMTSIGN (consentire collegamento remoto)
valore impostato dal comando CFGSYSSEC 40
valore di sistema QSECURITY (livello sicurezza)
descrizione 3
valore impostato dal comando CFGSYSSEC 40
valore di sistema QSYSLIBL (elenco librerie di sistema)
protezione 87
valore di sistema QUSEADPAUT (utilizzo autorizzazione adottata) 81

valore di sistema QVFYOBJRST (Verifica ripristino oggetto)
utilizzo suggerito 87
valore di sistema utilizzo autorizzazione adottata (QUSEADPAUT) 81
Valore di sistema Verifica ripristino oggetto (QVFYOBJRST)
utilizzo suggerito 87
valore di sistema visualizzazione nformazioni di collegamento (QDSPSGNINF)
impostazione consigliata 23
valore impostato dal comando CFGSYSSEC 40
valore verifica parola d'ordine codificata (*VFYENCPWD) 117, 122
valori di sicurezza pianificati
con il parametro SECURELOC (ubicazione protetta) 117
descrizione 115
esempi dell'applicazione 116
valutazione
programmi pianificati 86
uscita registrata 85
Verifica ripristino oggetto (QVFYOBJRST)
valore di sistema 90
virus
definizione 77
meccanismi di protezione server iSeries 78
protezione contro 77
rilevazione 55
scansione 55
scansione per 78
virus del computer
definizione 77
meccanismi di protezione server iSeries 78
protezione contro 77
scansione per 78
visualizzare
membri profilo di gruppo 50
utenti autorizzati 53
visualizzazione
autorizzazione oggetto 55
controllo della sicurezza 32
profilo utente
autorizzazioni private 94
elenco profili attivi 30
pianificazione attivazione 30
pianificazione di scadenza 30
programmi di adozione 56
valore di sistema QAUDCTL (controllo) 32
valore di sistema QAUDLVL (livello di controllo) 32
voce coda lavori
suggerimenti sulla sicurezza 92
voce del giornale CP (Modifica profilo)
utilizzo suggerito 25, 26
voce di comunicazione
modalità 118
suggerimenti sulla sicurezza 93
utente predefinito 118
voce di giornale SV (valore di sistema)
utilizzo suggerito 87
voce di instradamento
rimozione voce PGMEVOKE 121
suggerimenti sulla sicurezza 92
voce giornale
CP (Modifica profilo)
utilizzo suggerito 25, 26
invio 57
ricezione
programma di uscita 83

W

Wizard, sicurezza 11
Wizard di sicurezza 11
Wizard di sicurezza iSeries 11

Riservato ai commenti del lettore

iSeries
Suggerimenti e strumenti per la sicurezza di iSeries
Versione 5

Pubblicazione N. SC13-3198-07

Commenti relativi alla pubblicazione in oggetto potranno contribuire a migliorarla. Sono graditi commenti pertinenti alle informazioni contenute in questo manuale ed al modo in cui esse sono presentate. Si invita il lettore ad usare lo spazio sottostante citando, ove possibile, i riferimenti alla pagina ed al paragrafo.

Si prega di non utilizzare questo foglio per richiedere informazioni tecniche su sistemi, programmi o pubblicazioni e/o per richiedere informazioni di carattere generale.

Per tali esigenze si consiglia di rivolgersi al punto di vendita autorizzato o alla filiale IBM della propria zona oppure di chiamare il ″Supporto Clienti″ IBM al numero verde 800-017001.

I suggerimenti ed i commenti inviati potranno essere usati liberamente dall'IBM e dalla Selfin e diventeranno proprietà esclusiva delle stesse.

Commenti:

Si ringrazia per la collaborazione.

Per inviare i commenti è possibile utilizzare uno dei seguenti modi.

- Spedire questo modulo all'indirizzo indicato sul retro.
- Inviare un fax al numero: +39-0823-353137
- Spedire una nota via email a: translationassurance@selfin.it

Se è gradita una risposta dalla Selfin, si prega di fornire le informazioni che seguono:

Nome

Indirizzo

Società

Numero di telefono

Indirizzo e-mail

Indicandoci i Suoi dati, Lei avrà l'opportunità di ottenere dal responsabile del Servizio di Translation Assurance della Selfin S.p.A. le risposte ai quesiti o alle richieste di informazioni che vorrà sottoporci. I Suoi dati saranno trattati nel rispetto di quanto stabilito dalla legge 31 dicembre 1996, n.675 sulla "Tutela delle persone e di altri soggetti rispetto al trattamento di dati personali". I Suoi dati non saranno oggetto di comunicazione o di diffusione a terzi; essi saranno utilizzati "una tantum" e saranno conservati per il tempo strettamente necessario al loro utilizzo.

Selfin S.p.A.
Translation Assurance

Via Pozzillo

Località Ponteselice
81100 CASERTA

Printed in Denmark by IBM Danmark A/S

SC13-3198-07