System i

Sicurezza
Riferimenti alla sicurezza

Versione 6 Release 1

SC13-3195-10

System i

Sicurezza
Riferimenti alla sicurezza

Versione 6 Release 1

SC13-3195-10

Nota

Prima di utilizzare queste informazioni ed il prodotto da esse supportato, leggere le informazioni contenute in Appendice I, “Informazioni particolari”, a pagina 771.

Questa edizione si applica alla Versione 6, release 1, livello di modifica 0 di IBM i5/OS (numero prodotto 5761-SS1) ed a tutti i release e livelli di modifica successivi salvo diversamente indicato nelle nuove edizioni. Questa versione non è utilizzabile su modelli di computer RISC o CISC.

Questa edizione sostituisce SC13-3195-09.

Indice

Appendice F. Layout di voci di giornale di controllo 595

Novità in V6R1

Informazioni nuove o modificate in maniera significativa per la raccolta di argomenti Riferimenti alla sicurezza.

Nuovi valori di sistema

Blocco modifica parola d'ordine (QPWDCHGBLK)
Il valore di sistema Blocco modifica parola d'ordine (QPWDCHGBLK) specifica il periodo di tempo durante il quale le modifiche ad una parola d'ordine sono bloccate dopo l'ultima operazione di modifica della parola d'ordine riuscita.

Intervallo avvertenza scadenza parola d'ordine (QPWDEXPWRN)
Il valore di sistema Intervallo avvertenza scadenza parola d'ordine (QPWDEXPWRN) specifica il numero di giorni prima della scadenza della parola d'ordine in cui i messaggi di avvertenza della scadenza della parola d'ordine iniziano ad essere visualizzati quando un utente accede.

Regole parola d'ordine (QPWDRULES)
Il valore di sistema Regole parola d'ordine (QPWDRULES) specifica le regole utilizzate per controllare se una parola d'ordine è formata correttamente. È possibile specificare più di un valore per il valore di sistema QPWDRULES, a meno che non venga specificato *PWDSYSVAL.

Elenco specifiche codifica SSL (Secure Sockets Layer) (QSSLCSL)
Il valore di sistema Elenco specifiche codifica SSL (Secure Sockets Layer) (QSSLCSL) determina l'elenco di specifiche di codifica supportato dall'SSL di sistema.

Controllo codifica SSL (Secure Sockets Layer)(QSSLCSLCTL)
Il valore di sistema Controllo codifica SSL (Secure Sockets Layer)(QSSLCSLCTL) specifica se il sistema o l'utente controlla il valore di sistema Elenco specifiche codifica SSL (Secure Sockets Layer) (QSSLCSL).

Protocolli SSL (Secure Sockets Layer) (QSSLPCL)
Il valore di sistema Protocolli SSL (Secure Sockets Layer) (QSSLPCL) specifica i protocolli SSL (Secure Sockets Layer) supportati dall'SSL di sistema.

Come visualizzare le novità o le modifiche

Per consentire di individuare i punti in cui sono state apportate modifiche tecniche, vengono utilizzate:

- L'immagine  per contrassegnare l'inizio delle informazioni nuove o modificate.
- L'immagine  per segnalare dove finiscono le informazioni nuove o modificate.

Nei file PDF, vengono visualizzate delle barre (|) a sinistra delle informazioni nuove e modificate.

Capitolo 1. Introduzione alla sicurezza System i

La famiglia IBM Systems si rivolge a una vasta gamma di utenti. La sicurezza sulla piattaforma System i è abbastanza flessibile da soddisfare i requisiti di questa ampia gamma di utenti e situazioni.

Un piccolo sistema potrebbe avere da tre a cinque utenti ed un sistema di grandi dimensioni potrebbe avere diverse migliaia di utenti. Alcune installazioni hanno tutte le proprie stazioni di lavoro in una sola area, relativamente protetta. Altre hanno utenti ampiamente distribuiti, inclusi utenti che si connettono tramite la composizione di un numero telefonico ed utenti indiretti collegati tramite personal computer o reti di sistemi. È necessario comprendere le caratteristiche e le opzioni disponibili in modo che sia possibile adattarle ai propri requisiti di sicurezza.

La sicurezza sul sistema ha tre importanti obiettivi:

Riservatezza:
- La protezione contro la diffusione di informazioni a persone non autorizzate
- La limitazione dell'accesso alle informazioni riservate
- La protezione nei confronti di utenti del sistema curiosi e di estranei

Integrità:
- La protezione rispetto a modifiche non autorizzate dei dati
- La limitazione della manipolazione dei dati ai programmi autorizzati
- La garanzia dell'affidabilità dei dati

Disponibilità:
- La prevenzione di modifiche accidentali o della distruzione dei dati
- La protezione rispetto ai tentativi compiuti da estranei di utilizzare illecitamente o distruggere risorse di sistema

La sicurezza del sistema è spesso associata a minacce esterne, come ad esempio hacker o concorrenti in affari. Tuttavia, la protezione contro possibili danni al sistema da parte di utenti di sistema autorizzati è spesso il maggior vantaggio di una buona progettazione del sistema di sicurezza. In un sistema privo di valide funzioni di sicurezza, la pressione del tasto sbagliato potrebbe causare la cancellazione di importanti informazioni. La sicurezza del sistema può impedire questo tipo di incidente.

Le migliori funzioni del sistema di sicurezza non possono dare buoni risultati se non sono associate ad una buona pianificazione. La sicurezza impostata parzialmente, senza pianificazione, può essere poco chiara. Diventa difficile la manutenzione e il controllo. La pianificazione non implica la progettazione anticipata della sicurezza per ogni file, programma ed unità. Implica l'attuazione di un approccio globale alla sicurezza del sistema e la comunicazione di tale approccio agli sviluppatori dell'applicazione, ai programmatori e agli utenti di sistema.

Quando si pianifica la sicurezza nel sistema e si decide la quantità di sicurezza necessaria, considerare questi aspetti:
- Vi è una standard o una normativa aziendale che richiede un certo livello di sicurezza?
- I revisori della società richiedono qualche livello di sicurezza?
- Quanto è importante il sistema e i dati in esso contenuti per l'azienda?
- Quanto è importante la protezione dall'errore fornita dalle funzioni della sicurezza?
- Quali sono i requisiti di sicurezza della società previsti per il futuro?

Per facilitare l'installazione, molte delle funzioni di sicurezza nel sistema non sono attivate quando viene consegnato il sistema. In questa raccolta di argomenti sono forniti consigli per portare il sistema ad un livello di sicurezza ragionevole. Considerare i requisiti di sicurezza della propria installazione quando si valutano i suggerimenti.

Sicurezza fisica

La sicurezza fisica include la protezione dell'unità di sistema, dei dispositivi del sistema e dei supporti magnetici per la copia di riserva da danni volontari o involontari. La maggior parte delle misure intraprese per proteggere la sicurezza fisica del sistema sono esterne al sistema stesso. Tuttavia, il sistema viene fornito con una chiave di blocco che impedisce l'esecuzione di funzioni non autorizzate nell'unità di sistema.

Nota: è necessario ordinare espressamente la funzione chiave di blocco per alcuni modelli.

Informazioni correlate

Planning physical security

Sicurezza blocco a chiave

È possibile richiamare e modificare la posizione del blocco a chiave tramite l'API QWCRIPLA (Richiamo attributi IPL) o il comando CHGIPLA (Modifica attributi IPL).

Il blocco a chiave nel pannello di controllo 940x controlla l'accesso a varie funzioni del pannello di controllo del sistema.

La funzione blocco a chiave consente all'utente remoto di accedere ad ulteriori funzioni disponibili nel pannello di controllo. Ad esempio, controlla da dove verrà eseguito l'IPL della macchina ed in quale ambiente, i5/OS o DST (Dedicated Service Tools).

Il valore di sistema i5/OS QRMTSRVATR controlla l'accesso remoto. Questo valore viene fornito con impostazione predefinita su disattivato il che non consentirà la sostituzione del blocco a chiave. Il valore di sistema può essere modificato per consentire l'accesso remoto, ma non richiede le autorizzazioni speciali *SECADM e *ALLOBJ per la modifica.

Riferimenti correlati

"Attributo servizio remoto (QRMTSRVATR)" a pagina 42
Attributo servizio remoto (QRMTSRVATR) controlla la capacità di analisi dei problemi del servizio del sistema remoto. Il valore consente al sistema di essere analizzato in remoto.

Livello di sicurezza

La piattaforma System i offre cinque livelli di sicurezza. È possibile scegliere il livello di sicurezza che si desidera che il sistema applichi impostando il relativo valore di sistema (QSECURITY).

Livello 10:
Il livello 10 non è più supportato.

Livello 20:
Il sistema richiede un ID utente ed una parola d'ordine per l'accesso. A tutti gli utenti viene dato accesso agli oggetti.

Livello 30:
Il sistema richiede un ID utente ed una parola d'ordine per l'accesso. Viene applicata la sicurezza delle risorse.

Livello 40:
Il sistema richiede un ID utente ed una parola d'ordine per l'accesso. Viene applicata la sicurezza delle risorse. Vengono anche applicate ulteriori funzioni di protezione dell'integrità.

Livello 50:

Il sistema richiede un ID utente ed una parola d'ordine per l'accesso. Viene applicata la sicurezza delle risorse. Vengono applicate la protezione di integrità del livello 40 e la protezione di integrità potenziata. Il livello di sicurezza 50 è destinato a piattaforme System i con elevati requisiti di sicurezza ed è progettato per soddisfare i criteri di sicurezza CC (Common Criteria).

Riferimenti correlati

Capitolo 2, "Valore del valore di sistema Sicurezza sistema (QSecurity)", a pagina 9
È possibile scegliere il livello di sicurezza che si desidera che il sistema applichi impostando il relativo valore di sistema (QSECURITY).

Valori di sistema

I *valori di sistema* forniscono la personalizzazione di numerose caratteristiche della piattaforma System i. È possibile utilizzare i valori di sistema per definire impostazioni sulla sicurezza dell'intero sistema.

Ad esempio, è possibile specificare le seguenti impostazioni:

- Quanti tentativi di accesso sono consentiti in un'unità.
- Se il sistema scollega automaticamente una stazione di lavoro non attiva.
- Quanto spesso vanno modificate le parole d'ordine.
- La lunghezza e la composizione delle parole d'ordine.

Concetti correlati

Capitolo 3, "Valori di sistema Sicurezza", a pagina 25
I valori di sistema consentono di personalizzare molte caratteristiche del sistema. Un gruppo di valori di sistema vengono utilizzati per definire impostazioni di sicurezza su tutto il sistema.

Firma

È possibile migliorare l'integrità tramite la firma degli oggetti software utilizzati.

Un componente chiave della sicurezza è l'*integrità*: essere in grado di garantire che gli oggetti nel sistema non sono stati manomessi o alterati. Il software del sistema operativo System i è protetto da firme digitali.

La firma dell'oggetto software è particolarmente importante se l'oggetto è stato trasmesso attraverso Internet o memorizzato su supporto magnetico che si sospetta potrebbe essere stato modificato. La firma digitale può essere utilizzata per rilevare se l'oggetto è stato alterato.

Le firma digitali ed il loro uso per la verifica dell'integrità software, possono essere gestiti in conformità alle normative di sicurezza utilizzando il valore di sistema Verifica ripristino oggetto (QVFYOBJRST), il comando Controllo integrità oggetto (CHKOBJITG) e lo strumento Digital Certificate Manager. Inoltre, è possibile scegliere di firmare i propri programmi (tutti i programmi su licenza forniti con il sistema sono firmati).

È possibile limitare l'aggiunta di firme digitali ad una memoria certificato digitale utilizzando l'API Aggiunta programma di verifica e limitare la reimpostazione delle parole d'ordine nella memoria certificato digitale. L'SST (System Service Tools) fornisce una nuova opzione di menu, denominata "Gestione sicurezza sistema" nella quale è possibile limitare l'aggiunta di certificati digitali.

Informazioni correlate

Using digital signatures to protect software integrity

Digital Certificate Manager

Abilitazione del single sign-on

Single *sign-on* è un processo di autenticazione in cui un utente può accedere a più di un sistema immettendo un ID utente singolo e una parola d'ordine. Nelle reti eterogenee attuali, composte da server con partizioni e più piattaforme, gli amministratori devono affrontare la complessità di gestire l'identificazione e l'autenticazione per gli utenti della rete.

Per abilitare un ambiente single sign-on, IBM fornisce due tecnologie che cooperano per consentire agli utenti di accedere con il nome utente e la parola d'ordine Windows ed essere autenticati per le piattaforme System i nella rete. NAS (Network Authentication Service) e EIM (Enterprise Identity Mapping) sono due tecnologie che un amministratore deve configurare per abilitare un ambiente single sign-on. Windows 2000, Windows XP, AIX e z/OS utilizzano il protocollo Kerberos per autenticare gli utenti per la rete. Un sistema sicuro, centralizzato, detto KDC (key distribution center), autentica i principal (utenti Kerberos) per la rete.

Mentre NAS (Network Authentication Service) consente ad una piattaforma System i di condividere il dominio Kerberos, EIM fornisce un meccanismo per associare questi principal Kerberos ad un singolo identificativo EIM che rappresenta tale utente nell'intera organizzazione. Altre identità utente, come ad esempio un nome utente i5/OS, possono anche essere associate a tale identificativo EIM. Quando un utente si collega alla rete e accede ad una piattaforma System i, non vengono richiesti ID utente e parola d'ordine. Se l'autenticazione Kerberos ha esito positivo, le applicazioni possono ricercare l'associazione all'identificativo EIM per individuare il nome utente i5/OS. L'utente non ha più bisogno di una parola d'ordine per accedere alla piattaforma System i poiché è già autenticato tramite il protocollo Kerberos. Gli amministratori possono gestire a livello centrale le identità utente con EIM mentre gli utenti di rete devono solo gestire una parola d'ordine. È possibile abilitare il single sign-on configurando NAS (Network Authentication Service) e EIM (Enterprise Identity Mapping) sul sistema.

Informazioni correlate

Scenario: Creating a single signon test environment

Profili utente

Sul sistema operativo i5/OS, ogni profilo utente ha un profilo utente.

Al livello di sicurezza 10, il sistema crea automaticamente un profilo al primo accesso dell'utente. A livelli di sicurezza più elevati, è necessario creare un profilo utente prima che un utente possa collegarsi.

Il profilo utente è uno strumento flessibile e potente. Controlla le attività dell'utente e personalizza l'aspetto del sistema. Il seguente elenco descrive alcune importanti funzioni di sicurezza del profilo utente:

Autorizzazione speciale
: Le autorizzazioni speciali determinano se all'utente è consentito eseguire funzioni di sistema, come ad esempio la creazione di profili utente o la modifica dei lavori di altri utenti.

Menu iniziale e programma iniziale
: Il menu ed il programma iniziale determinano cosa visualizza l'utente dopo l'accesso al sistema. È possibile limitare un utente ad una serie specifica di attività limitando l'utente ad un menu iniziale.

Possibilità limitate
: Il campo possibilità limitate nel profilo utente determina se l'utente può immettere comandi e modificare il menu iniziale o il programma iniziale durante l'accesso.

Concetti correlati

Capitolo 4, "Profili utente", a pagina 79
I profili utente rappresentano uno strumento flessibile e potente. La loro creazione può facilitare notevolmente la protezione e la personalizzazione del sistema per gli utenti.

Profili di gruppo

Un *profilo di gruppo* è un tipo speciale di profilo utente. Piuttosto che fornire l'autorizzazione a ciascun utente singolarmente, è possibile utilizzare un profilo di gruppo per definire l'autorizzazione per un gruppo di utenti.

Un profilo di gruppo può possedere oggetti nel sistema. È possibile anche utilizzare un profilo di gruppo come modello nella creazione di singoli profili utente utilizzando la funzione di copia profilo.

Concetti correlati

"Pianificazione dei profili di gruppo" a pagina 256
Il profilo di gruppo è uno strumento utile da utilizzare quando diversi utenti dispongono di requisiti sulla sicurezza simili. È possibile creare direttamente file di gruppo o rendere un profilo esistente un profilo di gruppo. Quando si utilizzano profili di gruppo, è possibile gestire in maniera più efficiente l'autorizzazione e ridurre il numero di singole autorizzazioni private per gli oggetti.

"Proprietà gruppo degli oggetti" a pagina 154
Questo argomento fornisce informazioni dettagliate sulla proprietà gruppo degli oggetti.

"Gruppo principale per un oggetto" a pagina 155
È possibile specificare un gruppo principale per un oggetto.

"Copia profili utente" a pagina 127
È possibile creare un profilo utente copiando un altro profilo utente o un profilo di gruppo.

Sicurezza delle risorse

La capacità di accedere ad un oggetto viene chiamata *autorizzazione*. La sicurezza delle risorse sul sistema operativo i5/OS consente di controllare le autorizzazioni oggetto definendo chi può utilizzare gli oggetti e in che modo è possibile utilizzarli.

È possibile specificare autorizzazioni dettagliate, come ad esempio l'aggiunta di record o la modifica di record. O è possibile utilizzare le sottoserie definite dal sistema di autorizzazioni: *ALL, *CHANGE, *USE ed *EXCLUDE.

File, programmi e librerie sono gli oggetti più comuni che richiedono protezione di sicurezza, ma è possibile specificare l'autorizzazione per qualsiasi oggetto nel sistema. Il seguente elenco descrive le funzioni della sicurezza delle risorse:

Profili di gruppo
Un gruppo di utenti simili può condividere la stessa autorizzazione ad utilizzare oggetti.

Elenchi di autorizzazioni
Oggetti con esigenze di sicurezza simili possono essere raggruppati in un elenco. È possibile concedere l'autorizzazione all'elenco piuttosto che ai singoli oggetti.

Proprietà oggetto
Ogni oggetto sul sistema dispone di un proprietario. Gli oggetti possono appartenere ad un profilo utente individuale o ad un profilo di gruppo. Un'assegnazione corretta della proprietà dell'oggetto aiuta a gestire le applicazioni e delegare responsabilità per la sicurezza delle informazioni.

Gruppo principale
È possibile specificare un gruppo principale per un oggetto. L'autorizzazione del gruppo principale viene memorizzata con l'oggetto. L'utilizzo di gruppi principali può semplificare la gestione dell'autorizzazione e migliorare le prestazioni del controllo autorizzazioni.

Autorizzazione libreria
È possibile inserire file e programmi che hanno requisiti di protezione simili in una libreria e limitare l'accesso a tale libreria. Spesso è più semplice rispetto a limitare l'accesso ad ogni singolo oggetto.

Autorizzazione indirizzario
È possibile utilizzare l'autorizzazione indirizzario nello stesso modo in cui si utilizza l'autorizzazione alla libreria. È possibile raggruppare gli oggetti in un indirizzario e proteggere l'indirizzario invece che i singoli oggetti.

Autorizzazione oggetto
Nei casi in cui la limitazione dell'accesso ad una libreria o ad un indirizzario non è abbastanza specifica, è possibile limitare l'autorizzazione ad accedere a singoli oggetti.

Autorizzazione pubblica
Per ogni oggetto, è possibile definire quale tipo di accesso è disponibile per qualsiasi utente di sistema che non dispone di altre autorizzazioni all'oggetto. L'autorizzazione pubblica è un mezzo efficace per proteggere informazioni e garantire buone prestazioni.

Autorizzazione adottata
L'autorizzazione adottata aggiunge l'autorizzazione di un proprietario di programma all'autorizzazione dell'utente che esegue il programma. L'autorizzazione adottata risulta un utile strumento quando un utente ha bisogno di un'autorizzazione differente per un oggetto, a seconda della situazione.

Archivio autorizzazioni
Un archivio autorizzazioni memorizza le informazioni sull'autorizzazione per un file di database descritto dal programma. Le informazioni sull'autorizzazione vengono conservate, anche quando si cancella il file. Gli archivi autorizzazioni sono comunemente utilizzati durante la conversione da System/36, poiché le applicazioni System/36 spesso cancellano e ricreano file.

Autorizzazione a livello campo
Autorizzazioni a livello campo vengono fornite a campi singoli in un file di database. È possibile utilizzare le istruzioni SQL per gestire questa autorizzazione.

Concetti correlati

Capitolo 5, "Sicurezza delle risorse", a pagina 141
Questa sezione descrive ognuno dei componenti della sicurezza delle risorse e spiega come partecipino alla protezione delle informazioni sul sistema. Inoltre, questo capitolo spiega come utilizzare i comandi CL e i pannelli per impostare la sicurezza delle risorse sul sistema.

Giornale di controllo sicurezza

È possibile utilizzare i giornali di controllo sicurezza per controllare l'efficacia della sicurezza sul sistema.

Il sistema operativo i5/OS fornisce la capacità di registrare eventi relativi alla sicurezza in un giornale di controllo sicurezza. Diversi valori di sistema, valori profilo utente e valori oggetto controllano quali eventi vengono registrati.

Concetti correlati

Capitolo 9, "Controllo della sicurezza su System i", a pagina 275
Questa sezione descrive le tecniche per il controllo dell'efficacia della sicurezza sul proprio sistema.

Sicurezza CC (Common Criteria)

Common Criteria è un framework per la valutazione, l'analisi e la verifica indipendente di prodotti rispetto a una serie di requisiti di sicurezza.

Il 10 agosto 2005 IBM ha ricevuto una certificazione CC (Common Criteria) di i5/OS V5R3M0 all'EAL (Evaluated Assurance Level) 4 incrementata con ALC_FLR.2 del CAPP (Controlled Access Protection Profile), Versione 1.d, dell'8 ottobre 1999. Per ordinare l'Evaluated System, ordinare il Common Criteria FC 1930 in 5722-SS1.

Solo i clienti che devono effettuare l'esecuzione in una configurazione CC (Common Criteria) dovrebbero ordinare questo numero di dispositivo.

Il prodotto viene reso disponibile sulla pagina Validated Products List del sito Web Common Criteria Evaluation and Validation Scheme (http://www.nsa.gov/ia/industry/niap.cfm).

Lotto dischi indipendente

I lotti dischi indipendenti forniscono la capacità di raggruppare memoria che può essere scollegata o collegata indipendentemente dai dati del sistema o altri dati non correlati. I termini iASP (*independent auxiliary storage pool*) e *lotto dischi indipendente* rappresentano dei sinonimi.

Un lotto dischi indipendente può essere commutabile tra più sistemi in un ambiente cluster o collegato privatamente ad un singolo sistema. Per quanto riguarda V5R2, modifiche funzionali ai lotti dischi indipendenti hanno implicazioni di sicurezza per il sistema. Ad esempio, quando si esegue CRTUSRPRF, non è possibile creare un profilo utente (*USRPRF) in un lotto dischi indipendente. Tuttavia, quando un utente viene autorizzato in forma privata su un oggetto all'interno del lotto dischi indipendente, tale utente è il proprietario di un oggetto su un lotto dischi indipendenti oppure è il gruppo principale di un oggetto in un lotto dischi indipendente, il nome del profilo viene memorizzato sul lotto dischi indipendente. Se il lotto dischi indipendente viene spostato su un altro sistema, l'autorizzazione privata, la proprietà dell'oggetto e le voci del gruppo principali verranno collegate al profilo con lo stesso nome sul sistema di destinazione. Se un profilo non esiste sul sistema di destinazione, verrà creato un profilo. L'utente non disporrà di alcuna autorizzazione speciale e la parola d'ordine verrà impostata su *NONE.

I lotti dischi indipendenti supportano numerosi oggetti basati sulla libreria e UDFS (user-defined file systems). Tuttavia, diversi oggetti non sono consentiti nei lotti dischi indipendenti. In i5/OS V5R1, è possibile utilizzare lotti dischi indipendenti solo con UDFS.

Informazioni correlate

Supported and unsupported object types

Capitolo 2. Valore del valore di sistema Sicurezza sistema (QSecurity)

È possibile scegliere il livello di sicurezza che si desidera che il sistema applichi impostando il relativo valore di sistema (QSECURITY).

Panoramica

Scopo: specificare il livello di sicurezza che deve essere applicato al sistema.

Modalità:
WRKSYSVAL *SEC (comando Gestione valori di sistema) o Menu SETUP, opzione 1 (Modifica opzioni di sistema)

Autorizzazione:
*ALLOBJ e *SECADM

Voce di giornale:
SV

Nota: prima di eseguire la modifica su un sistema di produzione, leggere la sezione appropriata relativa alla migrazione da un livello ad un altro.

Livelli di sicurezza

Il sistema offre cinque livelli di sicurezza:

10 **Nessuna sicurezza applicata al sistema**

Nota: non è possibile impostare il valore di sistema QSECURITY al livello di sicurezza 10.

20 Sicurezza collegamento

30 Sicurezza collegamento e risorsa

40 Sicurezza collegamento e risorsa; protezione integrità

50 Sicurezza collegamento e risorsa; protezione integrità potenziata

Il sistema viene consegnato al livello 40, il che fornisce sicurezza dell'accesso e delle risorse e protezione dell'integrità. Per ulteriori informazioni, consultare "Livello di sicurezza 40" a pagina 14.

Se si desidera modificare il livello di sicurezza, utilizzare il comando Gestione valori di sistema (WRKSYSVAL). Il livello di sicurezza minimo che si dovrebbe utilizzare è 30. Tuttavia, è consigliabile il livello 40 o superiore. La modifica diviene operativa alla successiva esecuzione di un IPL (initial program load). La Tabella 1 mette a confronto i livelli di sicurezza nel sistema:

Tabella 1. Livelli di sicurezza: confronto funzioni

Funzione	Livello 20	Livello 30	Livello 40	Livello 50
Nome utente richiesto per l'accesso.	Sì	Sì	Sì	Sì
Parola d'ordine richiesta per l'accesso.	Sì	Sì	Sì	Sì
Sicurezza parola d'ordine attiva.	Sì	Sì	Sì	Sì
Sicurezza menu e programma iniziale attiva.	Sì[1]	Sì[1]	Sì[1]	Sì[1]
Supporto Possibilità limitate attivo.	Sì	Sì	Sì	Sì
Sicurezza risorsa attiva.	No	Sì	Sì	Sì

Tabella 1. Livelli di sicurezza: confronto funzioni (Continua)

Funzione	Livello 20	Livello 30	Livello 40	Livello 50
Accesso a tutti gli oggetti.	Sì	No	No	No
Profilo utente creato automaticamente.	No	No	No	No
Funzioni controllo sicurezza disponibili.	Sì	Sì	Sì	Sì
Impossibile creare o ricompilare programmi che contengono istruzioni limitate.	Sì	Sì	Sì	Sì
Errore al tempo di esecuzione dei programmi che utilizzano interfacce non supportate.	No	No	Sì	Sì
Protezione memoria hardware potenziata applicata all'intera memoria.	No	No	Sì	Sì
La libreria QTEMP è un oggetto temporaneo.	No	No	No	No
Gli oggetti *USRSPC, *USRIDX e *USRQ possono essere creati solo nelle librerie specificate nel valore di sistema QALWUSRDMN.	Sì	Sì	Sì	Sì
I puntatori utilizzati nei parametri sono convalidati per programmi dominio utente in esecuzione nello stato sistema.	No	No	Sì	Sì
Sono applicate regole di gestione messaggi tra programmi stato sistema e utente.	No	No	No	Sì
Non è possibile modificare direttamente lo spazio associato di un programma.	No	No	Sì	Sì
I blocchi controllo interni sono protetti.	No	No	Sì	Sì [2]

[1] Quando si specifica LMTCPB(*YES) nel profilo utente.

[2] Al livello 50, viene applicata maggiore protezione dei blocchi di controllo interni rispetto al livello 40. Consultare "Prevenzione della modifica dei blocchi di controlli interni" a pagina 21.

Autorizzazioni speciali predefinite

Il livello di sicurezza del sistema determina quali sono le autorizzazioni speciali predefinite per ogni classe utente. Quando si crea un profilo utente, è possibile selezionare autorizzazioni speciali in base alla classe utente. Autorizzazioni speciali vengono anche aggiunte ed eliminate dai profili utente quando si modificano i livelli di sicurezza.

È possibile specificare per un utente queste autorizzazioni speciali:

***ALLOBJ**
L'autorizzazione speciale a tutti gli oggetti fornisce all'utente l'autorizzazione di eseguire tutte le operazioni sugli oggetti.

***AUDIT**
L'autorizzazione speciale al controllo consente ad un utente di definire le caratteristiche del controllo del sistema, degli oggetti e degli utenti di sistema.

***IOSYSCFG**
L'autorizzazione speciale alla configurazione del sistema consente ad un utente di configurare le unità di immissione ed emissione nel sistema.

***JOBCTL**
L'autorizzazione speciale al controllo del lavoro consente ad un utente di controllare lavori batch e stampa sul sistema.

***SAVSYS**
L'autorizzazione speciale al salvataggio del sistema consente ad un utente di salvare e ripristinare oggetti.

***SECADM**
L'autorizzazione speciale di amministratore della sicurezza consente ad un utente di gestire i profili utente sul sistema.

***SERVICE**
L'autorizzazione speciale per la manutenzione consente ad un utente di eseguire funzioni di manutenzione software nel sistema.

***SPLCTL**
L'autorizzazione speciale al controllo spool consente un controllo non limitato di lavori batch e code di emissione nel sistema.

È anche possibile impedire ad utenti con autorizzazioni *SECADM e *ALLOBJ di modificare questo valore di sistema relativo alla sicurezza tramite il comando CHGSYSVAL. È possibile specificare questa limitazione in SST (System Service Tools) con l'opzione ″Gestione sicurezza sistema″.

Nota: questa limitazione si applica a diversi altri valori di sistema.
Per dettagli su come limitare le modifiche ai valori di sistema relativi alla sicurezza ed un elenco completo dei valori di sistema interessati, consultare Valori di sistema Sicurezza.

La Tabella 2 indica le autorizzazioni speciali predefinite per ogni classe utente. Le voci indicano che l'autorizzazione è assegnata solo ai livelli di sicurezza 10 e 20, a tutti i livelli di sicurezza o a nessuno.

Tabella 2. Autorizzazioni speciali predefinite per le classi utente per livello di sicurezza

Autorizzaz. speciale	**Classi utente**				
	***SECOFR**	***SECADM**	***PGMR**	***SYSOPR**	***USER**
*ALLOBJ	Tutto	10 o 20	10 o 20	10 o 20	10 o 20
*AUDIT	Tutto				
*IOSYSCFG	Tutto				
*JOBCTL	Tutto	10 o 20	10 o 20	Tutto	
*SAVSYS	Tutto	10 o 20	10 o 20	Tutto	10 o 20
*SECADM	Tutto	Tutto			
*SERVICE	Tutto				
*SPLCTL	Tutto				

Nota: gli argomenti "Classe utente" a pagina 85 e "Autorizzazione speciale" a pagina 91 forniscono ulteriori informazioni sulle classi utente e le autorizzazioni speciali.

Considerazioni

Un livello di sicurezza 30 o superiore è consigliato poiché il sistema non concede automaticamente agli utente accesso a tutte le risorse. A livelli di sicurezza inferiori, a tutti gli utenti viene concessa l'autorizzazione speciale *ALLOBJ.

Al livello di sicurezza 30 (o inferiore), gli utenti sono in grado di richiamare le interfacce di sistema che passano al profilo utente QSECOFR o di concedere agli utenti accesso a risorse a cui normalmente non potrebbero accedere. Al livello di sicurezza 40, agli utenti non è consentito di richiamare direttamente queste interfacce. Pertanto, il livello di sicurezza 40 o superiore è fortemente consigliato.

Il livello di sicurezza 40 fornisce ulteriore protezione di integrità senza influenzare le prestazioni di sistema. Le applicazioni che non vengono eseguite al livello di sicurezza 40 hanno un impatto negativo sulle prestazioni al livello di sicurezza 30. Esse fanno sì che il sistema risponda alle violazioni di dominio.

Il livello di sicurezza 50 è destinato a sistemi con requisiti di sicurezza molto elevati. Se si esegue il sistema al livello di sicurezza 50, è possibile notare un qualche effetto sulle prestazioni a causa del controllo aggiuntivo effettuato dal sistema.

Anche se si desidera concedere a tutti gli utenti accesso a tutte le informazioni, si consideri l'eventualità di far funzionare il proprio sistema al livello di sicurezza 30. È possibile utilizzare la capacità di autorizzazione pubblica per fornire agli utenti accesso alle informazioni. L'utilizzo del livello di sicurezza 30 dall'inizio offre all'utente la flessibilità necessaria a proteggere qualche risorsa di importanza critica quando appare opportuno senza dover verificare di nuovo tutte le applicazioni.

Concetti correlati

"Livello di sicurezza" a pagina 2
La piattaforma System i offre cinque livelli di sicurezza. È possibile scegliere il livello di sicurezza che si desidera che il sistema applichi impostando il relativo valore di sistema (QSECURITY).

Attività correlate

"Disabilitzione livello di sicurezza 50" a pagina 22
Una volta passati al livello di sicurezza 50, è possibile scoprire che è necessario tornare temporaneamente al livello di sicurezza 30 o 40. Ad esempio, potrebbe essere necessario verificare gli errori di integrità delle nuove applicazioni; oppure è possibile scoprire problemi di integrità che non appaiono ai livelli di sicurezza inferiori.

Livello di sicurezza 10

Al livello di sicurezza 10, non vi è alcuna protezione di sicurezza. Pertanto, il livello di sicurezza 10 non è consigliato.

A partire dalla Versione 4 Release 3, non è possibile impostare il livello di sicurezza su 10. Se il sistema è attualmente al livello 10, rimarrà al livello 10 quando si installa la Versione 4 Release 3. Se si modifica il livello di sistema in qualche altro valore, non è possibile riportarlo al livello 10.

Quando un nuovo utente si collega, il sistema crea un profilo utente con un nome profilo uguale all'ID utente specificato sul pannello di accesso. Se lo stesso utente si collega successivamente con un ID utente differente, viene creato un nuovo profilo utente. L'Appendice B, "Profili utente forniti da IBM", a pagina 341 mostra i valori predefiniti utilizzati quando il sistema crea automaticamente un profilo utente.

Il sistema esegue il controllo autorizzazioni a tutti i livelli di sicurezza. Poiché a tutti i profili utente creati al livello di sicurezza 10 viene concessa l'autorizzazione speciale *ALLOBJ, gli utenti superano con esito positivo quasi ogni controllo autorizzazioni ed hanno accesso a tutte le risorse. Se si desidera verificare l'effetto del passaggio ad un livello di sicurezza superiore, è possibile eliminare l'autorizzazione speciale *ALLOBJ dai profili utente e concedere a tali profili l'autorizzazione ad utilizzare specifiche risorse. Tuttavia, questo non fornisce alcuna protezione di sicurezza. Chiunque può collegarsi con un nuovo ID utente e viene creato un nuovo profilo con autorizzazione speciale *ALLOBJ. Non è possibile impedire questo inconveniente al livello di sicurezza 10.

Livello di sicurezza 20

Il livello di sicurezza 20 fornisce più funzioni di sicurezza del livello 10. Tuttavia, poiché al livello di sicurezza 20 tutti i profili vengono creati con l'autorizzazione speciale *ALLOBJ per impostazione predefinita, il livello di sicurezza 20 non è consigliato.

Il livello di sicurezza 20 garantisce le seguenti funzioni di sicurezza:

- Sono necessari sia ID utente che parola d'ordine per l'accesso.

- Solo un responsabile della riservatezza o qualcuno con autorizzazione speciale *SECADM può creare profili utente.
- Viene applicato il valore possibilità limitate specificato nel profilo utente.

Passaggio al livello 20 dal livello 10

Quando si passa dal livello 10 al livello 20, qualsiasi profilo utente creato automaticamente al livello 10 viene conservato. La parola d'ordine per ogni profilo utente creato al livello 10 è uguale al nome profilo utente. Non vengono apportate modifiche alle autorizzazioni speciali nei profili utente.

È opportuno considerare il seguente elenco di attività consigliate se si pianifica di passare dal livello 10 al livello 20 dopo che il sistema è stato in produzione:

- Elencare tutti i profili utente nel sistema utilizzando il comando Visualizzazione utenti autorizzati (DSPAUTUSR).
- Creare nuovi profili utenti con nomi standardizzati o copiare i profili esistenti e fornire loro nomi nuovi, standardizzati.
- Impostare la scadenza della parola d'ordine in ogni profilo esistente, forzando ogni utente ad assegnare una nuova parola d'ordine.
- Impostare i valori di sistema relativi alla composizione della parola d'ordine per impedire agli utenti di assegnare parole d'ordine banali.
- Esaminare i valori predefiniti nella "Valori predefiniti per i profili utente" a pagina 341 nell'Appendice B, "Profili utente forniti da IBM", a pagina 341 per qualsiasi modifica si voglia apportare ai profili automaticamente creati al livello di sicurezza 10.

Passaggio al livello 20 da un livello superiore

Quando si passa da un livello di sicurezza superiore al livello 20, vengono aggiunte delle autorizzazioni speciali ai profili utente. Così facendo, l'utente ha, almeno, l'autorizzazione speciale predefinita per la classe utente.

Quando quando si passa al livello 20 da un livello di sicurezza superiore, il sistema aggiunge l'autorizzazione speciale *ALLOBJ ad ogni profilo utente. Questo consente agli utenti di visualizzare, modificare o cancellare qualsiasi oggetto nel sistema.

Fare riferimento alla Tabella 2 a pagina 11 per vedere in cosa differiscono le autorizzazioni speciali tra il livello 20 e livelli di sicurezza superiori.

Livello di sicurezza 30

Il livello di sicurezza 30 fornisce più funzioni di sicurezza del livello di sicurezza 20.

Il livello 30 garantisce le seguenti funzioni di sicurezza, oltre a quelle fornite al livello 20:

- Agli utenti deve essere specificamente concessa l'autorizzazione ad utilizzare risorse nel sistema.
- Solo a profili utente creati con la classe di sicurezza *SECOFR viene concessa automaticamente l'autorizzazione speciale *ALLOBJ.

Passaggio al livello 30 da un livello inferiore

Quando si passa al livello di sicurezza 30 da un livello di sicurezza inferiore, il sistema modifica tutti i profili utente per aggiornare le autorizzazioni speciali la prossima volta che si esegue un IPL (initial program load).

Le autorizzazioni speciali concesse all'utente al livello 10 o 20, ma che non dovrebbe avere al livello 30 o superiore, vengono eliminate. Le autorizzazioni speciali assegnate all'utente non associate alla relativa classe utente non vengono modificate. Ad esempio, l'autorizzazione speciale *ALLOBJ viene eliminata da

tutti i profili utente tranne da quelli con una classe utente di *SECOFR. Consultare la Tabella 2 a pagina 11 per un elenco di autorizzazioni speciali predefinite e delle differenze tra livello 10 o 20 ed i livelli di sicurezza elevati.

Se il sistema ha eseguito applicazioni ad un livello di sicurezza inferiore, si dovrebbe configurare e verificare la sicurezza delle risorse prima di passare al livello di sicurezza 30. Prendere in considerazione l'esecuzione delle seguenti attività consigliate:

- Per ogni applicazione, impostare le autorizzazioni appropriate per gli oggetti applicazione.
- Verificare ogni applicazione utilizzando i profili utente effettivi o speciali profili utente di verifica.
  - Eliminare l'autorizzazione speciale *ALLOBJ dai profili utente utilizzati per la verifica.
  - Concedere le autorizzazioni applicazione appropriate ai profili utente.
  - Eseguire l'applicazione utilizzando i profili utente.
  - Controllare gli errori autorizzazione ricercando i messaggi di errore o utilizzando il giornale di controllo sicurezza.
- Quando tutte le applicazioni vengono eseguite con esito positivo con i profili di verifica, concedere le autorizzazioni appropriate per gli oggetti applicazione ai profili utente produzione che hanno accesso all'applicazione.
- Se il valore di sistema QLMTSECOFR (limite responsabile riservatezza) è 1 (Sì), gli utenti con autorizzazione speciale *ALLOBJ o *SERVICE devono essere specificamente autorizzati per le unità al livello di sicurezza 30 o superiore. È possibile concedere a tali utenti l'autorizzazione *CHANGE per le unità selezionate, concedere l'autorizzazione QSECOFR *CHANGE per le unità o modificare il valore di sistema QLMTSECOFR in 0.
- Modificare il livello di sicurezza nel sistema ed eseguire un IPL (initial program load).

Se si desidera passare al livello 30 senza definire autorizzazioni per singoli oggetti, rendere l'autorizzazione pubblica per gli oggetti applicazione sufficientemente elevata per eseguire l'applicazione. Eseguire le verifiche dell'applicazione per accertarsi che non accadano errori di autorizzazione.

Riferimenti correlati

"Definizione della modalità di accesso alle informazioni" a pagina 142
È possibile definire quali operazioni possono essere eseguite su oggetti, dati e campi.

Livello di sicurezza 40

Il livello di sicurezza 40 previene potenziali rischi per l'integrità o la sicurezza da parte di programmi che possono aggirare la sicurezza in particolari casi. Il livello di sicurezza 50 fornisce una protezione dell'integrità potenziata per installazioni con requisiti di sicurezza rigidi.

La Tabella 3 mette a confronto le modalità in cui le funzioni di sicurezza sono supportate al livello 30, 40 e 50.

Tabella 3. Confronto dei livelli di sicurezza 30, 40 e 50

Descrizione scenario	Livello 30	Livello 40	Livello 50
Un programma tenta di accedere agli oggetti utilizzando interfacce non supportate.	Voce di giornale AF [1]	Voce di giornale AF [1]; esito negativo dell'operazione.	Voce di giornale AF [1]; esito negativo dell'operazione.
Un programma tenta di utilizzare un'istruzione limitata.	Voce di giornale AF [1]; esito negativo dell'operazione.	Voce di giornale AF [1]; esito negativo dell'operazione.	Voce di giornale AF [1]; esito negativo dell'operazione.
L'utente che inoltra un lavoro non dispone dell'autorizzazione *USE per il profilo utente specificato nella descrizione lavoro.	Voce di giornale AF [1]	Voce di giornale AF[1]; il lavoro non viene eseguito.	Voce di giornale AF[1]; il lavoro non viene eseguito.

Tabella 3. Confronto dei livelli di sicurezza 30, 40 e 50 (Continua)

Descrizione scenario	Livello 30	Livello 40	Livello 50
Un utente tenta un accesso predefinito senza un ID utente e una parola d'ordine.	Voce di giornale AF [1]	Voce di giornale AF [1]; accesso non riuscito.	Voce di giornale AF [1]; accesso non riuscito.
Un programma stato *USER tenta di scrivere nell'area di sistema del disco definita come di sola lettura o nessun accesso.	È possibile che il tentativo abbia esito positivo.	Voce di giornale AF; [1] esito negativo dell'operazione.	Voce di giornale AF; [1] esito negativo dell'operazione.
È stato effettuato un tentativo di ripristinare un programma privo di valore di convalida. [2]	Non è stata eseguita alcuna convalida. Il programma deve essere convertito prima di poter essere utilizzato.	Non è stata eseguita alcuna convalida. Il programma deve essere convertito prima di poter essere utilizzato.	Non è stata eseguita alcuna convalida. Il programma deve essere convertito prima di poter essere utilizzato.
È stato effettuato un tentativo di ripristinare un programma che dispone di un valore di convalida.	Il programma di convalida viene eseguito.	Il programma di convalida viene eseguito.	Il programma di convalida viene eseguito.
È stato effettuato un tentativo di modificare lo spazio associato del programma.	Il tentativo ha esito positivo.	Voce di giornale AF; [1] esito negativo dell'operazione.	Voce di giornale AF; [1] esito negativo dell'operazione.
È stato effettuato un tentativo di modificare lo spazio indirizzo di un lavoro.	Il tentativo ha esito positivo.	Voce di giornale AF; [1] esito negativo dell'operazione.	Voce di giornale AF; [1] esito negativo dell'operazione.
Un programma stato utente tenta di chiamare o trasferire il controllo ad un programma dominio sistema.	Il tentativo ha esito positivo.	Voce di giornale AF; [1] esito negativo dell'operazione.	Voce di giornale AF; [1] esito negativo dell'operazione.
È stato effettuato un tentativo di creare un oggetto dominio utente di tipo *USRSPC, *USRIDX o *USRQ in una libreria non inclusa nel valore di sistema QALWUSRDMN.	Esito negativo dell'operazione.	Esito negativo dell'operazione.	Esito negativo dell'operazione.
Un programma stato utente invia un messaggio di eccezione ad un programma stato sistema che non si trova immediatamente sopra di esso nello stack di chiamata.	Il tentativo ha esito positivo.	Il tentativo ha esito positivo.	Esito negativo dell'operazione.
Un parametro viene passato ad un programma dominio utente in esecuzione nello stato sistema.	Il tentativo ha esito positivo.	Viene eseguita la convalida del parametro.	Viene eseguita la convalida del parametro.
Un comando fornito da IBM* viene modificato per eseguire un programma differente utilizzando il comando CHGCMD. Il comando viene modificato di nuovo per eseguire il programma originale fornito da IBM, che è un programma dominio sistema. Un utente tenta di eseguire il comando.	Il tentativo ha esito positivo.	Voce di giornale AF;[1, 3] esito negativo dell'operazione.[3]	Voce di giornale AF;[1, 3] esito negativo dell'operazione. [3]

[1] Una voce di tipo AF (authority failure/errore di autorizzazione) viene scritta nel giornale di controllo (QAUDJRN), se la funzione del controllo è attiva. Consultare il Capitolo 9, "Controllo della sicurezza su System i", a pagina 275 per ulteriori informazioni sulla funzione di controllo.

[2] I programmi creati prima della Versione 1 Release 3 non hanno un valore di convalida.

[3] Quando si modifica un comando fornito da IBM, esso non può più richiamare un programma dominio sistema.

Se si utilizza la funzione di controllo a livelli di sicurezza inferiori, il sistema registra voci di giornale per la maggior parte delle azioni riportate nella Tabella 3 a pagina 14, tranne quelle rilevate dalla funzione protezione hardware potenziata. Si ricevono avvertenze sotto forma di voci di giornale per potenziali violazioni dell'integrità. Al livello 40 e superiore, le violazioni dell'integrità fanno sì che il sistema non riesca ad eseguire l'operazione tentata.

Prevenzione dell'utilizzo di interfacce non supportate

Al livello di sicurezza 40 e superiore, il sistema previene i tentativi di chiamare direttamente programmi di sistema non documentati come interfacce a livello chiamata.

Ad esempio, la chiamata diretta al programma che elabora il comando per il comando SIGNOFF dà esito negativo.

Il sistema utilizza l'attributo dominio di un oggetto e l'attributo stato di un programma per applicare questa protezione.

- **Dominio:**

  Ogni oggetto appartiene al dominio *SYSTEM o al dominio *USER. Solo i programmi stato *SYSTEM possono accedere agli oggetti dominio *SYSTEM oppure i programmi stato *INHERIT chiamati da programmi stato *SYSTEM.

  È possibile visualizzare il dominio di un oggetto utilizzando il comando Visualizzazione descrizione oggetto (DSPOBJD) e specificando DETAIL(*FULL). È anche possibile utilizzare i seguenti comandi:

  – Visualizzazione programma (DSPPGM) per visualizzare il dominio di un programma
  – Visualizzazione programma di servizio (DSPSRVPGM) per visualizzare il dominio di un programma di servizio

- **Stato:**

  I programmi sono stato *SYSTEM, stato *INHERIT o stato *USER. I programmi stato *USER possono accedere direttamente solo ad oggetti dominio *USER. È possibile accedere ad oggetti dominio *SYSTEM utilizzando il comando o l'API (application programming interface) appropriati. Gli stati *SYSTEM e *INHERIT sono riservati ai programmi forniti da IBM.

  È possibile visualizzare lo stato di un programma utilizzando il comando DSPPGM (Visualizzazione programma). È possibile visualizzare lo stato di un programma di servizio utilizzando il comando DSPSRVPGM (Visualizzazione programma di servizio).

La Tabella 4 riporta le regole di accesso dominio e stato:

Tabella 4. Accesso dominio e stato

	Dominio oggetto	
Stato programma	***USER**	***SYSTEM**
*USER	YES	NO [1]
*SYSTEM	YES	YES

[1] Una violazione del dominio o dello stato provoca l'esito negativo dell'operazione al livello di sicurezza 40 e superiore. A tutti i livelli di sicurezza, una voce di tipo AF viene scritta nel giornale di controllo se è attiva la funzione di controllo.

Voce di giornale:

Quando vengono soddisfatte le seguenti condizioni, una voce AF (authority failure/errore autorizzazione), tipo di violazione D o R, viene scritto nel giornale QAUDJRN:

- la funzione di controllo è attiva
- Il valore di sistema QAUDLVL include *PGMFAIL

- Si è tentato di utilizzare un'interfaccia non supportata

Protezione delle descrizioni lavoro

Se un nome profilo utente viene utilizzato come valore per il campo Utente in una descrizione lavoro, qualsiasi lavoro inoltrato con la descrizione lavoro può essere eseguito con tale profilo utente. Pertanto, un utente non autorizzato potrebbe inoltrare un lavoro da eseguire con il profilo utente specificato nella descrizione lavoro.

Al livello di sicurezza 40 e superiore, il lavoro avrà esito negativo se l'utente che inoltra il lavoro non dispone di un'autorizzazione *USE sia per la descrizione lavoro che per il profilo utente specificato nella descrizione lavoro. Al livello di sicurezza 30, il lavoro si esegue se chi lo inoltra dispone dell'autorizzazione *USE per la descrizione lavoro.

Voce di giornale:

Quando vengono soddisfatte le seguenti condizioni, una voce AF, tipo di violazione J, viene scritta nel giornale QAUDJRN:

- La funzione di controllo è attiva
- Il valore di sistema QAUDLVL include *AUTFAIL
- Un utente inoltra un lavoro, quando non è autorizzato al profilo utente nella descrizione lavoro.

Accesso senza ID utente e parola d'ordine

Il livello di sicurezza determina la modalità di controllo, da parte del sistema, dell'accesso senza un ID utente e una parola d'ordine.

Al livello di sicurezza 30 e inferiori, l'accesso tramite tasto Invio senza ID utente e parola d'ordine è possibile con certe descrizioni di sottosistemi. Al livello di sicurezza 40 e superiori, il sistema interrompe qualsiasi tentativo di accesso senza ID utente e parola d'ordine.

Voce di giornale:

Quando vengono soddisfatte le seguenti condizioni, una voce AF, tipo di violazione S, viene scritta nel giornale QAUDJRN:

- La funzione di controllo è attiva
- Il valore di sistema QAUDLVL include *AUTFAIL
- Un utente tenta di accedere senza immettere un ID utente e una parola d'ordine e la descrizione sottosistema consente questa operazione

Si noti che il tentativo fallisce al livello di sicurezza 40 e superiore.

Concetti correlati

"Descrizioni sottosistema" a pagina 220
Le descrizioni sottosistema eseguono diverse funzioni sul sistema.

Protezione memoria hardware potenziata

La protezione memoria hardware potenziata consente la definizione di blocchi di informazioni di sistema ubicati sulla memoria come lettura-scrittura, sola lettura o nessun accesso.

Al livello di sicurezza 40 e superiore, il sistema controlla come i programmi stato *USER accedono a questi blocchi protetti.

La protezione memoria hardware potenziata è supportata su tutti i modelli System i.

Voce di giornale:

Quando vengono soddisfatte le seguenti condizioni, una voce AF, tipo di violazione R, viene scritto nel giornale QAUDJRN:

- La funzione di controllo è attiva
- Il valore di sistema QAUDLVL include *PGMFAIL
- Un programma tenta di scrivere su un'area della memoria protetta dalla funzione protezione memoria hardware potenziata

Protezione dello spazio associato di un programma

Per programmi OPM (original program model), al livello di sicurezza 40 e superiore, lo spazio associato di un oggetto programma non può essere modificato direttamente dai programmi stato utente. Per programmi ILE (integrated language environment), lo spazio associato di un oggetto programma non può essere modificato dai programmi stato utente a qualsiasi livello di sicurezza.

Protezione dello spazio indirizzo di un lavoro

Al livello di sicurezza 50, un programma stato utente non può ottenere l'indirizzo per un altro lavoro nel sistema. Perciò, un programma stato utente non può gestire direttamente oggetti associati ad un altro lavoro.

Convalida parametri

Le interfacce al sistema operativo i5/OS sono programmi stato sistema nel dominio utente. Quando dei parametri vengono passati tra programmi stato utente e programmi stato sistema, quei parametri devono essere controllati per impedire che qualche valore imprevisto metta a rischio l'integrità del sistema operativo.

Quando si esegue il sistema al livello di sicurezza 40 o 50, il sistema controlla in modo specifico ogni parametro passato tra un programma stato utente ed un programma stato sistema nel dominio utente. Questo è necessario perché il sistema separi il dominio sistema e utente e soddisfi i requisiti del livello di sicurezza CC (Common Criteria). È possibile notare qualche effetto sulle prestazioni a causa di questo ulteriore controllo.

Convalida dei programmi in fase di ripristino

Quando viene creato un programma, il sistema calcola un valore di convalida, che viene memorizzato con il programma. Quando il programma viene ripristinato, il valore di convalida viene calcolato di nuovo e confrontato con il valore di convalida memorizzato con il programma.

Se i valori di convalida non corrispondono, il sistema esegue l'azione in base ai valori di sistema Forzatura conversione al ripristino (QFRCCVNRST) e Abilitazione ripristino oggetto (QALWOBJRST).

Oltre ad un valore di convalida, un programma può facoltativamente avere una firma digitale che può essere verificata al ripristino. Qualsiasi operazione di sistema relativa alle firme digitali è controllata dai valori di sistema QVFYOBJRST e QFRCCVNRST. I tre valori di sistema, Verifica oggetto al ripristino (QVFYOBJRST), QFRCCVNRST e QALWOBJRST, agiscono come una serie di filtri per stabilire se un programma verrà ripristinato senza modifiche, se verrà ricreato (convertito) quando viene ripristinato o se non verrà ripristinato nel sistema.

Nota: i programmi stato di sistema devono disporre di una firma digitale IBM valida. Altrimenti, non possono essere ripristinati, indipendentemente da come sono impostati i valori di sistema

Il primo filtro è il valore di sistema QVFYOBJRST. Controlla l'operazione di ripristino su alcuni oggetti che possono avere la firma digitale. Dopo che un oggetto è stato controllato con esito positivo e viene convalidato da questo valore di sistema, l'oggetto passa al secondo filtro, il valore di sistema QFRCCVNRST. Con questo valore di sistema l'utente specifica se convertire programmi, programmi di servizio o oggetti modulo durante un'operazione di ripristino. Questo valore di sistema impedisce anche

il ripristino di certi oggetti. Solo quando gli oggetti sono passati attraverso i primi due filtri passano al filtro finale, il valore di sistema QALWOBJRST. Questo valore di sistema controlla se gli oggetti con attributi critici per la sicurezza possono essere ripristinati.

Note:

1. I programmi creati per il sistema operativo i5/OS possono contenere informazioni che consentono la ricreazione del programma al momento del ripristino, senza richiedere l'origine del programma.
2. I programmi creati per i5/OS Versione 5, Release 1 e successive, contengono le informazioni necessarie per la nuova creazione anche quando viene eliminata la capacità di osservare il programma.
3. I programmi creati per release precedenti alla Versione 5, Release 1 possono essere ricreati al momento del ripristino solo se la capacità di osservare il programma non è stata cancellata.

Riferimenti correlati

"Valori di sistema relativi alla sicurezza" a pagina 39
Questo argomento descrive i valori di sistema relativi alla sicurezza sul sistema operativo i5/OS.

Passaggio al livello di sicurezza 40

Prima di eseguire la migrazione al livello 40, accertarsi che tutte le applicazioni vengano eseguite con esito positivo al livello di sicurezza 30. Il livello di sicurezza 30 consente di verificare la sicurezza delle risorse per tutte le proprie applicazioni.

Attenersi a questa procedura per migrare al livello di sicurezza 40:

1. Attivare la funzione di controllo sicurezza, se non è già stata attivata. L'argomento "Impostazione del controllo della sicurezza" a pagina 313 fornisce istruzioni complete per l'impostazione della funzione di controllo.
2. Assicurarsi che il valore di sistema QAUDLVL includa *AUTFAIL e *PGMFAIL. *PGMFAIL registra voci di giornale per qualsiasi tentativo di accesso che violi la protezione dell'integrità al livello di sicurezza 40.
3. Controllare nel giornale di controllo le voci *AUTFAIL e *PGMFAIL mentre si eseguono tutte le applicazioni al livello di sicurezza 30. Prestare particolare attenzione ai seguenti codici di errore nelle voci di tipo AF:

   C Errore convalida oggetto

   D Violazione (dominio) interfaccia non supportata

   J Errore autorizzazione descrizione lavoro e profilo utente

   R Tentativo di accedere all'area protetta del disco (protezione memoria hardware potenziata)

   S Tentativo di accesso predefinito

   Questi codici indicano la presenza di rischi per l'integrità nelle applicazioni. Al livello di sicurezza 40, questi programmi hanno esito negativo.
4. Se si dispone di programmi creati prima della Versione 1 Release 3, utilizzare il comando CHGPGM con il parametro FRCCRT per creare valori di convalida per tali programmi. Al livello di sicurezza 40, il sistema converte qualsiasi programma ripristinato senza un valore di convalida. Questo può far aumentare considerevolmente il tempo di ripristino. Consultare l'argomento "Convalida dei programmi in fase di ripristino" a pagina 18 per ulteriori informazioni sulla convalida del programma.

   Nota: ripristinare le librerie di programmi come parte della verifica dell'applicazione. Controllare nel giornale di controllo eventuali errori di convalida.
5. In base alle voci nel giornale di controllo, intraprendere i passi necessari a correggere le applicazioni ed impedire errori di programma.

6. Modificare il valore di sistema QSECURITY in 40 ed eseguire un IPL.

Disabilitazione livello di sicurezza 40

l'utente potrebbe desiderare di tornare temporaneamente al livello 30 dal livello 40 per verificare la presenza di errori di integrità nelle nuove applicazioni. Oppure, si può scoprire che non è stata effettuata una verifica sufficientemente accurata prima di passare al livello di sicurezza 40.

È possibile passare dal livello di sicurezza 40 al livello 30 senza mettere a rischio la sicurezza delle proprie risorse. Non vengono apportate modifiche alle autorizzazioni speciali nei profili utente quando si passa dal livello 40 al livello 30. Dopo la verifica delle applicazioni e la risoluzione di qualunque errore presente nel giornale di controllo, è possibile tornare al livello 40.

Attenzione: Se si passa dal livello 40 al livello 20, vengono aggiunte alcune autorizzazioni speciali a tutti i profili utente. (Consultare la Tabella 2 a pagina 11.) In questo modo si elimina la protezione della sicurezza risorse.

Livello di sicurezza 50

Il livello di sicurezza 50 è stato progettato per soddisfare alcuni dei requisiti definiti dalla dichiarazione di conformità CAPP (Controlled Access Protection Profile) per CC (Common Criteria). Il livello di sicurezza 50 fornisce protezione di integrità potenziata, oltre a quella fornita dal livello di sicurezza 40, per installazioni con requisiti di sicurezza rigidi.

Le funzioni di sicurezza incluse per il livello di sicurezza 50 sono descritte negli argomenti che seguono:

- Limitazione dei tipi oggetto dominio utente (*USRSPC, *USRIDX e *USRQ)
- Limitazione della gestione messaggi tra programmi stato utente e sistema
- Prevenzione della modifica di tutti i blocchi d controlli interni

Limitazione oggetti dominio utente

La maggior parte degli oggetti vengono creati nel dominio di sistema. Quando si esegue il sistema al livello di sicurezza 40 o 50, è possibile accedere agli oggetti dominio sistema solo tramite i comandi e le API forniti.

Questi tipi di oggetti possono essere di dominio utente o sistema:

- Spazio utente (*USRSPC)
- Indice utente (*USRIDX)
- Coda utente (*USRQ)

Oggetti del tipo *USRSPC, *USRIDX e *USRQ nel dominio utente possono essere direttamente gestiti senza utilizzare API e comandi forniti dal sistema. Questo consente ad un utente di accedere ad un oggetto senza creare un record di controllo.

Nota: oggetti di tipo *PGM, *SRVPGM e *SQLPKG possono anche trovarsi nel dominio utente. Il loro contenuto non può essere gestito direttamente e non sono interessati dalle limitazioni.

Al livello di sicurezza 50, ad un utente non deve essere consentito passare informazioni rilevanti per la sicurezza a un altro utente senza potere scrivere un record di controllo. Per applicare questo punto:

- Al livello di sicurezza 50, nessun lavoro può ottenere la possibilità di accedere alla libreria QTEMP per un altro lavoro. Perciò, se gli oggetti dominio utente vengono memorizzati nella libreria QTEMP, non possono essere utilizzati per passare informazioni ad un altro utente.
- Per garantire la compatibilità con le applicazioni esistenti che utilizzano oggetti dominio utente, è possibile specificare ulteriori librerie nel valore di sistema QALWUSRDMN. Il valore di sistema

QALWUSRDMN viene applicato a tutti i livelli di sicurezza. Consultare “Consentire oggetti dominio utente (QALWUSRDMN)” a pagina 27 per ulteriori informazioni.

Attività correlate

“Passaggio al livello di sicurezza 50”
Se il livello di sicurezza attuale è 10 o 20, modificare il livello di sicurezza in 40 prima di modificarlo in 50. Se il livello di sicurezza attuale è 30 o 40, è necessario effettuare la valutazione del valore QALWUSRDMN e ricompilare alcuni programmi per preparare il livello di sicurezza 50.

Limitazione della gestione messaggi

Messaggi inviati tra programmi forniscono il potenziale per rischi di integrità.

Al livello di sicurezza 50, è possibile limitare i messaggi inviati tra programmi per proteggere l’integrità del sistema.

Quanto segue si applica alla gestione messaggi al livello di sicurezza 50:

- Qualsiasi programma stato utente può inviare un messaggio di qualsiasi tipo a qualsiasi altro programma stato utente.
- Qualsiasi programma stato sistema può inviare un messaggio di qualsiasi tipo a qualsiasi programma stato utente o sistema.
- Un programma stato utente può inviare un messaggio non di eccezione a qualsiasi programma stato sistema.
- Un programma stato utente può inviare un messaggio tipo eccezione (stato, notifica, o uscita) ad un programma stato sistema se risulta vera una delle seguenti condizioni:
  - Il programma stato sistema è un processore di richieste.
  - Il programma stato sistema ha chiamato un programma stato utente.

    Nota: il programma stato utente che invia il messaggio di eccezione non è necessario che sia il programma chiamato dal programma stato sistema. Ad esempio, in questo stack di chiamata, un messaggio di eccezione può essere inviato al Programma A dal Programma B, C o D:

Programma A	Stato sistema
Programma B	Stato utente
Programma C	Stato utente
Programma D	Stato utente

- Quando un programma stato utente riceve un messaggio da un’origine esterna (*EXT), qualsiasi puntatore nel testo di sostituzione del messaggio viene rimosso.

Prevenzione della modifica dei blocchi di controlli interni

Al livello di sicurezza 40, alcuni blocchi di controlli interni, come ad esempio il blocco controllo lavoro, non possono essere modificati da un programma stato utente. Al livello di sicurezza 50, nessun blocco di controlli interni al sistema può essere modificato. Questo include l’ODP (open data path), gli spazi per comandi e programmi CL ed il blocco controllo lavoro ambiente S/36.

Passaggio al livello di sicurezza 50

Se il livello di sicurezza attuale è 10 o 20, modificare il livello di sicurezza in 40 prima di modificarlo in 50. Se il livello di sicurezza attuale è 30 o 40, è necessario effettuare la valutazione del valore QALWUSRDMN e ricompilare alcuni programmi per preparare il livello di sicurezza 50.

Molte delle misure di sicurezza supplementari che vengono applicate al livello di sicurezza 50 non danno origine a voci del giornale di controllo ai livelli di sicurezza inferiori. Perciò, un'applicazione non può essere verificata per tutte le possibili condizioni di errore di integrità prima di passare al livello di sicurezza 50.

Le azioni che danno luogo ad errori al livello di sicurezza 50 non sono comuni nel software dell'applicazione normale. La maggior parte del software che si esegue con esito positivo al livello di sicurezza 40 si esegue anche al livello di sicurezza 50.

Se il sistema è attualmente in esecuzione al livello di sicurezza 30, completare i passi descritti nella sezione "Passaggio al livello di sicurezza 40" a pagina 19 per prepararsi al passaggio al livello di sicurezza 50.

Se il sistema è attualmente in esecuzione al livello di sicurezza 30 o 40, effettuare quanto segue per prepararsi per il livello di sicurezza 50:

- valutare il valore di sistema QALWUSRDMN. Il controllo degli oggetti dominio utente è importante per l'integrità del sistema.
- Ricompilare qualsiasi programma COBOL che assegni l'unità nella clausola SELECT a WORKSTATION se i programmi COBOL sono stati compilati utilizzando un compilatore precedente a V2R3.
- Ricompilare qualsiasi programma COBOL ambiente S/36 che sia stato compilato utilizzando un compilatore precedente a V2R3.
- Ricompilare qualsiasi programma RPG/400 o RPG* ambiente System/38 che utilizzi file video se è stato compilato utilizzando un compilatore precedente a V2R2.

È possibile passare direttamente dal livello di sicurezza 30 al livello di sicurezza 50. L'esecuzione al livello di sicurezza 40 come fase intermedia non arreca vantaggi significativi per la verifica.

Se l'esecuzione attualmente avviene al livello di sicurezza 40, è possibile passare al livello di sicurezza 50 senza ulteriore verifica. Il livello di sicurezza 50 non può essere verificato in anticipo. L'ulteriore protezione di integrità applicata al livello di sicurezza 50 non produce messaggi di errore o voci di giornale ai livelli di sicurezza inferiori.

Concetti correlati

"Limitazione oggetti dominio utente" a pagina 20
La maggior parte degli oggetti vengono creati nel dominio di sistema. Quando si esegue il sistema al livello di sicurezza 40 o 50, è possibile accedere agli oggetti dominio sistema solo tramite i comandi e le API forniti.

Disabilitzione livello di sicurezza 50

Una volta passati al livello di sicurezza 50, è possibile scoprire che è necessario tornare temporaneamente al livello di sicurezza 30 o 40. Ad esempio, potrebbe essere necessario verificare gli errori di integrità delle nuove applicazioni; oppure è possibile scoprire problemi di integrità che non appaiono ai livelli di sicurezza inferiori.

È possibile passare dal livello di sicurezza 50 al livello 30 o 40 senza mettere a rischio la sicurezza delle proprie risorse. Non vengono apportate modifiche alle autorizzazioni speciali nei profili utente quando si passa dal livello 50 al livello 30 o 40. Dopo la verifica delle applicazioni e la risoluzione di qualunque errore presente nel giornale di controllo, è possibile tornare al livello 50.

Attenzione: Se si passa dal livello 50 al livello 20, vengono aggiunte alcune autorizzazioni speciali a tutti i profili utente. In questo modo si elimina la protezione della sicurezza risorse.

Riferimenti correlati

Capitolo 2, “Valore del valore di sistema Sicurezza sistema (QSecurity)”, a pagina 9
È possibile scegliere il livello di sicurezza che si desidera che il sistema applichi impostando il relativo valore di sistema (QSECURITY).

Capitolo 3. Valori di sistema Sicurezza

I valori di sistema consentono di personalizzare molte caratteristiche del sistema. Un gruppo di valori di sistema vengono utilizzati per definire impostazioni di sicurezza su tutto il sistema.

È possibile porre un limite agli utenti che intendono modificare i valori di sistema relativi alla sicurezza. Gli SST (System service tools) e i DST (dedicated service tools) consentono di bloccare questi valori di sistema. In questo modo, è possibile impedire persino ad un utente che dispone dell'autorizzazione *SECADM e *ALLOBJ di modificare questi valori di sistema con il comando CHGSYSVAL. Inoltre, per limitare le modifiche a questi valori di sistema, è possibile inoltre limitare l'aggiunta di certificati digitali alla memoria preposta con la API Aggiunta programma di verifica e limitare la reimpostazione della parola d'ordine sulla memoria dei certificati digitali.

Nota: se si bloccano i valori di sistema relativi alla sicurezza ed è necessario eseguire un'operazione di ripristino come parte del ripristino di un sistema, accertarsi di dover sbloccare i valori di sistema per completare la suddetta operazione. Ciò garantisce la possibilità di modificare i valori di sistema durante l'IPL (initial program load).

È possibile limitare i seguenti valori di sistema utilizzando l'opzione di blocco:

Tabella 5. Valori di sistema che possono essere bloccati

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

È possibile utilizzare l'SST (system service tools) o il DST (dedicated service tools) per bloccare e sbloccare i valori di sistema relativi alla sicurezza. Tuttavia, è necessario utilizzare il DST in caso di modalità di ripristino poiché l'SST non è disponibile in questa modalità. In caso contrario, utilizzare SST per bloccare o sbloccare i valori di sistema relativi alla sicurezza.

Per bloccare o sbloccare i valori di sistema relativi alla sicurezza con il comando Avvio programmi di manutenzione sistema (STRSST), seguire i passi di seguito riportati:

Nota: è necessario disporre di un ID utente e di una parola d'ordine per i programmi di manutenzione per bloccare o sbloccare i valori di sistema relativi alla sicurezza.

1. Aprire un'interfaccia basata sui caratteri.
2. Sulla riga comandi, immettere `STRSST`.
3. Immettere l'ID utente e la parola d'ordine dei programmi di manutenzione.
4. Selezionare l'opzione 7 (Gestione sicurezza di sistema).
5. Immettere 1 per sbloccare i valori di sistema relativi alla sicurezza oppure 2 per bloccare i valori di sistema relativi alla sicurezza nel parametro **Consenti modifiche valori di sistema sicurezza**.

Per bloccare o sbloccare i valori di sistema relativi alla sicurezza mediante i DST (dedicated service tools) durante un IPL non presidiato di un ripristino di sistema, seguire i passi di seguito riportati:

1. Dal pannello IPL o Installazione del sistema, selezionare l'opzione 3 (Utilizzo DST (Dedicated Service Tools)).

   Nota: questa fase presuppone che l'utente sia in modalità di ripristino e che stia eseguendo un IPL presidiato.
2. Collegarsi a DST utilizzando l'ID utente e la parola d'ordine dei programmi di manutenzione.
3. Selezionare l'opzione 13 (Gestione sicurezza di sistema).
4. Immettere 1 per sbloccare i valori di sistema relativi alla sicurezza oppure 2 per bloccare i valori di sistema relativi alla sicurezza nel parametro **Consenti modifiche valori di sistema sicurezza**.

Concetti correlati

"Valori di sistema" a pagina 3
I *valori di sistema* forniscono la personalizzazione di numerose caratteristiche della piattaforma System i. È possibile utilizzare i valori di sistema per definire impostazioni sulla sicurezza dell'intero sistema.

Valori di sistema della sicurezza generali

Questo argomento introduce i valori di sistema generali che è possibile utilizzare per controllare la sicurezza sul sistema operativo i5/OS .

Panoramica:

I valori di sistema della sicurezza generali consentono all'utente di impostare la funzione della sicurezza per supportare le decisioni prese durante lo sviluppo della normativa di sicurezza. Ad esempio, nella normativa di sicurezza l'utente stabilisce che i sistemi contenenti informazioni riservate, come i pagamenti dei clienti o gli inventari delle retribuzioni, necessitano di un livello maggiore di sicurezza rispetto ai sistemi utilizzati per verificare le applicazioni sviluppate all'interno della propria azienda. È possibile pianificare e impostare un livello di sicurezza su questi sistemi che corrisponda alle decisioni prese durante lo sviluppo della propria normativa di sicurezza.

Scopo: specificare i valori di sistema che controllano la sicurezza sul sistema.

Modalità:
`WRKSYSVAL *SEC` (Comando Gestione valore di sistema)

Autorizzazione:
*ALLOBJ e *SECADM

Voce di giornale:
SV

Nota: Le modifiche diventano effettive immediatamente. L'IPL viene richiesto solo quando si modifica il livello di sicurezza (valore di sistema QSECURITY) o il livello della parola d'ordine (valore di sistema QPWDLVL).

Di seguito vengono elencati i valori di sistema generali che controllano la sicurezza del sistema:

QALWUSRDMN
Consentire oggetti dominio utente nelle librerie

QCRTAUT
Creazione autorizzazione pubblica predefinita

QDSPSGNINF
Visualizzazione informazioni sul collegamento

QFRCCVNRST
Forzatura conversione durante ripristino

QINACTITV
Intervallo supero tempo lavoro inattivo

QINACTMSGQ
Coda messaggi lavoro inattivo

QLMTDEVSSN
Limite sessioni unità

QLMTSECOFR
Limitazione responsabile riservatezza

QMAXSIGN
Numero massimo di tentativi di collegamento

QMAXSGNACN
Azione quando si supera il numero massimo di tentativi di collegamento

QRETSVRSEC
Conservazione sicurezza server

QRMTSIGN
Richieste di collegamento remoto

QSCANFS
Scansione file system

QSCANFSCTL
Scansione controllo file system

QSECURITY
Livello di sicurezza

QSHRMEMCTL
Controllo memoria condivisa

QUSEADPAUT
Utilizzare autorizzazione adottata

QVFYOBJRST
Verificare l'oggetto al ripristino

Consentire oggetti dominio utente (QALWUSRDMN)

A tutti gli oggetti viene assegnato un attributo dominio quando vengono creati. Un dominio è una caratteristica di un oggetto che controlla la modalità con cui i programmi possono accedere all'oggetto. Il valore di sistema Consenti oggetti dominio utente (QALWUSRDMN) specifica le librerie che possono contenere gli oggetti di dominio utente di tipo *USRSPC, *USRIDX e *USRQ.

I sistemi con elevati requisiti di sicurezza richiedono la limitazione degli oggetti *USRSPC, *USRIDX, *USRQ utente. Il sistema non è in grado di controllare il movimento delle informazioni verso e provenienti dagli oggetti del dominio utente. La limitazione non viene applicata agli oggetti dominio utente di tipo programma (*PGM), programma server (*SRVPGM) e pacchetti SQL (*SQLPKG).

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 6. Valori possibili per il valore di sistema QALWUSRDMN:

***ALL**	Gli oggetti del dominio utente possono essere contenuti in tutte le librerie e gli indirizzari sul sistema. Questo è il valore fornito.
***DIR**	Gli oggetti del dominio utente possono essere contenuti in tutti gli indirizzari sul sistema.
nome-libreria	I nomi di un massimo di 50 librerie che possono contenere gli oggetti del dominio utente di tipo *USRSPC, *USRIDX e *USRQ. Se vengono elencate le singole librerie, la libreria QTEMP *deve* essere inserita nell'elenco.

Valore consigliato: per la maggior parte dei sistemi, il valore consigliato è *ALL. Se il sistema dispone di un requisito elevato di sicurezza, è necessario consentire la presenza degli oggetti del dominio utente solo nella libreria QTEMP.

Alcuni sistema dispongono di software applicativi che si basano sui tipi di oggetto *USRSPC, *USRIDX o *USRQ. Per questi sistemi, l'elenco delle librerie per il valore di sistema QALWUSRDMN deve comprendere le librerie che vengono utilizzate dal software dell'applicazione. L'autorizzazione pubblica di ciascuna delle librerie posizionate in QALWUSRDMN, tranne che QTEMP, deve essere impostata su *EXCLUDE. Ciò limita il numero di utenti che possono utilizzare l'interfaccia MI per leggere o modificare i dati negli oggetti del dominio utente in queste librerie senza essere controllati.

Nota: se si esegue il comando RCLSTG (Riacqusizione memoria), gli oggetti del dominio utente potrebbero dover essere spostati dentro e fuori la libreria QRCL (riacquisizione memoria). Per eseguire il comando RCLSTG con esito positivo, potrebbe essere necessario aggiungere la libreria QRCL al valore di sistema QALWUSRDMN. Per proteggere la sicurezza del sistema, impostare l'autorizzazione pubblica per la libreria QRCL su *EXCLUDE. Rimuovere la libreria QRCL dal valore di sistema QALWUSRDMN una volta terminata l'esecuzione del comando RCLSTG.

Autorizzazione per i nuovi oggetti (QCRTAUT)

Il valore di sistema Autorizzazione per i nuovi oggetti (QCRTAUT) specifica l'autorizzazione pubblica per per un oggetto appena creato.

Il valore di sistema QCRTAUT viene utilizzato per stabilire l'autorizzazione pubblica per l'oggetto appena creato se vengono soddisfatte le seguenti condizioni:

- L'autorizzazione alla creazione (CRTAUT) per la libreria del nuovo oggetto viene impostato su *SYSVAL.
- Il nuovo oggetto viene creato con l'autorizzazione pubblica (AUT) di *LIBCRTAUT.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 7. Valori possibili per il valore di sistema QCRTAUT:

***CHANGE**	Gli utenti possono modificare gli oggetti appena creati.
***USE**	Gli utenti possono visualizzare, ma non modificare, gli oggetti gli oggetti appena creati.
***ALL**	Gli utenti possono eseguire tutte le funzioni sui nuovi oggetti.
***EXCLUDE**	L'utente non può utilizzare i nuovi oggetti.

Valori consigliati:
*CHANGE

Il valore di sistema QCRTAUT non viene utilizzato per gli oggetti creati negli indirizzari nel file system migliorato.

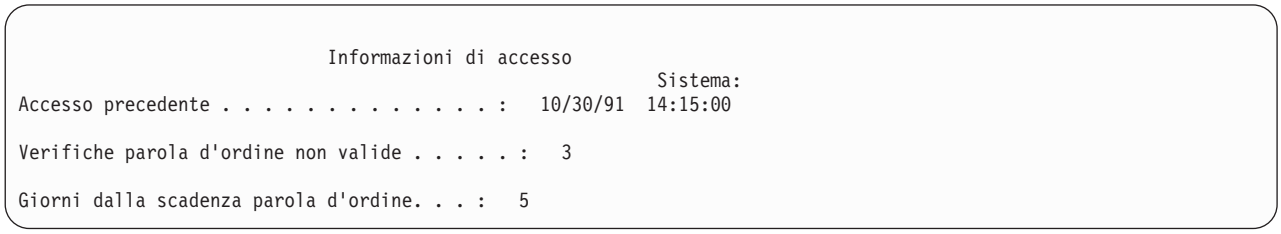
Attenzione: Diverse librerie fornite da IBM, compresa QSYS, dispongono di un valore CRTAUT *SYSVAL. Se si modifica il valore di sistema di QCRTAUT in un valore diverso da *CHANGE, è possibile riscontrare dei problemi durante il collegamento alle unità nuove o create automaticamente. Per impedire questi problemi durante la modifica del valore di sistema QCRTAUT in un valore diverso da *CHANGE, assicurarsi che tutte le descrizioni delle unità e le relative code messaggi associate dispongano di un'autorizzazione PUBLIC *CHANGE. Per far ciò, è necessario modificare il valore CRTAUT per la libreria QSYS in *CHANGE da *SYSVAL.

Visualizza informazioni di accesso (QDSPSGNINF)

Il valore di sistema Visualizza informazioni di accesso (QDSPSGNINF) determina se il pannello Informazioni di accesso viene visualizzato una volta effettuato l'accesso.

Il pannello Informazioni di accesso visualizza quanto segue:

- Data dell'ultimo accesso
- Qualsiasi verifica della parola d'ordine non valida
- Il numero di giorni dalla scadenza della parola d'ordine (se la parola d'ordine scade entro l'intervallo di avvertenza della scadenza della parola d'ordine (QPWDEXPWRN)))



Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 8. Valori possibili per il valore di sistema QDSPSGNINF:

0	Il pannello non viene visualizzato.
1	Viene visualizzato il pannello.

Valore consigliato: si consiglia 1 (Viene visualizzato il pannello) in modo tale che gli utenti possano controllare i tentativi di utilizzo dei rispettivi profili e sapere quando è necessaria una nuova parola d'ordine.

Nota: è possibile specificare la visualizzazione delle informazioni di accesso anche nei singoli profili utente.

Intervallo supero tempo lavoro inattivo (QINACTITV)

Il valore di sistema QINACTITV (Intervallo supero tempo lavoro inattivo) specifica, in minuti, per quanto tempo il sistema consente ad un lavoro di essere inattivo prima di eseguire un'azione.

Una stazione di lavoro viene considerata inattiva se si trova in stato di attesa di un pannello o di immissioni messaggi senza interazione dell'utente. Alcuni esempi di interazione utente sono:

- Utilizzo del tasto Invio

- Utilizzo della funzione di paginazione
- Utilizzo dei tasti funzione
- Utilizzo del tasto di aiuto

Le sessioni di emulazione tramite System i Access sono incluse. I lavori locali che vengono collegati ad un sistema remoto vengono esclusi. I lavori che vengono collegati dall'FTP (file transfer protocol) vengono esclusi. Per controllare il supero tempo delle connessioni FTP, modificare il parametro INACTTIMO sul comando Modifica attributo FTP (CHGFTPA). Per controllare il supero tempo delle sessioni telnet prima della V4R2, utilizzare il comando Modifica attributi telnet (CHGTELNA).

I seguenti esempi mostrano come il sistema determina i lavori inattivi:
- Un utente utilizza la funzione di richiesta del sistema per avviare un secondo lavoro interattivo. Un'interazione di sistema, come ad esempio il tasto Invio, sul lavoro fa in modo che entrambi i lavori vengano contrassegnati come attivi.
- Un lavoro System i Access può sembrare inattivo al sistema se l'utente sta eseguendo funzioni PC, come ad esempio la modifica di un documento, senza interagire con il sistema.

Il valore di sistema QINACTMSGQ determina l'azione eseguita dal sistema quando un lavoro inattivo supera l'intervallo specificato.

Una volta avviato il sistema, questo controlla i lavori inattivi all'intervallo specificato dal valore di sistema QINACTITV. Ad esempio, se il sistema viene avviato alle 9:46 del mattino e il valore di sistema QINACTITV indica 30 minuti, i lavori inattivi vengono controllati alle 10:16, 10:46, 11:16 e così via. Se si rileva un lavoro che è stato inattivo per 30 o più minuti, il sistema esegue l'azione specificata dal valore di sistema QINACTMSGQ. In questo esempio, se un lavoro diventa inattivo alle 10:17, non sarà disponibile fino alle 11:16. Al controllo delle 10:46, è risultato inattivo per soli 29 minuti.

I valori di sistema QINACTITV e QINACTMSGQ garantiscono la sicurezza impedendo agli utenti di abbandonare le stazioni di lavoro collegate. Una stazione di lavoro inattiva potrebbe permettere ad un utente autorizzato di accedere al sistema.

Tabella 9. Valori possibili per il valore di sistema QINACTITV:

***NONE:**	Il sistema non controlla i lavori inattivi.
intervallo-in-minuti	Specificare un valore compreso tra 5 e 300. Quando un lavoro è stato inattivo per quel numero di minuti, il sistema intraprende l'azione specificata in QINACTMSGQ.

Valore consigliato: 60 minuti

Coda messaggi supero tempo lavoro inattivo (QINACTMSGQ)

Il valore di sistema Coda messaggi supero tempo lavoro inattivo (QINACTMSGQ) specifica l'azione eseguita dal sistema quando si raggiunge l'intervallo di supero tempo di lavoro inattivo.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 10. Valori possibili per il valore di sistema QINACTMSGQ:

***ENDJOB**	Lavori inattivi terminati. Se il lavoro inattivo è un lavoro di gruppo,[1] vengono terminati anche tutti i lavori associati al gruppo. Se il lavoro è parte di un lavoro secondario, [1] entrambi i lavori vengono terminati. L'azione effettuata da *ENDJOB equivale ad eseguire il comando `ENDJOB JOB(nome) OPTION (*IMMED) ADLINTJOBS(*ALL)` sul lavoro inattivo.

Tabella 10. Valori possibili per il valore di sistema QINACTMSGQ: (Continua)

***DSCJOB**	Il lavoro inattivo viene scollegato, come i lavori secondari o di gruppo[1] ad esso associati. Il valore di sistema intervallo supero tempo lavoro scollegato (QDSCJOBITV) controlla se il sistema, alla fine, termina i lavori scollegati. Consultare "Intervallo di superotempo lavoro disconnesso (QDSCJOBITV)" a pagina 42 per ulteriori informazioni. **Attenzione:** il sistema non può scollegare alcuni lavori, come ad esempio PC Organizer e la funzione text-assist del PC (PCTA). Nel caso in cui il sistema non possa scollegare un lavoro inattivo, esso termina il lavoro.
nome-coda-messaggi	Il messaggio CPI1126 viene inviato alla coda messaggi specificata quando si raggiunge l'intervallo di supero tempo del lavoro inattivo. Questo messaggio afferma: `Il lavoro &3/&2/&1; non è stato attivo.` La coda messaggi deve esistere prima che possa essere specificata per il valore di sistema QINACTMSGQ. Questa coda messaggi viene ripulita automaticamente durante un IPL. Se si assegna QINACTMSGQ come coda messaggi dell'utente, tutti i messaggi nella coda messaggi dell'utente vengono persi durante l'IPL.
[1] L'argomento Work management descrive i lavori di gruppo e i lavori secondari.	

Valore consigliato: *DSCJOB è consigliato a meno che gli utenti non eseguano i lavori System i Access. L'utilizzo di *DSCJOB quando sono in esecuzione alcuni lavori System i Access equivale a terminare i lavori. Può causare la perdita significativa di informazioni. Utilizzare l'opzione *coda-messaggi* se si dispone del programma su licenza System i Access. L'argomento CL Programming mostra un esempio di scrittura di un programma per la gestione dei messaggi.

Utilizzo della coda: un utente o un programma può monitorare la coda messaggi ed eseguire l'azione necessaria, come ad esempio la chiusura del lavoro o l'invio di un messaggio di avvertenza all'utente. L'utilizzo della coda messaggi consente di prendere decisioni su unità particolari e profili utente, invece che trattare tutte le unità inattive nello stesso modo. Questo metodo è consigliato quando si utilizza il programma su licenza System i Access.

Se una stazione di lavoro con due lavori secondari è inattiva, due messaggi vengono inviati alla coda messaggi (uno per ogni lavoro secondario). Un utente o un programma può utilizzare il comando Fine lavoro (ENDJOB) per terminare uno o entrambi i lavori secondari. Se un lavoro inattivo dispone di uno o più lavori di gruppo, viene inviato un singolo messaggio alla coda messaggi. I messaggi continuano ad essere inviato alla coda messaggi per ciascun intervallo durante il quale il lavoro non è attivo.

Limite sessioni unità (QLMTDEVSSN)

Il valore di sistema Limite sessioni unità (QLMTDEVSSN) specifica se il numero di sessioni unità consentite a un utente è limitato.

Questo valore non limita il menu Richiesta sistema o un secondo collegamento dalla stessa unità. Se un utente dispone di un lavoro scollegato, l'utente può collegarsi al sistema con una nuova sessione unità.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 11. Valori possibili per il valore di sistema QLMTDEVSSN:

0	L'utente non è limitato a un numero specifico di sessioni unità.
1	L'utente è limitato a una singola sessione unità.

Tabella 11. Valori possibili per il valore di sistema QLMTDEVSSN: (Continua)

2 - 9	L'utente è limitato al numero specificato di sessioni unità.

Valore consigliato: 1 (Sì) è consigliato poiché limitando gli utenti ad una singola unità si riduce la probabilità di condividere le parole d'ordine e di lasciare le unità non presidiate.

Nota: la limitazione delle sessioni di unità può essere specificata anche nei singoli profili utente.

Limitazione responsabile della riservatezza (QLMTSECOFR)

Il valore di sistema Limitazione responsabile della riservatezza (QLMTSECOFR) controlla se un utente con l'autorizzazione speciale a tutti gli oggetti (*ALLOBJ) o al servizio (*SERVICE) può accedere ad una qualsiasi stazione di lavoro. Limitare i profili utente potenti a determinate stazioni di controllo ben controllate fornisce la protezione della sicurezza.

Il valore di sistema QLMTSECOFR viene rinforzato solo al livello di sicurezza 30 e ai livelli superiori. "Stazioni di lavoro" a pagina 215 fornisce ulteriori informazioni sull'autorizzazione richiesta per collegarsi ad una stazione di lavoro.

L'utente può collegarsi alla console in qualsiasi momento con i profili QSECOFR, QSRV e QSRVBAS, senza preoccuparsi dell'impostazione del valore QLMTSECOFR.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 12. Valori possibili per il valore di sistema QLMTSECOFR:

1	Un utente con l'autorizzazione speciale *ALLOBJ o *SERVICE può collegarsi ad una stazione di lavoro solo se è stato specificatamente autorizzato (vale a dire, se dispone dell'autorizzazione *CHANGE) alla stazione di lavoro o se il profilo utente QSECOFR è stato autorizzato (con autorizzazione *CHANGE) alla stazione di lavoro. Questa autorizzazione non può provenire dall'autorizzazione pubblica.
0	Gli utenti con l'autorizzazione speciale *ALLOBJ o *SERVICE possono collegarsi ad ogni stazione di lavoro per la quale dispongono dell'autorizzazione *CHANGE. Possono ricevere l'autorizzazione *CHANGE mediante l'autorizzazione privata o pubblica oppure perché dispongono dell'autorizzazione speciale*ALLOBJ.

Valore consigliato: 1 (Sì)

Numero massimo di tentativi di accesso (QMAXSIGN)

Il valore di sistema Numero massimo di tentativi di accesso (QMAXSIGN) controlla il numero di tentativi consecutivi di accesso o di verifica della parola d'ordine non validi, effettuati da utenti locali e remoti.

I tentativi di accesso o di verifica parola d'ordine non corretti possono essere causati da un ID utente non corretto, da una parola d'ordine non corretta o da un'autorizzazione non appropriata per l'utilizzo della stazione di lavoro.

Una volta raggiunto il numero massimo di tentativi di accesso o di verifica parola d'ordine, il valore di sistema QMAXSGNACN viene utilizzato per stabilire l'azione da eseguire. Un messaggio CPF1393 viene inviato alla coda messaggi QSYSOPR (e alla coda messaggi QSYSMSG se esistente nella libreria QSYS) per informare il responsabile della riservatezza di una possibile intrusione.

Se si crea la coda messaggi QSYSMSG nella libreria QSYS, i messaggi sugli eventi di sistema critici vengono inviati a quella coda messaggi e alla coda QSYSOPR. La coda messaggi QSYSMSG può essere controllata separatamente da un programma o da un operatore di sistema. Ciò fornisce una protezione ulteriore delle risorse di sistema. I messaggi critici del sistema in QSYSOPR vengono alcune volte saltati a causa del volume dei messaggi inviati a quella coda messaggi.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 13. Valori possibili per il valore di sistema QMAXSIGN:

3	Un utente può eseguire al massimo 3 tentativi di accesso o di verifica parola d'ordine.
***NOMAX**	Il sistema consente un numero illimitato di tentativi di accesso o di verifica parola d'ordine non corretti. Questa impostazione consente ad un possibile intruso un numero illimitato di possibilità di indovinare una combinazione ID utente e parola d'ordine valida.
limite	Specificare un valore compreso tra 1 e 25. Il numero consigliato di tentativi di accesso o di verifica parola d'ordine è tre. In genere tre tentativi sono sufficienti per correggere gli errori di battitura, tuttavia è un numero abbastanza ridotto per impedire l'accesso non autorizzato.

Valore consigliato: 3

Operazione quando si raggiunge il numero massimo di tentativi di collegamento (QMAXSGNACN)

Il valore di sistema QMAXSGNACN (Operazione quando si raggiunge il numero massimo di tentativi di collegamento) stabilisce come il sistema deve procedere quando si raggiunge il numero massimo di tentativi di verifica di collegamento o parola d'ordine su una stazione di lavoro.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 14. Valori possibili per il valore di sistema QMAXSGNACN:

3	Disabilitare sia il profilo utente che l'unità.
1	Disabilitare solo l'unità.
2	Disabilitare solo il profilo utente.

Il sistema disabilita un'unità disattivandola. L'unità viene disabilitata solo se i tentativi di collegamento non validi sono consecutivi sulla stessa unità. Un collegamento valido reimposta il conteggio dei tentativi di collegamento non validi per l'unità.

Il sistema disabilita un profilo utente modificando il parametro *Stato* su *DISABLED. Il profilo utente viene disabilitato quando il numero di tentativi di collegamento non validi eseguiti dall'utente raggiunte il valore specificato nel valore di sistema QMAXSIGN, senza considerare se i tentativi di collegamento non validi provengono dalla stessa unità o da unità diverse. Una verifica parola d'ordine o o collegamento valida reimposta il conteggio dei tentativi di collegamento non validi nel profilo utente.

Se si crea la coda messaggi QSYSMSG in QSYS, il messaggio inviato (CPF1397) contiene il nome dell'utente e dell'unità. Per questo motivo, è possibile controllare la disabilitazione dell'unità in base all'unità utilizzata.

"Numero massimo di tentativi di accesso (QMAXSIGN)" a pagina 32 fornisce ulteriori informazioni sulla coda messaggi QSYSMSG.

Se il profilo QSECOFR viene disabilitato, è possibile collegarsi come QSECOFR alla console e abilitare il profilo. Se la console viene disattivata e nessun altro utente può attivarla, è necessario eseguire l'IPL del sistema per rendere disponibile la console.

Valore consigliato: 3

Conservazione sicurezza server (QRETSVRSEC)

Il valore di sistema Conservazione sicurezza server (QRETSVRSEC) determina se le informazioni di autenticazione decodificabili associate ai profili utente o alle voci dell'elenco di convalida (*VLDL) possono essere conservate sul sistema host. Tale impostazione non comprende la parola d'ordine del profilo utente System i.

Se si modifica il valore da 1 a 0, il sistema disabilita l'accesso alle informazioni di autenticazione. Se si riporta il valore su 1, il sistema riabilita l'accesso alle informazioni di autenticazione.

Le informazioni di autenticazione possono essere eliminate dal sistema impostando su 0 il valore di sistema QRETSVRSEC ed eseguendo il comando CLRSVRSEC (Eliminazione dati sicurezza server). In caso di un numero elevato di profili utente o elenchi di convalida sul sistema, è possibile che l'esecuzione del comando CLRSVRSEC richieda un lungo periodo di tempo.

Il campo di dati codificati di una voce dell'elenco di convalida viene solitamente utilizzato per memorizzare le informazioni di autenticazione. Le applicazioni specificano se memorizzare i dati codificati in un modulo codificabile o non codificabile. Se le applicazioni scelgono un modulo codificabile e il valore QRETSVRSEC è stato modificato da 1 a 0, le informazioni sul campo dei dati codificati non sono accessibili dalla voce. Se il campo dei dati codificati di una voce dell'elenco di convalida viene memorizzato in un modulo non codificabile, questo non viene coinvolto dal valore di sistema QRETSVRSEC.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 15. Valori possibili per il valore di sistema QRETSVRSEC:

0	I dati della sicurezza server non vengono conservati.
1	I dati della sicurezza server vengono conservati.

Valore consigliato: 0

Concetti correlati

"Utilizzo elenchi di convalida" a pagina 261
Gli oggetti dell'elenco di convalida forniscono alle applicazioni un metodo per memorizzare in modo sicuro le informazioni di autenticazione utente.

Accensione e riavvio remoti (QRMTIPL)

Una parte del piano di sicurezza del sistema consiste nel determinare se consentire agli utenti di accendere e riavviare il sistema. Il valore di sistema Accensione e riavvio remoti (QRMTIPL) consente di avviare il sistema remoto utilizzando il telefono ed un modem o il segnale SPCN.

Quando QRMTIPL è impostato su 1 (Sì), qualsiasi chiamata telefonica prova il riavvio del sistema. Anche se il valore di sistema è relativo alle opzioni di riavvio del sistema, ha delle implicazioni per sicurezza.

Ovviamente non si desidera che i sistemi vengano riavviati inavvertitamente da un utente. Tuttavia, se si utilizza un sistema remoto per gestire il sistema è necessario consentire il riavvio remoto.

Tabella 16. Valori possibili per il valore di sistema Accensione e riavvio remoti (QRMTIPL)

0	Non consentire accensione e riavvio remoti
1	Abilitazione accensione e riavvio remoti

Informazioni correlate

Valori di sistema Riavvio: Consentire accensione e riavvio remoti

Controllo accesso remoto (QRMTSIGN)

Il valore di sistema Controllo accesso remoto (QRMTSIGN) specifica come il sistema gestisce le richieste di accesso remoto.

Esempi di accesso remoto sono il pass-through della stazione video da un altro sistema, la funzione di stazione di lavoro del programma su licenza System i e l'accesso TELNET.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 17. Valori possibili per il valore di sistema QRMTSIGN:

***FRCSIGNON**	Le richieste di accesso remoto devono seguire la normale procedura di accesso.
***SAMEPRF**	Quando i nomi dei profili utente origine e di destinazione corrispondono, è possibile che il pannello di accesso venga saltato in caso di richiesta di accesso automatico. La verifica della parola d'ordine ha luogo prima dell'utilizzo del programma pass-through di destinazione. Se una parola d'ordine non valida viene inviata durante un tentativo di accesso automatico, la sessione di pass-through viene terminata e un messaggio di errore viene inviato all'utente. Tuttavia, se i nomi dei profili differiscono, *SAMEPRF indica che la sessione viene terminata con un errore di sicurezza anche se l'utente ha immesso una parola d'ordine valida per il profilo utente remoto. Il pannello di accesso viene visualizzato per i tentativi di pass-through che non richiedono l'accesso automatico.
***VERIFY**	Il valore *VERIFY consente di saltare il pannello di accesso del sistema di destinazione se, insieme alla richiesta di accesso automatico, vengono inviate delle informazioni di sicurezza valide. Se la parola d'ordine non è valida per il profilo utente di destinazione specificato, la sessione pass-through termina con un errore di sicurezza. Se il sistema di destinazione dispone di un valore QSECURITY pari a 10, vengono abilitate tutte le richieste di accesso automatico. Il pannello di accesso viene visualizzato per i tentativi di pass-through che non richiedono l'accesso automatico.
***REJECT**	Nessun accesso remoto autorizzato.
	Per l'accesso TELNET, non è necessario eseguire alcuna operazione per *REJECT.
nome-programma nome-libreria	Il programma specificato viene eseguito all'inizio e alla fine di ogni sessione pass-through.

Valore consigliato: *REJECT è consigliato se non si desidera consentire gli accessi pass-through o System i Access. Se si desidera consentire l'accesso pass-through o System i Access, utilizzare *FRCSIGNON o *SAMEPRF.

Il manuale Remote Workstation Support  contiene informazioni dettagliate sul valore di sistema QRMTSIGN. Inoltre contiene i requisiti per un programma di accesso remoto e un esempio.

Scansione file system (QSCANFS)

Il valore di sistema Scansione file system (QSCANFS) consente di selezionare l'opzione per specificare l'IFS (Integrated File System) in cui gli oggetti verranno scansionati.

Ad esempio, è possibile utilizzare questa opzione per eseguire la scansione per un virus. La scansione dell'IFS (Integrated file system) viene abilitata quando i programmi di uscita vengono registrati con uno qualsiasi dei punti di uscita relativi alla scansione dell'IFS (integrated file system). Il valore di sistema QSCANFS specifica l'IFS in cui gli oggetti verranno scansionati quando si registrano i programmi di uscita con uno qualsiasi dei punti di uscita relativi alla scansione dell'IFS (integrated file system).

I punti di uscita relativi alla scansione dell'IFS sono:

- QIBM_QP0L_SCAN_OPEN — Scansione IFS (Integrated file system) su uscita aperta.
- QIBM_QP0L_SCAN_CLOSE — Scansione IFS (Integrated file system) su uscita chiusa.

Per ulteriori informazioni sugli IFS (integrated file system), consultare l'argomento Integrated file system.

Tabella 18. Valori possibili per il valore di sistema QSCANFS:

***NONE**	Nessun oggetto IFS verrà scansionato.
***ROOTOPNUD**	Gli oggetti di tipo *STMF contenuti negli indirizzari *TYPE2 nei file system "root" (/), QOpenSys e negli UDFS (user-defined file system) verranno scansionati.

Valore consigliato: il valore consigliato è *ROOTOPNUD in modo tale che i file system "root" (/), QOpenSys e UDFS (user-defined file system) vengano scansionati quando gli utenti registrano i programmi di uscita con i punti di uscita relativi alla scansione dell'IFS (Integrated File System).

Riferimenti correlati

"Scansione controllo file system (QSCANFSCTL)"
Il valore di sistema Scansione controllo file system (QSCANFSCTL) controlla la scansione dell'IFS (Integrated File System) abilitato quando i programmi di uscita vengono registrati con uno qualsiasi dei punti di uscita relativi alla scansione dell'IFS (Integrated File System).

Informazioni correlate

*TYPE2 directories

Scansione controllo file system (QSCANFSCTL)

Il valore di sistema Scansione controllo file system (QSCANFSCTL) controlla la scansione dell'IFS (Integrated File System) abilitato quando i programmi di uscita vengono registrati con uno qualsiasi dei punti di uscita relativi alla scansione dell'IFS (Integrated File System).

QSCANFSCTL gestisce il valore di sistema di scansione file system per fornire controlli granulari sulla modalità e gli elementi sottoposti a scansione nel IFS (integrated file system). È possibile selezionare differenti opzioni di scansione o scegliere di utilizzare le opzioni di scansione predefinite. Inoltre, è possibile selezionare diverse opzioni di scansione che controllano la modalità e gli oggetti sottoposti a scansione dai programmi di uscita registrati. Queste opzioni sono descritte nella seguente tabella:

Tabella 19. Valori possibili per il valore di sistema QSCANFSCTL:

***NONE**	Nessun controllo specificato per i punti di uscita relativi alla scansione dell'IFS.

Tabella 19. Valori possibili per il valore di sistema QSCANFSCTL: (Continua)

***ERRFAIL**	In caso di errore durante il richiamo del programma di uscita (ad esempio, quando non si trova il programma o quando il programma di uscita segnala un errore), il sistema non riuscirà ad eseguire la richiesta che ha eseguito il trigger sulla chiamata del programma di uscita. Se questo valore non viene specificato, il sistema salterà il programma di uscita e lo tratterà come se l'oggetto non fosse stato scansionato.
***FSVRONLY**	Verranno scansionati solo gli accessi mediante i server file. Ad esempio, verranno scansionati gli accessi mediante NFS (Network File System) e altri metodi del server file. Qualora non fosse specificato, verranno scansionati tutti gli accessi.
***NOFAILCLO**	Il sistema non riporterà errori durante le richieste di chiusura con un'indicazione di errore della scansione, anche se l'oggetto non è riuscito ad eseguire una scansione che era stata eseguita come parte del processo di chiusura. Inoltre, questo valore sovrascriverà la specifica *ERRFAIL per il processo di chiusura ma non per gli altri punti di uscita relativi alla scansione.
***NOPOSTRST**	Una volta ripristinati gli oggetti, questi non verranno scansionati proprio perché sono stati ripristinati. Se l'attributo dell'oggetto è ″l'oggetto non verrà sottoposto a scansione″, l'oggetto non verrà mai scansionato. Se l'attributo dell'oggetto è ″l'oggetto verrà sottoposto a scansione solo se è stato modificato dall'ultima scansione″, l'oggetto verrà scansionato solo se è stato modificato dopo il ripristino. Se non è specificato *NOPOSTRST, gli oggetti verranno scansionati almeno una volta dopo il ripristino. Se l'attributo dell'oggetto è ″l'oggetto non verrà sottoposto a scansione″, l'oggetto verrà scansionato una volta dopo il ripristino. Se l'attributo dell'oggetto è ″l'oggetto verrà sottoposto a scansione solo se è stato modificato dall'ultima scansione″, l'oggetto verrà scansionato dopo il ripristino poiché il ripristino verrà trattato come una modifica all'oggetto. In generale, potrebbe risultare rischioso ripristinare gli oggetti senza scansionarli almeno una volta. Si consiglia di utilizzare questa opzione solo quando si è certi che gli oggetti sono stati scansionati prima del loro salvataggio o che provengono da un'origine affidabile.
***NOWRTUPG**	Il sistema non tenterà di aggiornare l'accesso per il descrittore scansione inviato al programma di uscita per includere l'accesso alla scrittura. Qualora non fosse specificato, il sistema tenterà di eseguire l'aggiornamento all'accesso alla scrittura.
***USEOCOATR**	Il sistema utilizzerà la specifica dell'attributo ″modifica solo oggetto″ per scansionare l'oggetto solo se è stato modificato (non perché il software di scansione ha indicato un aggiornamento). Qualora non fosse specificato, l'attributo ″modifica solo oggetto″ non verrà utilizzato e l'oggetto verrà scansionato una volta modificato e quando il software di scansione indica un aggiornamento.

Valore consigliato: se si desidera specificare i valori più restrittivi per la scansione IFS (integrated file system), le impostazioni consigliate sono *ERRFAIL e *NOWRTUPG. Ciò garantisce che gli errori restituiti dai programmi di uscita di scansione impediscano le operazioni associate e non forniscano al programma di uscita livelli di accesso aggiuntivi. Tuttavia, il valore *NONE rappresenta la scelta ideale per la maggior parte degli utenti. Quando si installa il codice fornito da un'origine affidabile, si consiglia di specificare il valore *NOPOSTRST per il periodo di tempo necessario per l'installazione.

Riferimenti correlati

"Scansione file system (QSCANFS)" a pagina 36
Il valore di sistema Scansione file system (QSCANFS) consente di selezionare l'opzione per specificare l'IFS (Integrated File System) in cui gli oggetti verranno scansionati.

Controllo memoria condivisa (QSHRMEMCTL)

Il valore di sistema Controllo memoria condivisa (QSHRMEMCTL) definisce gli utenti che possono utilizzare la memoria condivisa o connessa con capacità di scrittura.

È possibile che l'ambiente contenga delle applicazioni, che eseguono ciascuna lavori differenti, ma che condividono puntatori. L'utilizzo di queste API fornisce migliori prestazioni delle applicazioni e ne semplifica lo sviluppo consentendo memoria condivisa e file di flusso tra queste differenti applicazioni e i lavori. Tuttavia, l'utilizzo di queste API potrebbe potenzialmente costituire un rischio per il sistema e le risorse. Un programmatore può avere accesso alla scrittura ed essere in grado di aggiungere, modificare e cancellare le voci nella memoria condivisa o nel file di flusso.

Per modificare questo valore di sistema, gli utenti devono disporre delle autorizzazioni speciali *ALLOBJ e *SECADM. La modifica apportata a questo valore di sistema viene applicata immediatamente.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 20. Valori possibili per il valore di sistema QSHRMEMCTL:

0	Gli utenti non possono utilizzare la memoria condivisa o la memoria collegata con funzione di scrittura. Questo valore indica che gli utenti non possono utilizzare le API di memoria condivisa (ad esempio, l'API shmat() — Shared Memory Attach) e non possono utilizzare gli oggetti di memoria collegata con funzione di scrittura (ad esempio, l'API mmap() — Memory Map a File fornisce questa funzione). Utilizzare questo valore negli ambienti con requisiti di sicurezza elevati.
1	Gli utenti possono utilizzare la memoria condivisa o la memoria collegata con funzione di scrittura. Questo valore indica che gli utenti possono utilizzare le API di memoria condivisa (ad esempio l'API shmat() — Shared Memory Attach) e possono utilizzare gli oggetti di memoria collegata con funzione di scrittura (ad esempio l'API mmap() — Memory Map a File fornisce questa funzione).

Valore consigliato: 1

Utilizzo autorizzazione adottata (QUSEADPAUT)

Il valore di sistema Utilizzo autorizzazione adottata (QUSEADPAUT) definisce gli utenti che possono creare i programmi con l'attributo di utilizzo autorizzazione adottata (*USEADPAUT(*YES)).

Tutti gli utenti autorizzati dal valore di sistema QUSEADPAUT possono creare o modificare i programmi e i programmi di servizio in modo da utilizzare l'autorizzazione adottata se l'utente dispone dell'autorizzazione necessaria per il programma o il programma di servizio.

Il valore di sistema può contenere il nome di un elenco di autorizzazioni. L'autorizzazione dell'utente viene controllata nell'elenco. Se l'utente dispone almeno dell'autorizzazione *USE per l'elenco di autorizzazioni specificato, tale utente può creare, modificare o aggiornare i programmi o i programmi di servizio con l'attributo USEADPAUT(*YES). L'autorizzazione all'elenco di autorizzazioni non può provenire da un'autorizzazione adottata.

Se un elenco di autorizzazioni viene specificato nel valore di sistema e l'elenco di autorizzazioni non è presente, la funzione che si è tentato di eseguire non verrà completata. Viene inviato un messaggio che spiega tale situazione.

Tuttavia, se il programma viene creato con la API QPRCRTPG e viene specificato il valore *NOADPAUT nella mascherina dell'opzione, il programma viene creato con esito positivo anche se l'elenco di autorizzazioni non esiste.

Se viene richiesta una o più funzioni sul comando o sulla API e l'elenco di autorizzazioni non è presente, la funzione non viene eseguita.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 21. Valori possibili per il valore di sistema QUSEADPAUT:

autorizzazione nome elenco	Viene segnalato un messaggio di diagnostica per indicare che il programma viene creato con USEADPAUT(*NO) se tutte le seguenti condizioni sono vere: • L'utente non dispone dell'autorizzazione per accedere all'elenco di autorizzazioni specificato. • Non si sono verificati altri errori durante la creazione del programma o del programma di servizio.
***NONE**[1]	Tutti gli utenti possono creare, modificare o aggiornare programmi e programmi di servizio al fine di utilizzare l'autorizzazione del programma che li ha richiamati nel caso in cui l'utente disponga dell'autorizzazione necessaria al programma o al programma di servizio.
[1] *NONE indica che non viene utilizzato alcun elenco di autorizzazioni e per impostazione predefinita a tutti gli utenti verrà consentito l'accesso ai programmi che utilizzano l'autorizzazione adottata.	

Valore consigliato: per le macchine di produzione, creare un elenco di autorizzazioni con l'autorizzazione *PUBLIC(*EXCLUDE). Specificare questo elenco di autorizzazioni per il valore di sistema QUSEADPAUT. Ciò impedisce che chiunque possa creare programmi che utilizzando l'autorizzazione adottata.

L'utente deve prestare molta attenzione alla sicurezza dell'applicazione prima di creare l'elenco di autorizzazioni per il valore di sistema QUSEADPAUT. Tale indicazione si rivela estremamente importante negli ambienti di sviluppo delle applicazioni.

Valori di sistema relativi alla sicurezza

Questo argomento descrive i valori di sistema relativi alla sicurezza sul sistema operativo i5/OS.

Panoramica:

Scopo: specificare i valori di sistema relativi alla sicurezza sul sistema.

Modalità:
WRKSYSVAL (Comando Gestione valore di sistema)

Autorizzazione:
*ALLOBJ e *SECADM

Voce di giornale:
SV

Nota: Le modifiche diventano effettive immediatamente. IPL non richiesto.

Le seguenti informazioni sono descrizioni di altri valori di sistema relativi alla sicurezza sul sistema. Questi valori di sistema non vengono inseriti nel gruppo *SEC sul pannello Gestione valore di sistema.

QAUTOCFG
Configurazione automatica dell'unità

QAUTOVRT
Configurazione automatica delle unità virtuali

QDEVRCYACN
Azione di ripristino dell'unità

QDSCJOBITV
Intervallo supero tempo lavoro scollegato

Nota: questo valore di sistema viene trattato anche nell'argomento Valori di sistema Lavori: Intervallo di superotempo per i lavori disconnessi.

QRMTSRVATR
Attributo servizio remoto

QSSLCSL
Elenco specifiche codifica SSL (Secure Sockets Layer)

QSSLCSLCTL
Controllo codifica SSL (Secure Sockets Layer)

QSSLPCL
Protocolli SSL (Secure Sockets Layer)

Concetti correlati

"Convalida dei programmi in fase di ripristino" a pagina 18
Quando viene creato un programma, il sistema calcola un valore di convalida, che viene memorizzato con il programma. Quando il programma viene ripristinato, il valore di convalida viene calcolato di nuovo e confrontato con il valore di convalida memorizzato con il programma.

Configurazione automatica dell'unità (QAUTOCFG)

Il valore di sistema Configurazione automatica dell'unità (QAUTOCFG) configura automaticamente le unità collegate in locale. Il valore specifica se le unità aggiunte al sistema vengono configurate automaticamente.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 22. Valori possibili per il valore di sistema QAUTOCFG:

0	Configurazione automatica disattivata. L'utente deve configurare manualmente le unità o i programmi di controllo locali nuovi aggiunti al sistema.
1	Configurazione automatica attivata. Il sistema configura automaticamente le unità o i programmi di controllo locali nuovi aggiunti al sistema. L'operatore riceve un messaggio che specifica le modifiche apportate alla configurazione del sistema.

Valore consigliato: quando si inizializza l'impostazione di un sistema o quando si aggiunge un numero considerevole di nuove unità, il valore di sistema deve essere impostato su 1. Per tutte le altre operazioni, il valore di sistema deve essere impostato su 0.

Configurazione automatica delle unità virtuali (QAUTOVRT)

Il valore di sistema Configurazione automatica delle unità virtuali (QAUTOVRT) specifica se se le unità virtuali pass-throug e le unità virtuali a schermo intero TELNET (in contrapposizione all'unità virtuale della funzione della stazione di lavoro) vengono configurate automaticamente.

Un'*unità virtuale* rappresenta la descrizione di un'unità che non dispone di un hardware associato. Viene utilizzata per stabilire una connessione tra un utente e una stazione di lavoro fisica collegata ad un sistema remoto.

Consentendo al sistema di configurare automaticamente le unità virtuali si facilita la connessione degli utenti al sistema mediante il pass-through o il telnet. Senza la configurazione automatica, un utente che tenta di entrare ha un numero limitato di tentativi per ciascuna unità virtuale. Il limite viene stabilito dal responsabile della riservatezza utilizzando il valore di sistema QMAXSIGN. Con la configurazione automatica attivata, il limite reale è più alto. Il limite di collegamento al sistema viene moltiplicato per il numero di unità virtuali che possono essere create dal supporto di configurazione automatica. Questo supporto viene definito dal valore di sistema QAUTOVRT.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 23. Valori possibili per il valore di sistema QAUTOVRT:

0	Nessuna unità virtuale viene creata automaticamente.
numbero-di- unità- virtuali	Specificare un valore compreso tra 1 e 9999. Se un numero di unità inferiore a quello specificato viene collegato a un programma di controllo virtuale e nessuna unità è disponibile nel momento in cui un utente tenta un pass-through o un TELNET a schermo intero, il sistema configura una nuova unità.

valore consigliato: 0

Informazioni correlate

Remote Workstation Support

Impostazione TCP/IP

Azione di ripristino dell'unità (QDEVRCYACN)

Il valore di sistema QDEVRCYACN (Device Recovery Action) specifica quale azione intraprendere quando si verifica un errore I/E in una stazione di lavoro di un lavoro interattivo.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 24. Valori possibili per il valore di sistema QDEVRCYACN:

***DSCMSG**	Scollega il lavoro. Quando ci si collega nuovamente, un messaggio di errore viene inviato al programma dell'applicazione dell'utente.
***MSG**	Segnala il messaggio di errore I/O al programma dell'applicazione dell'utente. Il programma dell'applicazione eseguire il ripristino dell'errore.
***DSCENDRQS**	Scollega il lavoro. Quando ci si collega nuovamente, viene eseguita una funzione di cancellazione della richiesta per riportare il controllo del lavoro all'ultimo livello di richiesta.
***ENDJOB**	Termina il lavoro. Viene creata la registrazione di un lavoro per il lavoro stesso. Un messaggio che specifica l'avvenuta chiusura del lavoro a causa di un errore nell'unità viene inviato alla registrazione del lavoro e alla registrazione QHST. Per ridurre l'effetto sulle prestazioni causato dalla chiusura del lavoro, la priorità del lavoro viene ridotta di 10, il lasso di tempo viene impostato su 100 millisecondi e l'attributo relativo all'eliminazione viene impostato su Sì.

Tabella 24. Valori possibili per il valore di sistema QDEVRCYACN: (Continua)

***ENDJOBNOLIST**	Termina il lavoro. Non viene creata la registrazione di un lavoro per il lavoro stesso. Un messaggio che specifica l'avvenuta chiusura del lavoro a causa di un errore nell'unità viene inviato alla registrazione QHST.

Quando si specifica un valore *MSG o *DSCMSG, l'azione di ripristino dell' unità non viene eseguita fino a quando il lavoro non esegue la successiva operazione I/E. In un ambiente LAN/WAN, ciò potrebbe permettere lo scollegamento di un'unità e il collegamento di un'altra, utilizzando lo stesso indirizzo, prima che si verifichi la successiva operazione di I/E per il lavoro. Il lavoro può essere ripristinato dal messaggio di errore I/E e continuare l'esecuzione sulla seconda unità. Per evitare ciò, è necessario specificare un'azione di ripristino dell'unità *DSCENDRQS, *ENDJOB o *ENDJOBNOLIST. Queste azioni di ripristino delle unità vengono eseguite immediatamente quando si verifica un errore I/E, come ad esempio in caso spegnimento.

Valore consigliato: *DSCMSG

Nota: le autorizzazioni speciali *ALLOBJ e *SECADM non sono richieste per la modifica di questo valore.

Intervallo di superotempo lavoro disconnesso (QDSCJOBITV)

Il valore di sistema Intervallo di superotempo per i lavori disconnessi (QDSCJOBITV) determina se e quando il sistema termina un lavoro disconnesso. L'intervallo è specificato in minuti.

Se si imposta il valore di sistema QINACTMSGQ per disconnettere i lavori inattivi (*DSCJOB), alla fine è necessario impostare QDSCJOBITV per terminare i lavori disconnessi. Un lavoro disconnesso utilizza risorse di sistema e conserva tutti i blocchi sugli oggetti.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 25. Valori possibili per il valore di sistema QDSCJOBITV:

240	Il sistema termina un lavoro scollegato dopo 240 minuti.
***NONE**	Il sistema non termina automaticamente un lavoro scollegato.
tempo-in-minuti	Specificare un valore compreso tra 5 e 1440.

valore consigliato: 120

Attributo servizio remoto (QRMTSRVATR)

Attributo servizio remoto (QRMTSRVATR) controlla la capacità di analisi dei problemi del servizio del sistema remoto. Il valore consente al sistema di essere analizzato in remoto.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

I valori abilitati per il valore di sistema QRMTSRVATR sono:

Tabella 26. Valori possibili per il valore di sistema QRMTSRVATR:

0	Attributo servizio remoto disattivato.
1	Attributo servizio remoto attivato.

Valore consigliato: 0

Concetti correlati

"Sicurezza blocco a chiave" a pagina 2
È possibile richiamare e modificare la posizione del blocco a chiave tramite l'API QWCRIPLA (Richiamo attributi IPL) o il comando CHGIPLA (Modifica attributi IPL).

Elenco specifiche codifica SSL (Secure Sockets Layer) (QSSLCSL)

Il valore di sistema Elenco specifiche codifica SSL (Secure Sockets Layer) (QSSLCSL) determina l'elenco di specifiche di codifica supportato dall'SSL di sistema.

L'SSL di sistema specifica la sequenza dei valori in QSSLCSL per ordinare l'elenco di specifiche di codifica predefinito dell'SSL di sistema. Le voci dell'elenco di specifiche di codifica predefinito sono definite dal sistema e possono variare in base ai limiti del release. Se una suite di codifica predefinita viene rimossa dal valore di sistema QSSLCSL, essa viene rimossa anche dall'elenco di specifiche di codifica. La suite di codifica predefinita viene aggiunta nuovamente all'elenco predefinito delle specifiche di codifica quando la codifica viene aggiunta nuovamente nel valore di sistema QSSLCSL. Non è possibile aggiungere altre suite di codifica all'elenco di specifiche di codifica predefinito oltre la serie definita dal sistema per il release. Inoltre, non è possibile aggiungere una suite di codifica a QSSLCSL se il valore di protocollo SSL richiesto per la suite di codifica non è impostato per il valore di sistema QSSLPCL (Elenco protocolli SSL).

I valori del valore di sistema QSSLCSL sono di sola lettura a meno che il valore di sistema Controllo codifica SSL (QSSLCSLCTL) non sia impostato su *USRDFN.

I valori consentiti per il valore di sistema QSSLCSL sono i seguenti:

- *RSA_AES_128_CBC_SHA
- *RSA_RC4_128_SHA
- *RSA_RC4_128_MD5
- *RSA_AES_256_CBC_SHA
- *RSA_3DES_EDE_CBC_SHA
- *RSA_DES_CBC_SHA
- *RSA_EXPORT_RC4_40_MD5
- *RSA_EXPORT_RC2_CBC_40_MD5
- *RSA_NULL_SHA
- *RSA_NULL_MD5
- *RSA_RC2_CBC_128_MD5
- *RSA_3DES_EDE_CBC_MD5
- *RSA_DES_CBC_MD5

Nota: l'utente deve disporre delle autorizzazioni speciali *IOSYSCFG, *ALLOBJ e *SECADM per modificare questo valore di sistema.

È possibile fare riferimento all'argomento Elenco specifiche codifica SSL (Secure Sockets Layer) nella raccolta di argomenti Valori di sistema per ulteriori informazioni sui valori forniti.

Informazioni correlate

Valori di sistema Sicurezza: Elenco specifiche codifica SSL (Secure Sockets Layer)

System SSL Properties

Controllo codifica SSL (Secure Sockets Layer)(QSSLCSLCTL)

Il valore di sistema Controllo codifica SSL (Secure Sockets Layer)(QSSLCSLCTL) specifica se il sistema o l'utente controlla il valore di sistema Elenco specifiche codifica SSL (Secure Sockets Layer) (QSSLCSL).

I valori consentiti per il valore di sistema QSSLCSLCTL sono i seguenti:

- *OPSYS
- *USRDFN

Nota: l'utente deve disporre delle autorizzazioni speciali *IOSYSCFG, *ALLOBJ e *SECADM per modificare questo valore di sistema.

È possibile fare riferimento all'argomento Controllo codifica SSL (Secure Sockets Layer) nella raccolta di argomenti Valori di sistema per ulteriori informazioni sui valori forniti.

Informazioni correlate

Valori di sistema Sicurezza: Controllo codifica SSL (Secure Sockets Layer)

Protocolli SSL (Secure Sockets Layer) (QSSLPCL)

Il valore di sistema Protocolli SSL (Secure Sockets Layer) (QSSLPCL) specifica i protocolli SSL (Secure Sockets Layer) supportati dall'SSL di sistema.

I valori consentiti per il valore di sistema QSSLPCL sono i seguenti:

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

Nota: l'utente deve disporre delle autorizzazioni speciali *IOSYSCFG, *ALLOBJ e *SECADM per modificare questo valore di sistema.

È possibile fare riferimento all'argomento Protocolli SSL (Secure Sockets Layer) nella raccolta di argomenti Valori di sistema per ulteriori informazioni sui valori forniti.

Informazioni correlate

Valori di sistema Sicurezza: Protocolli SSL (Secure Sockets Layer)

Valori di sistema di ripristino relativi alla sicurezza

Questo argomento descrive i valori di sistema di ripristino relativi alla sicurezza sul sistema operativo i5/OS.

Panoramica:

Scopo: controlla come e quali oggetti relativi alla sicurezza vengono ripristinati sul sistema.

Modalità:
WRKSYSVAL*SEC (Comando Gestione valore di sistema)

Autorizzazione:
*ALLOBJ e *SECADM

Voce di giornale:
SV

Nota: Le modifiche diventano effettive immediatamente. IPL non richiesto.

Le seguenti informazioni sono descrizioni dei valori di sistema correlati al ripristino di oggetti relativi alla sicurezza sul sistema che dovrebbero essere considerati anche durante il ripristino degli oggetti. Consultare la Tabella 19 a pagina 36 per ulteriori informazioni sul valore di sistema QSCANFSCTL *NOPOSTRST.

QVFYOBJRST
Verificare l'oggetto al ripristino

QFRCCVNRST
Forzatura conversione al ripristino

QALWOBJRST
Consente il ripristino degli oggetti sensibili alla sicurezza

Seguono le descrizioni di questi valori di sistema. Per ciascun valore, vengono visualizzate le possibili scelte. Le scelte sottolineate rappresentano i valori predefiniti forniti dal sistema.

Concetti correlati

"Ripristino dei programmi" a pagina 270
Il ripristino dei programmi sul sistema, programmi ottenuti da un'origine sconosciuta, potrebbe danneggiare la sicurezza. Questo argomento fornisce informazioni sui fattori che dovrebbero essere presi in considerazione durante il ripristino dei programmi.

Verifica oggetto al ripristino (QVFYOBJRST)

Il valore di sistema Verifica oggetto al ripristino (QVFYOBJRST) determina se gli oggetti devono disporre di firme digitali per essere ripristinati sul sistema.

È possibile impedire ogni eventuale ripristino di un oggetto, a meno che tale oggetto non disponga di una firma digitale corretta proveniente da un fornitore di software sicuro. Questo valore si applica ai seguenti tipi di oggetti: *PGM, *SRVPGM, *SQLPKG, *CMD e *MODULE. Si applica inoltre anche agli oggetti *STMF contenenti programmi Java.

Quando si tenta di ripristinare un oggetto nel sistema, tre valori di sistema operano come filtri per stabilire se l'oggetto può essere ripristinato o meno. Il primo filtro è il valore di sistema Verifica oggetto al ripristino (QVFYOBJRST). Viene utilizzato per controllare il ripristino di alcuni oggetti che possono essere firmati digitalmente. Il secondo filtro è il valore di sistema, Forzatura conversione al ripristino (QFRCCVNRST). Questo valore di sistema consente di specificare se convertire i programmi, i programmi di servizio, i pacchetti SQL e gli oggetti modulo durante il ripristino. Inoltre, può impedire il ripristino di alcuni oggetti. Solo gli oggetti che superano i primi due filtri possono essere elaborati dal terzo filtro. Il terzo filtro è il valore di sistema QALWOBJRST (Abilitazione ripristino oggetto). Specifica se gli oggetti con attributi sensibili alla sicurezza possono essere ripristinati.

Se Digital Certificate Manager (i5/OS opzione 34) non è installato sul sistema, tutti gli oggetti, tranne quelli firmati da un'origine garantita dal sistema, vengono trattati come se non possedessero un firma quando si stabiliscono gli effetti del valore di sistema QVFYOBJRST durante un'operazione di ripristino.

| Gli oggetti modulo, programma e programma di servizio creati o convertiti su un sistema con un release
| precedente a V6R1 vengono considerati come non firmati quando vengono ripristinati su V6R1 o un
| sistema successivo. Allo stesso modo, gli oggetti modulo, programma e programma di servizio creati o
| convertiti su V6R1 o un release successivo vengono considerati come non firmati quando vengono
| ripristinati su un sistema precedente a V6R1.

La modifica apportata a questo valore di sistema viene applicata immediatamente.

Note:

1. questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.
2. Gli oggetti che dispongono degli attributi stato di sistema e stato di eredità devono disporre di una firma valida proveniente da un'origine garantita dal sistema. Gli oggetti nelle PTF del LIC (Licensed Internal Code) sono anche richiesti per avere una firma valida da un'origine garantita dal sistema. Se questi oggetti non hanno una firma valida, non possono essere ripristinati, indipendentemente dal valore del valore di sistema QVFYOBJRST.

Attenzione: quando si riceve il sistema, il valore di sistema QVFYOBJRST è impostato su 3. Se si modifica il valore QVFYOBJRST, è importante impostare il valore QVFYOBJRST su 3 o un valore inferiore prima di installare un nuovo release del sistema operativo i5/OS.

Tabella 27. Valori possibili per il valore di sistema QVFYOBJRST:

1	Non verificare le firme sul ripristino. Ripristinare tutti gli oggetti stato utente a prescindere dalla firma. Non utilizzare questo valore a meno che non si disponga di oggetti firmati da ripristinare, che daranno esito negativo alla verifica delle firme per un motivo valido.
2	Verificare gli oggetti sul ripristino. Ripristinare i comandi senza firma e gli oggetto con stato utente. Ripristinare i comandi con firma e gli oggetti con stato utente, anche se le firme non sono valide. Utilizzare questo valore solo se alcuni oggetti che si desidera ripristinare dispongono di firme non valide. In generale, non si consiglia di ripristinare oggetti con firme non valide sul sistema.
3	Verificare le firme sul ripristino. Ripristinare i comandi senza firma e gli oggetto con stato utente. Ripristinare i comandi con firma e gli oggetti con stato utente solo se le firme sono valide. Utilizzare questo valore per operazioni normali, quando si prevede che alcuni degli oggetti ripristinati siano senza firma ma si desidera garantire che tutti gli oggetti firmati abbiano firme valide. I comandi e i programmi creati o acquistati prima che le firme digitali fossero disponibili non disporranno delle firme. Questo valore consente il ripristino di tali comandi e programmi. Questo è il valore predefinito.
4	Verificare le firme sul ripristino. Non ripristinare i comandi e gli oggetti con stato utente non firmati. Ripristinare i comandi con firma e gli oggetti con stato utente, anche se le firme non sono valide. Utilizzare questo valore solo se alcuni oggetti che si desidera ripristinare contengono firme non valide, ma non si desidera considerare la possibilità di ripristinare oggetti non firmati. In generale, non si consiglia di ripristinare oggetti con firme non valide sul sistema.
5	Verificare le firme sul ripristino. Non ripristinare i comandi e gli oggetti con stato utente non firmati. Ripristinare i comandi con firma e gli oggetti con stato utente solo se le firme sono valide. Questo valore rappresenta il valore più restrittivo e deve essere utilizzato quando gli unici oggetti che si desidera ripristinare sono quelli che sono stati firmati da origini sicure.

Alcuni comandi utilizzano una firma che non include tutte le parti dell'oggetto. Alcune parti del comando non sono firmate mentre altre sono firmate solo se contengono un valore non predefinito. Questo tipo di firma consente di apportare alcune modifiche al comando senza invalidare la rispettiva firma. Esempi di modifiche che non invalideranno questi tipi di firme comprendono:

- Modifica dei valori predefiniti dei comandi.
- Aggiunta di un programma di controllo della validità a un comando che non ne possiede uno.
- Modifica del parametro ″dove consentire l'esecuzione″.
- Modifica del parametro ″abilitazione utenti limitati″.

È possibile aggiungere la propria firma a questi comandi che includono queste aree dell'oggetto comando.

Valore consigliato: 3

Forzatura conversione al ripristino (QFRCCVNRST)

Il valore di sistema Forzatura conversione al ripristino (QFRCCVNRST) può forzare la conversione di alcuni tipi di oggetti durante un ripristino. Questo valore di sistema può anche impedire il ripristino di alcuni oggetti.

Il valore di sistema QFRCCVNRST specifica se convertire i seguenti tipi di oggetto durante un ripristino:
- programma (*PGM)
- programma di servizio (*SRVPGM)
- pacchetto SQL (*SQLPKG)
- modulo (*MODULE)

Un oggetto per il quale è stata specificata la conversione da parte del valore di sistema, ma che non può essere convertito in quando non contiene dati di creazione sufficienti, non verrà ripristinato.

Il valore *SYSVAL per il parametro FRCOBJCVN sui comandi di ripristino (RST, RSTLIB, RSTOBJ, RSTLICPGM) utilizza il valore di questo valore di sistema. Per questo motivo, è possibile attivare e disattivare la conversione per l'intero sistema modificando il valore QFRCCVNRST. Tuttavia, il parametro FRCOBJCVN sovrascrive, in alcuni casi, il valore di sistema. Se si specifica *YES e *ALL sul parametro FRCOBJCVN, tutte le impostazioni del valore di sistema verranno sovrascritte. La specifica di *YES e *RQD sul parametro FRCOBJCVN equivale a specificare '2' per questo valore di sistema e può sovrascrivere il valore di sistema quando è impostato su 0 o 1.

QFRCCVNRST è il secondo dei tre valori di sistema che operano consecutivamente come filtri per stabilire se un oggetto può essere ripristinato o meno o se viene convertito durante il ripristino. Il primo filtro, il valore di sistema Verifica oggetto al ripristino (QVFYOBJRST), controlla il ripristino di alcuni oggetti che possono essere firmati digitalmente. Solo gli oggetti che superano i primi due filtri vengono poi elaborati dal terzo filtro, il valore di sistema Abilitazione ripristino oggetto (QALWOBJRST), che specifica se gli oggetti con attributi sensibili alla sicurezza possono essere ripristinati.

| Se Digital Certificate Manager (i5/OS opzione 34) non è installato sul sistema, tutti gli oggetti, tranne
| quelli firmati da un'origine sicura del sistema, vengono trattati come se non possedessero un firma
| quando si stabiliscono gli effetti del valore di sistema QFRCCNVRST durante un'operazione di ripristino.

| Gli oggetti modulo, programma e programma di servizio creati o convertiti su un sistema con un release
| precedente a V6R1 vengono considerati come non firmati quando vengono ripristinati su V6R1 o un
| sistema successivo. Allo stesso modo, gli oggetti modulo, programma e programma di servizio creati o
| convertiti su V6R1 o un release successivo vengono considerati come non firmati quando vengono
| ripristinati su un sistema precedente a V6R1.

Il valore fornito di QFRCCVNRST è 1. Per tutti i valori di QFRCCVNRST, un oggetto che dovrebbe essere convertito ma che non può essere convertito non verrà ripristinato. Gli oggetti firmati digitalmente da un'origine sicura del sistema vengono ripristinati senza la conversione per tutti i valori di questo valore di sistema.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

La tabella seguente riassume i valori consentiti per QFRCCVNRST:

Tabella 28. Valori QFRCCVNRST

0	Non eseguire alcuna conversione. Non impedire il ripristino dei valori.
1	Gli oggetti con errori di convalida verranno convertiti.
2	Gli oggetti saranno convertiti se la relativa conversione viene richiesta per il sistema operativo corrente o la macchina corrente o se essi presentano un errore di convalida.
3	Verranno convertiti gli oggetti che potrebbero essere stati modificati, gli oggetti contenenti errori di convalida e gli oggetti che richiedono la conversione per poter essere utilizzati sulla versione corrente del sistema operativo o sulla macchina corrente.
4	Verranno convertiti gli oggetti contenenti dati di creazione sufficienti per essere convertiti e che non dispongono di firme digitali valide. Un oggetto che non contiene dati di creazione sufficienti verrà ripristinato senza la conversione. **Nota:** verranno convertiti gli oggetti (con o senza firma) che potrebbero essere stati modificati o che richiedono la conversione per poter essere utilizzati sulla versione corrente del sistema operativo o sulla macchina corrente; qualora non fosse eseguita la conversione, il ripristino non riuscirà.
5	Verranno convertiti gli oggetti contenenti dati di creazione sufficienti. Verrà ripristinato un oggetto che non contiene dati di creazione sufficienti per la conversione. **Nota:** non verranno ripristinati gli oggetti con errori di convalida che non possono esser convertiti, che si sospetta siano stati modificati o che richiedono la conversione per poter essere utilizzati sulla versione corrente del sistema operativo.
6	Tutti gli oggetti che non dispongono di una firma digitale valida verranno convertiti. **Nota:** un oggetto con una firma digitale valida che presenta anche un errore di convalida o che si sospetta sia stato modificato verrà convertito; qualora non fosse possibile convertirlo, non verrà ripristinato.
7	Ogni oggetto verrà convertito.
Quando un oggetto viene convertito, la firma digitale viene eliminata. Lo stato dell'oggetto convertito è stato dell'utente. Gli oggetti convertiti disporranno di un valore di convalida valido e non sono sospettati di essere stati modificati.	

Valore consigliato: 3 o superiore

Consenti ripristino degli oggetti sensibili alla sicurezza (QALWOBJRST)

Il valore di sistema Consenti ripristino degli oggetti sensibili alla sicurezza QALWOBJRST determina se gli oggetti sensibili alla sicurezza possono essere ripristinati sul sistema.

Quando si tenta di ripristinare un oggetto nel sistema, tre valori di sistema operano come filtri per stabilire se l'oggetto può essere ripristinato o se viene convertito durante il ripristino. Il primo filtro è il valore di sistema Verifica oggetto al ripristino (QVFYOBJRST). Viene utilizzato per controllare il ripristino di alcuni oggetti che possono essere firmati digitalmente. Il secondo filtro è il valore di sistema, Forzatura conversione al ripristino (QFRCCVNRST). Questo valore di sistema consente di specificare se convertire i programmi, i programmi di servizio, i pacchetti SQL e gli oggetti modulo durante il ripristino. Inoltre,

può impedire il ripristino di alcuni oggetti. Solo gli oggetti che superano i primi due filtri possono essere elaborati dal terzo filtro. Il terzo filtro è il valore di sistema QALWOBJRST (Abilitazione ripristino oggetto). Specifica se gli oggetti con attributi sensibili alla sicurezza possono essere ripristinati. È possibile utilizzarlo per impedire il ripristino di un oggetto con stato del sistema o di un oggetto che adotta l'autorizzazione.

Quando si riceve il sistema, il valore di sistema QALWOBJRST è impostato su *ALL. Questo valore è necessario per installare il sistema correttamente.

ATTENZIONE: è importante impostare il valore QALWOBJRST su *ALL prima di eseguire alcune attività del sistema, come ad esempio:

- Installare un nuovo rilascio del i5/OS programma su licenza.
- Installare nuovi programmi su licenza.
- Ripristinare il sistema.

Queste attività potrebbero restituire degli errori se il valore QALWOBJRST non è impostato su *ALL. Per garantire la sicurezza del sistema, riportare il valore QALWOBJRST sull'impostazione normale dopo aver completato l'attività del sistema.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

È possibile specificare più valori per il valore di sistema QALWOBJRST, a meno che non si specifichi *ALL o *NONE.

Tabella 29. Valori possibili per il valore di sistema QALWOBJRST:

***ALL**	Un utente con l'autorizzazione corretta può ripristinare qualsiasi oggetto sul sistema.
***NONE**	Gli oggetti sensibili alla sicurezza, come ad esempio i programmi con stato di sistema o i programmi che adottano l'autorizzazione, non possono essere ripristinati sul sistema.
***ALWSYSSTT**	Gli oggetti stato di sistema e di eredità possono essere ripristinati sul sistema.
***ALWPGMADP**	Gli oggetti che adottano l'autorizzazione possono essere ripristinati sul sistema.
***ALWPTF**	Gli oggetti stato di sistema e di eredità, gli oggetti che adottano l'autorizzazione, gli oggetti che hanno dell'attributo S_ISUID(set-user-ID) abilitato e gli oggetti che hanno l'attributo S_ISGID (set-group-ID) abilitato possono essere ripristinati sul sistema durante l'installazione della PTF.
***ALWSETUID**	Consentire il ripristino dei file con l'attributo S_ISUID (set-user-ID) abilitato.
***ALWSETGID**	Consentire il ripristino dei file con l'attributo S_ISGID (set-group-ID) abilitato.
***ALWVLDERR**	Consentire il ripristino degli oggetti che non superano le verifiche di convalida dell'oggetto. Se l'impostazione del valore di sistema QFRCCVNRST provoca la conversione dell'oggetto, gli errori di convalida saranno stati corretti.

Valore consigliato: il valore di sistema QALWOBJRST fornisce un metodo per proteggere il sistema dai programmi che potrebbero causare problemi seri. Per le normali operazioni, prendere in considerazione di impostare il valore su *NONE. Ricordarsi di modificarlo in *ALL prima di eseguire le attività elencate in precedenza. Se si esegue un ripristino regolare dei programmi e delle applicazioni sul sistema, è possibile dover impostare il valore di sistema QALWOBJRST su *ALWPGMADP.

Valori di sistema che si applicano alle parole d'ordine

Questo argomento descrive il valori di sistema che si applicano alle parole d'ordine. Questi valori di sistema richiedono che gli utenti modifichino le parole d'ordine con una certa regolarità e impediscono che gli utenti assegnino parole d'ordine banali e di facile intuizione. Inoltre, garantiscono che le parole d'ordine soddisfino i requisiti della propria rete di comunicazioni.

Panoramica:

Scopo: specificare i valori di sistema per impostare i requisiti per le parola d'ordine assegnate dagli utenti.

Modalità:
WRKSYSVAL *SEC (Comando Gestione valore di sistema)

Autorizzazione:
*ALLOBJ e *SECADM

Voce di giornale:
SV

Nota: Le modifiche diventano effettive immediatamente (ad eccezione di QPWDLVL). IPL non richiesto.

Il valore di sistema controlla le parole d'ordine:

| **QPWDCHGBLK**
| Blocco modifica parola d'ordine

QPWDEXPITV
Intervallo di scadenza

| **QPWDEXPWRN**
| Avvertenza scadenza parola d'ordine

QPWDLVL
Livello parola d'ordine

QPWDLMTCHR
Caratteri limitati

QPWDLMTAJC
Limita i caratteri adiacenti

QPWDLMTREP
Limita i caratteri ripetitivi

QPWDMINLEN
Lunghezza minima

QPWDMAXLEN
Lunghezza massima

QPWDPOSDIF
Differenza posizione carattere

QPWDRQDDIF
Differenza richiesta

QPWDRQDDGT
Richiede carattere numerico

| **QPWDRULES**
| Regole parola d'ordine

QPWDVLDPGM
Programma di convalida parola d'ordine

I valori di sistema di composizione della parola d'ordine vengono applicati solo quando la parola d'ordine viene modificata mediante il comando CHGPWD, l'opzione del menu ASSIST per la modifica di una parola d'ordine o la API (application programming interface) QSYCHGPW. Tali valori non vengono applicati quando si imposta la parola d'ordine utilizzando il comando CRTUSRPRF o CHGUSRPRF.

Il sistema impedisce ad un utente di impostare la parola d'ordine uguale al nome profilo utente utilizzando il comando CHGPWD, il menu ASSIST o l'API QSYCHGPW API nelle seguenti condizioni.

- Il valore di sistema Regole parola d'ordine (QPWDRULES) ha un valore *PWDSYSVAL e il valore di sistema Lunghezza minima parola d'ordine (QPWDMINLEN) ha un valore diverso da 1.
- Il valore di sistema Regole parola d'ordine (QPWDRULES) ha un valore *PWDSYSVAL e il valore di sistema Lunghezza massima parola d'ordine (QPWDMAXLEN) ha un valore diverso da 10.
- Il valore di sistema Regole parola d'ordine (QPWDRULES) ha un valore *PWDSYSVAL e l'utente modifica gli altri valori di sistema di controllo parola d'ordine dai valori predefiniti.

Se l'utente dimentica la parola d'ordine, il responsabile della riservatezza può utilizzare il comando CHGUSRPRF (Modifica profilo utente) per impostare la parola d'ordine sullo stesso valore del nome del profilo o su un qualsiasi altro valore. Il campo Impost. parola d'ord. come scad. nel profilo utente può essere utilizzato per richiedere che la parola d'ordine venga modificata al successivo accesso dell'utente.

Informazioni correlate

Valori di sistema: panoramica sulle parole d'ordine

Blocco modifica parola d'ordine (QPWDCHGBLK)

Il valore di sistema Blocco modifica parola d'ordine (QPWDCHGBLK) specifica il periodo di tempo durante il quale le modifiche ad una parola d'ordine sono bloccate dopo l'ultima operazione di modifica della parola d'ordine riuscita.

La modifica apportata a questo valore di sistema viene applicata immediatamente.

Nota: questo valore di sistema è un valore limitato. Fare riferimento all'argomento Valori di sistema Sicurezza per i dettagli su come limitare le modifiche ai valori di sistema sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 30. Valori possibili per il valore di sistema QPWDCHGBLK:

***NONE**	È possibile modificare la parola d'ordine in qualsiasi momento.
1 - 99	Non è possibile modificare una parola d'ordine entro il numero di ore specificato dopo la precedente operazione di modifica della parola d'ordine riuscita.

Intervallo scadenza parola d'ordine (QPWDEXPITV)

Il valore di sistema Intervallo scadenza parola d'ordine (QPWDEXPITV) controlla il numero di giorni consentiti che la parola d'ordine debba essere modificata.

Se un utente tenta di accedere dopo la scadenza della parola d'ordine, il sistema visualizza un pannello che richiede di modificare la parola d'ordine prima che l'utente acceda.

```
                          Informazioni di accesso
                                                                Sistema:
Parola d'ordine scaduta. Modificare la parola d'ordine per proseguire
con la richiesta di accesso.

Accesso precedente . . . . . . . . . . . . . :   10/30/99  14:15:00

Tentativi di accesso non validi. . . . . :   3
```

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 31. Valori possibili per il valore di sistema QPWDEXPITV:

***NOMAX**	Agli utenti non viene richiesto di modificare le parole d'ordine.
limite-in-giorni	Specificare un valore compreso tra 1 e 366.

Valore consigliato: da 30 a 90

Nota: nei singoli profili utente è necessario specificare anche un intervallo di scadenza della parola d'ordine.

Intervallo avvertenza scadenza parola d'ordine (QPWDEXPWRN)

Il valore di sistema Intervallo avvertenza scadenza parola d'ordine (QPWDEXPWRN) specifica il numero di giorni prima della scadenza della parola d'ordine in cui i messaggi di avvertenza della scadenza della parola d'ordine iniziano ad essere visualizzati quando un utente accede.

La modifica apportata a questo valore di sistema viene applicata immediatamente.

Nota: questo valore di sistema è un valore limitato. Fare riferimento all'argomento Valori di sistema Sicurezza per i dettagli su come limitare le modifiche ai valori di sistema sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 32. Valori possibili per il valore di sistema QPWDEXPWRN:

7	Specifica che il messaggio di avvertenza della scadenza della parola d'ordine dovrebbe iniziare ad essere visualizzato 7 giorni prima della scadenza della parola d'ordine.
1 - 99	Specifica il numero di giorni prima della scadenza della parola d'ordine in cui i messaggi di avvertenza della scadenza della parola d'ordine iniziano ad essere visualizzati.

Valore consigliato: 14 (giorni)

Livello parola d'ordine (QPWDLVL)

È possibile impostare il livello della parola d'ordine del sistema per consentire le parole d'ordine del profilo utente con una lunghezza compresa tra 1 e 10 caratteri o per consentire le parole d'ordine del profilo utente con una lunghezza compresa tra 1 e 128 caratteri.

Il livello di parola d'ordine può essere impostato in modo da consentire una frase di accesso come valore della parola d'ordine. Il termine *parola d'ordine* viene utilizzato a volte nell'informatica per descrivere un

valore di una parola d'ordine che può essere molto lungo e che può possedere, in caso, poche limitazioni sui caratteri utilizzati nel valore della parola d'ordine. In una frase d'ordine è possibile utilizzare gli spazi vuoti tra le lettere; ciò consente all'utente di disporre di una parola d'ordine che rappresenta una frase o parte di essa. Le uniche restrizioni per una frase di accesso consistono nell'impossibilità di iniziare con un asterisco (*) e nell'eliminazione degli spazi finali. Prima di modificare il livello della parola d'ordine del sistema, rivedere la sezione Pianificazione delle modifiche al livello di una parola d'ordine.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 33. Valori possibili per il valore di sistema QPWDLVL:

0	Il sistema supporta le parole d'ordine del profilo utente con una lunghezza compresa tra 1 e 10 caratteri. I caratteri accettati sono A-Z, 0-9, i caratteri $, @, # e la sottolineatura. • QPWDLVL 0 deve essere utilizzato se il sistema comunica con altre piattaforme System i in una rete e se quei sistemi sono in esecuzione con un valore QPWDLVL 0 o su un release del sistema operativo inferiore a V5R1M0. • QPWDLVL 0 deve essere utilizzato se il sistema comunica con un qualsiasi altro sistema che limita la lunghezza delle parole d'ordine da 1 a 10 caratteri. • QPWDLVL 0 deve essere utilizzato se il sistema comunica con il prodotto Supporto i5/OS per Risorse di rete di Windows (i5/OS NetServer) e se il sistema comunica con altri sistemi che utilizzano parole d'ordine con una lunghezza compresa tra 1 e 10. Quando il valore QPWDLVL del sistema è impostato su 0, il sistema operativo creerà la parola d'ordine codificata da utilizzare per QPWDLVL 2 e 3. Il valore della parola d'ordine che può essere utilizzato per QPWDLVL 2 e 3 corrisponderà alla stessa parola d'ordine utilizzata per QPWDLVL 0 o 1.
1	QPWDLVL 1 è il supporto equivalente di QPWDLVL 0 con la seguente eccezione: le parole d'ordine i5/OS NetServer per i client Windows 95/98/ME verranno rimosse dal sistema. **Nota:** il prodotto i5/OS Netserver funzionerà con i client Windows NT/2000/XP/Vista quando il livello parola d'ordine è 1 o 3. Se si utilizza il supporto client per il prodotto i5/OS NetServer, non è possibile utilizzare il valore QPWDLVL 1. QPWDLVL 1 aumenta la sicurezza delle piattaforme System i rimuovendo tutte le parole d'ordine i5/OS NetServer dal sistema.
2	Il sistema supporta le parole d'ordine del profilo utente con una lunghezza compresa tra 1 e 128 caratteri. Sono consentiti i caratteri in maiuscolo e minuscolo. Le parole d'ordine possono essere composte qualsiasi carattere e saranno sensibili al maiuscolo e minuscolo. QPWDLVL 2 viene considerato come un livello di compatibilità. Questo livello consente di ritornare a QPWDLVL 0 o 1 se la parola d'ordine creata su QPWDLVL 2 o 3 soddisfa i requisiti di lunghezza e di sintassi di una parola d'ordine valida su QPWDLVL 0 o 1. • QPWDLVL 2 può essere utilizzato se il sistema comunica con il prodotto Supporto i5/OS per Risorse di rete di Windows (i5/OS NetServer) a condizione che la lunghezza della parola d'ordine sia compresa tra 1 e 14 caratteri. • QPWDLVL 2 non può essere utilizzato se il sistema comunica con altre piattaforme System i in una rete e se questi sistemi sono in esecuzione con un valore QPWDLVL 0 o 1 o un release del sistema operativo inferiore a V5R1M0. • QPWDLVL 2 non può essere utilizzato se il sistema comunica con un qualsiasi altro sistema che limita la lunghezza delle parole d'ordine da 1 a 10 caratteri. Quando si modifica QPWDLVL in 2, le parole d'ordine codificate non vengono eliminate dal sistema.

Tabella 33. Valori possibili per il valore di sistema QPWDLVL: (Continua)

3	Il sistema supporta le parole d'ordine del profilo utente con una lunghezza compresa tra 1 e 128 caratteri. Sono consentiti i caratteri in maiuscolo e minuscolo. Le parole d'ordine possono essere composte qualsiasi carattere e saranno sensibili al maiuscolo e minuscolo. • QPWDLVL 3 non può essere utilizzato se il sistema comunica con altre piattaforme System i in una rete e se quei sistemi sono in esecuzione con un valore QPWDLVL 0 o 1 o su un release del sistema operativo inferiore a V5R1M0. • QPWDLVL 3 non può essere utilizzato se il sistema comunica con un qualsiasi altro sistema che limita la lunghezza delle parole d'ordine da 1 a 10 caratteri. • QPWDLVL 3 non può essere utilizzato se il sistema comunica con prodotto Supporto i5/OS per Risorse di rete di Windows (i5/OS NetServer). **Nota:** il prodotto i5/OS Netserver funzionerà con i client Windows NT/2000/XP/Vista quando il livello parola d'ordine è 1 o 3. Tutte le parole d'ordine dei profili utente utilizzate per QPWDLVL 0 e 1 vengono eliminate dal sistema quando QPWDLVL è impostato su 3. Passare da QPWDLVL 3 a QPWDLVL 0 o 1 richiede di passare a QPWDLVL 2 prima di andare a 0 o a 1. QPWDLVL 2 consente di creare le parole d'ordine dei profili utente che possono essere utilizzate per QPWDLVL 0 o 1 se i requisiti della lunghezza e della sintassi della parola d'ordine soddisfano le regole impostate per QPWDLVL 0 o 1.

È necessario prestare molta attenzione se si desidera modificare il livello delle parole d'ordine del sistema e passare dalle parole d'ordine con 1-10 caratteri a quelle con 1-128 caratteri. Se il sistema comunica con altri sistemi in una rete, tutti i sistemi devono essere in grado di gestire le parole d'ordine più lunghe.

Le modifiche apportate a questo valore di sistema diventano effettive al successivo IPL. Per verificare i valori dei livelli delle parole d'ordine correnti e in sospeso, utilizzare il comando DSPSECA (Visualizzazione attributi sicurezza).

Lunghezza minima parole d'ordine (QPWDMINLEN)

Il valore di sistema Lunghezza minima parole d'ordine (QPWDMINLEN) controlla il numero minimo di caratteri un una parola d'ordine.

Note:

1. questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.
2. Se il valore di sistema QPWDRULES è un valore diverso da *PWDSYSVAL, non è possibile modificare questo valore di sistema e il relativo valore verrà ignorato quando vengono controllate le nuove parole d'ordine per vedere se sono formate correttamente.

Tabella 34. Valori possibili per il valore di sistema QPWDMINLEN:

6	Per le parole d'ordine, sono richiesti un minimo di sei caratteri.
numero-minimo-di-caratteri	Specificare un valore compreso tra 1 e 10 quando il valore di sistema del livello della parola d'ordine (QPWDLVL) è 0 o 1. Specificare un valore compreso tra 1 e 128 quando il valore di sistema del livello della parola d'ordine (QPWDLVL) è impostato su 2 o 3.

Valore consigliato: 6 è consigliato per impedire che gli utenti assegnino parole d'ordine di facile intuizione, come ad esempio le iniziali o un singolo carattere.

Lunghezza massima parole d'ordine (QPWDMAXLEN)

Il valore di sistema Lunghezza massima parole d'ordine (QPWDMAXLEN) controlla il numero massimo di caratteri in una parola d'ordine.

Questa è un'ulteriore garanzia di sicurezza poiché impedisce agli utenti di specificare parole d'ordine troppo lunghe e che devono essere registrate in qualche modo in quanto non facilmente memorizzabili. Alcune reti di comunicazione richiedono che la lunghezza della parola d'ordine sia di 8 caratteri o meno. Utilizzare questo valore di sistema per assicurarsi che le parole d'ordine soddisfino i requisiti della rete.

Note:

1. questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.
2. Se il valore di sistema QPWDRULES specifica un valore diverso da *PWDSYSVAL, non è possibile modificare questo valore di sistema e il relativo valore verrà ignorato quando vengono controllate le nuove parole d'ordine per vedere se sono formate correttamente.

Tabella 35. Valori possibili per il valore di sistema QPWDMAXLEN:

8	Per la parola d'ordine è consentita una lunghezza massima di otto caratteri.
numero-massimo-di-caratteri	Specificare un valore compreso tra 1 e 10 quando il valore di sistema del livello della parola d'ordine (QPWDLVL) è 0 o 1. Specificare un valore compreso tra 1 e 128 quando il valore di sistema del livello della parola d'ordine (QPWDLVL) è impostato su 2 o 3.

Valore consigliato: 8

Differenza richiesta nelle parole d'ordine (QPWDRQDDIF)

Il valore di sistema Differenza richiesta nelle parole d'ordine (QPWDRQDDIF) controlla se la parola d'ordine deve essere diversa dalle precedenti.

Questo valore fornisce una sicurezza aggiuntiva impedendo agli utenti di specificare parole d'ordine precedentemente utilizzate. Inoltre, si impedisce ad un utente con parola d'ordine scaduta di modificarla e di riportarla immediatamente sulla parola d'ordine precedente.

Nota: il valore del valore di sistema QPWDRQDDIF determina quante di queste parole d'ordine precedenti vengono controllate per individuare una parola d'ordine duplicata. questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 36. Valori possibili per il valore di sistema QPWDRQDDIF:

Valore	*Numero di parole d'ordine precedenti di cui sono stati verificati i duplicati*
0	Sono ammesse 0 parole d'ordine duplicate.
1	32
2	24
3	18
4	12
5	10
6	8
7	6
8	4

Valore consigliato: Selezionare un valore 5 o inferiore per impedire l'utilizzo di parole d'ordine ripetute. Utilizzare una combinazione del valore di sistema Differenza richiesta nelle parole d'ordine (QPWDRQDDIF) e del valore di sistema Intervallo scadenza parola d'ordine (QPWDEXPITV) per

impedire che una parola d'ordine venga riutilizzata per almeno 6 mesi. Ad esempio, impostare il valore di sistema QPWDEXPITV su 30 (giorni) e il valore di sistema QPWDRQDDIF su 5 (10 parole d'ordine univoche). Questo indica che un utente medio, che modifica le parole d'ordine quando avvisato dal sistema, non ripeterà la parola d'ordine per circa 9 mesi.

Caratteri limitati per le parole d'ordine (QPWDLMTCHR)

Il valore di sistema Caratteri limitati per le parole d'ordine (QPWDLMTCHR) limita l'utilizzo di determinati caratteri in una parola d'ordine.

Questo valore fornisce una sicurezza aggiuntiva impedendo agli utenti di utilizzare caratteri specifici, come ad esempio le vocali, in una parola d'ordine. Limitando le vocali, gli utenti non possono formare parole reali per le loro parole d'ordine.

Il valore di sistema QPWDLMTCHR non viene applicato quando il valore di sistema del livello della parola d'ordine (QPWDLVL) è impostato su 2 o 3. Il valore di sistema QPWDLMTCHR può essere modificato in QPWDLVL 2 o 3, ma non verrà applicato fino a quando QPWDLVL non viene modificato in un valore 0 o 1.

Note:

1. questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.
2. Se il valore di sistema QPWDRULES specifica un valore diverso da *PWDSYSVAL, non è possibile modificare questo valore di sistema e il relativo valore verrà ignorato quando vengono controllate le nuove parole d'ordine per vedere se sono formate correttamente.

Tabella 37. Valori possibili per il valore di sistema QPWDLMTCHR:

***NONE**	Non esistono caratteri limitati per le parole d'ordine.
caratteri-limitati	Specificare fino ad un massimo di 10 caratteri limitati. I caratteri validi comprendono le lettere dalla A alla Z, i numeri da 0 a 9 e i caratteri speciali quali il cancelletto (#), il dollaro ($), la chiocciola (@) e la sottolineatura (_).

Valore consigliato: A, E, I, O o U. È possibile inoltre impedire l'utilizzo di caratteri speciali (#, $ e @) per problemi di compatibilità con altri sistemi.

Limitazione delle cifre consecutive per le parole d'ordine (QPWDLMTAJC)

Il valore di sistema Limitazione delle cifre consecutive per le parole d'ordine QPWDLMTAJC limita l'utilizzo di caratteri numerici consecutivi (adiacenti) in una parola d'ordine.

Questo valore fornisce una sicurezza aggiuntiva impedendo agli utenti di utilizzare dati di compleanno, numeri telefonici o una sequenza di numeri nella composizione delle parole d'ordine.

Note:

1. questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.
2. Se il valore di sistema QPWDRULES specifica un valore diverso da *PWDSYSVAL, non è possibile modificare questo valore di sistema e il relativo valore verrà ignorato quando vengono controllate le nuove parole d'ordine per vedere se sono formate correttamente.

Tabella 38. Valori possibili per il valore di sistema QPWDLMTAJC:

0	È possibile utilizzare caratteri numerici consecutivi in una parola d'ordine.
1	Non è possibile utilizzare caratteri numerici consecutivi in una parola d'ordine.

Limitazione dei caratteri ripetuti per le parole d'ordine (QPWDLMTREP)

Il valore di sistema Limitazione dei caratteri ripetuti per le parole d'ordine (QPWDLMTREP) limita la ripetizione dei caratteri in una parola d'ordine.

Questo valore fornisce una sicurezza aggiuntiva impedendo agli utenti di specificare parole d'ordine facili da individuare, come ad esempio lo stesso carattere ripetuto diverse volte.

Quando il valore di sistema del livello della parola d'ordine (QPWDLVL) è impostato su 2 o 3, la verifica dei caratteri ripetuti è sensibile al maiuscolo e minuscolo. Ciò indica che una 'a' in minuscolo non equivale ad una 'A' in maiuscolo.

Note:

1. questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.
2. Se il valore di sistema QPWDRULES specifica un valore diverso da *PWDSYSVAL, non è possibile modificare tale valore di sistema e il relativo valore sarà ignorato quando le nuove parole d'ordine verranno controllate per verificare che siano state formate correttamente.

Tabella 39. Valori possibili per il valore di sistema QPWDLMTREP:

0	Gli stessi caratteri possono essere utilizzati più di una volta all'interno di una parola d'ordine.
1	Lo stesso carattere non può essere utilizzato più di una volta in una parola d'ordine.
2	Lo stesso carattere non può essere utilizzato consecutivamente in una parola d'ordine.

La Tabella 40 mostra degli esempi delle parole d'ordine consentite in base al valore di sistema QPWDLMTREP.

Tabella 40. Parole d'ordine aventi caratteri che si ripetono con QPWDLVL 0 o 1

Esempio di parole d'ordine	Valore QPWDLMTREP 0	Valore QPWDLMTREP 1	Valore QPWDLMTREP 2
A11111	Consentito	Non consentito	Non consentito
BOBBY	Consentito	Non consentito	Non consentito
AIRPLANE	Consentito	Non consentito	Consentito
N707UK	Consentito	Non consentito	Consentito

Tabella 41. Parole d'ordine aventi caratteri che si ripetono con QPWDLVL 2 o 3

Esempio di parola d'ordine	Valore QPWDLMTREP 0	Valore QPWDLMTREP 1	Valore QPWDLMTREP 2
j222222	Consentito	Non consentito	Non consentito
ReallyFast	Consentito	Non consentito	Non consentito
Mom'sApPlePie	Consentito	Non consentito	Consentito
AaBbCcDdEe	Consentito	Consentito	Consentito

Differenza posizione carattere per le parole d'ordine (QPWDPOSDIF)

Il valore di sistema Differenza posizione carattere per le parole d'ordine (QPWDPOSDIF) controlla ogni posizione in una nuova parola d'ordine.

Questo valore di sistema fornisce una maggiore sicurezza impedendo agli utenti di utilizzare lo stesso carattere (alfabetico o numerico) in una posizione corrispondente alla stessa posizione nella parola d'ordine precedente.

Quando il valore di sistema del livello di parola d'ordine (QPWDLVL) è impostato su 2 o 3, la verifica dello stesso carattere è sensibile al maiuscolo e minuscolo. Ciò indica che una 'a' in minuscolo non equivale ad una 'A' in maiuscolo.

Note:

1. questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.
2. Se il valore di sistema QPWDRULES specifica un valore diverso da *PWDSYSVAL, non è possibile modificare questo valore di sistema e il relativo valore verrà ignorato quando vengono controllate le nuove parole d'ordine per vedere se sono formate correttamente.

Tabella 42. Valori possibili per il valore di sistema QPWDPOSDIF:

0	Gli stessi caratteri possono essere utilizzati in una posizione corrispondente alla stessa posizione nella parola d'ordine precedente.
1	Lo stesso carattere non può essere utilizzato in una posizione corrispondente alla stessa posizione nella parola d'ordine precedente.

Requisito per carattere numerico nelle parole d'ordine (QPWDRQDDGT)

Il valore di sistema Requisito per carattere numerico nelle parole d'ordine (QPWDRQDDGT) controlla se è richiesto un carattere numerico in una nuova parola d'ordine. Questo valore fornisce una maggiore sicurezza impedendo agli utenti di utilizzare tutti i caratteri alfabetici.

Note:

1. questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.
2. Se il valore di sistema QPWDRULES specifica un valore diverso da *PWDSYSVAL, non è possibile modificare questo valore di sistema e il relativo valore verrà ignorato quando vengono controllate le nuove parole d'ordine per vedere se sono formate correttamente.

Tabella 43. Valori possibili per il valore di sistema QPWDRQDDGT:

0	I caratteri numerici non sono richiesti nelle nuove parole d'ordine.
1	Nelle nuove parole d'ordine vengono richiesti uno o più caratteri numerici.

Valore consigliato: 1

Regole parola d'ordine (QPWDRULES)

Il valore di sistema Regole parola d'ordine (QPWDRULES) specifica le regole utilizzate per controllare se una parola d'ordine è formata correttamente. È possibile specificare più di un valore per il valore di sistema QPWDRULES, a meno che non venga specificato *PWDSYSVAL.

Le modifiche apportate a questo valore di sistema diventano operative alla successiva modifica di una parola d'ordine.

Nota: questo valore di sistema è un valore limitato. Fare riferimento all'argomento Valori di sistema Sicurezza per i dettagli su come limitare le modifiche ai valori di sistema sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 44. Valori possibili per il valore di sistema QPWDRULES:

***PWDSYSVAL**	Il valore specifica che il valore di sistema QPWDRULES viene ignorato e che gli altri valori di sistema della parola d'ordine vengono utilizzati per controllare se una parola d'ordine è formata correttamente. Questi altri valori di sistema della parola d'ordine includono QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF e QPWDQDDGT. **Nota:** se viene specificato un valore diverso da *PWDSYSVAL per QPWDRULES, i valori di sistema QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF, e QPWDRQDDGT vengono ignorati quando una nuova parola d'ordine viene controllata per vedere se è stata formata correttamente. Inoltre, qualsiasi tentativo di modifica a questi valori di sistema verrà rifiutato finché il valore di sistema QPWDRULES conterrà un valore diverso da *PWDSYSVAL.

***CHRLMTAJC**	Il valore specifica che una parola d'ordine non può modificare 2 o più ricorrenze consecutive dello stesso carattere. La funzione eseguita da questo valore equivale alla specifica di un valore 2 per il valore di sistema QPWDLMTREP. Se è stato specificato il valore *CHRLMTREP, non è possibile specificare questo valore.
	Esempi:
	`Better.test  non valido - tt`
	`fix11bugs  non valido - 11`
	`@12/A78  valido`
	`A1234A1234  valido`

***CHRLMTREP**	Il valore specifica che una parola d'ordine non può contenere 2 o più ricorrenze dello stesso carattere. La funzione eseguita da questo valore equivale alla specifica di un valore 1 per il valore di sistema QPWDLMTREP. Se è stato specificato il valore *CHRLMTAJC, non è possibile specificare questo valore.
	Esempi:
	`John.Jones  non valido - J o n`
	`THISONEOK  non valido - O`
	`@12/A78  valido`
	`AaCcEeFfGg  valido`

***DGTLMTAJC**	Il valore specifica che una parola d'ordine non può contenere 2 o più caratteri cifra adiacenti.
	Esempi:
	`@12/A78  non valido`
	`!@#$%a1234.  non valido`
	`THISONEOK  valido`
	`A1B2C3DE5  valido`

Tabella 44. Valori possibili per il valore di sistema QPWDRULES: (Continua)

***DGTLMTFST**	Il valore specifica che il primo carattere di una parola d'ordine non può essere un carattere cifra. Se sono stati specificati i valori *LTRLMTFST e *SPCCHRLMTFST, non è possibile specificare questo valore. Se il sistema sta funzionando al livello di sicurezza 0 o 1, esso funziona come se fosse specificato il valore *DGTLMTFST.
	Esempi:
	`16ST-SW-Roch  non valido - 1`
	`99BottlesOfBeer  non valido - 9`
	`@12/A78  valido`
	`Allow-this.1  valido`

***DGTLMTLST**	Il valore specifica che l'ultimo carattere della parola d'ordine non può essere un carattere cifra. Se sono stati specificati i valori *LTRLMTLST e *SPCCHRLMTLFST, non è possibile specificare questo valore.
	Esempi:
	`John.doe12  non valido - 2`
	`@12/A78  non è valido - 8`
	`THISONEOK  valido`
	`A1234b123.  valido`

***DGTMAXn**	Il valore specifica il numero massimo di caratteri cifra che possono essere utilizzati nella parola d'ordine. **n** è un numero compreso tra 0 e 9.
	
	È possibile specificare solo un valore *DGTMAXn. Se viene specificato anche un valore *DGTMINn, il valore n specificato per *DGTMAXn deve essere maggiore o uguale al valore n specificato per *DGTMINn.
	Esempi: per *DGTMAX2
	`Q12345678  non valido - 6 cifre di troppo`
	`3-2-1->Go  non valido - 1 cifra di troppo`
	`Rick1  valido`
	`Ed1-Jeff3  valido`

***DGTMINn**	Il valore specifica il numero minimo di caratteri cifra che devono essere utilizzati nella parola d'ordine. **n** è un numero compreso tra 0 e 9.
	
	È possibile specificare solo un valore *DGTMINn. Se viene specificato anche un valore *DGTMAXn, il valore n specificato per *DGTMAXn deve essere maggiore o uguale al valore n specificato per *DGTMINn.
	Esempi: per *DGTMIN3
	`Rick1  non valido - solo 1 cifra`
	`Ed1-Jeff3  non valido - solo 2 cifre`
	`3-2-1->Go  valido`
	`Q12345678  valido`

Tabella 44. Valori possibili per il valore di sistema QPWDRULES: (Continua)

***LMTSAMPOS**	Lo stesso carattere non può essere utilizzato in una posizione corrispondente alla stessa posizione nella parola d'ordine precedente. Questo valore esegue la stessa funzione del valore di sistema QPWDPOSDIF.
	
	Quando la parola d'ordine viene impostata dal comando CHGUSRPRF (Modifica profilo utente) o CRTUSRPRF (Creazione profilo utente), questa regola della parola d'ordine non può essere controllata poiché il valore della parola d'ordine precedente non viene fornito.
	Esempi: per *LMTSAMPOS quando la parola d'ordine precedente era Vote4Me:
	`Victory1 non valido - V in posizione 1`
	`Mine2love non valido - e in posizione 4`
	`vOTE-mE valido (maiuscole/minuscole diverse)`
	`Allisgood valido`

***LMTPRFNAME**	Il valore parola d'ordine in lettere maiuscole non può contenere il nome profilo utente in posizioni consecutive.
	Esempi: per *LMTPRFNAME con nome profilo JOHNB:
	`bigJOHNB9 non valido - posizioni 4-8`
	`JohnB78 non valido - posizioni 1-5`
	`J_ohn_B234 valido`
	`john_b valido`

***LTRLMTAJC**	Il valore specifica che una parola d'ordine non può contenere 2 o più caratteri lettera adiacenti.
	Esempi:
	`John.Smith non valido`
	`THISONEOK non valido`
	`@12/A78 valido`
	`A1234b1234 valido`

***LTRLMTFST**	Il valore specifica che il primo carattere della parola d'ordine non può essere un carattere lettera. Se sono stati specificati i valori *DGTLMTFST e *SPCCHRLMTFST, non è possibile specificare questo valore. Se il sistema sta funzionando con un valore QPWDLVL 0 o 1, non è possibile specificare sia *LTRLMTFST che *SPCCHRLMTFST.
	Esempi:
	`John.Smith non valido - J`
	`THISONEOK non valido - T`
	`@12/A78 valido`
	`16ST-SW-Roch valido`

***LTRLMTLST**	Il valore specifica che l'ultimo carattere della parola d'ordine non può essere un carattere lettera. Se sono stati specificati i valori *DGTLMTLST e *SPCCHRLMTLST, non è possibile specificare questo valore
	Esempi:
	`John.Smith non valido - h`
	`1Allow.It non valido - t`
	`@12/A78 valido`
	`(pay*rate) valido`

Tabella 44. Valori possibili per il valore di sistema QPWDRULES: (Continua)

***LTRMAXn**	Il valore specifica il numero massimo di caratteri lettera che possono essere utilizzati nella parola d'ordine. **n** è un numero compreso tra 0 e 9.
	
	È possibile specificare solo un valore *LTRMAXn. Se viene specificato anche un valore *LTRMINn, il valore n specificato per *LTRMAXn deve essere maggiore o uguale al valore n specificato per *LTRMINn.
	
	Se viene specificato anche un valore *MIXCASEn, il valore n specificato per *LTRMAXn deve essere maggiore o uguale al doppio del valore n specificato per *MIXCASEn.
	Esempi: per *LTRMAX4
	`THISONEOK  non valido - 5 lettere di troppo`
	`John.Smith1  non valido - 5 lettere di troppo`
	`John1423  valido`
	`A1b2.#456  valido`

***LTRMINn**	Il valore specifica il numero minimo di caratteri lettera che devono essere utilizzati nella parola d'ordine. **n** è un numero compreso tra 0 e 9.
	
	È possibile specificare solo un valore *LTRMINn. Se è stato specificato un valore *LTRMAXn, il valore n specificato per *LTRMAXn deve essere maggiore o uguale al valore n specificato per *LTRMINn.
	Esempi: per *LTRMIN2
	`@12/A78  non valido - solo 1 lettera`
	`!@#$%a1234  non valido - solo 1 lettera`
	`THISONEOK  valido`
	`A1234b1234  valido`

***MAXLENnnn**	Il valore specifica il numero massimo di caratteri in una parola d'ordine. **nnn** è un numero compreso tra 1 e 128 (senza zero iniziali). Questo valore esegue la stessa funzione del valore di sistema QPWDMAXLEN. Se il sistema sta funzionando al livello QPWDLVL 0 o 1, l'intervallo valido è compreso tra 1 e 10. Se il sistema sta funzionando al livello QPWDLVL 2 o 3, l'intervallo valido è compreso tra 1 e 128. Il valore nnn specificato deve essere sufficientemente grande da soddisfare tutte le limitazioni del primo e dell'ultimo carattere, *MIXCASEn, *DGTMAXn, *LTRMAXn, *SPCCHRMAXn e i requisiti di caratteri non adiacenti. Se viene specificato anche *MINLENnnn, il valore nnn specificato per *MAXLENnnn deve essere maggiore o uguale al valore nnn specificato per *MINLENnnn. Se non viene specificato alcun valore *MAXLENnnn, si presume un valore *MAXLEN10 se il sistema sta funzionando con un valore QPWDLVL 0 o 1 oppure un valore *MAXLEN128 se il sistema sta funzionando con un valore QPWDLVL 2 o 3.

Tabella 44. Valori possibili per il valore di sistema QPWDRULES: (Continua)

***MINLENnnn**	Il valore specifica il numero minimo di caratteri in una parola d'ordine. **nnn** è un numero compreso tra 1 e 128 (senza zero iniziali). Se il sistema sta funzionando al livello QPWDLVL 0 o 1, l'intervallo valido è compreso tra 1 e 10. Se il sistema sta funzionando al livello QPWDLVL 2 o 3, l'intervallo valido è compreso tra 1 e 128. Se viene specificato anche *MAXLENnnn, il valore nnn specificato per *MAXLENnnn deve essere maggiore o uguale al valore nnn specificato per *MINLENnnn. Se non viene specificato alcun valore *MINLENnnn, si presume un valore *MINLEN1.

***MIXCASEn**	Il valore specifica che la parola d'ordine deve contenere almeno n lettere maiuscole e n lettere minuscole. **n** è un numero compreso tra 0 e 9. Questo valore viene rifiutato se il sistema sta funzionando con un valore QPWDLVL 0 o 1 poiché è necessario che le parole d'ordine siano maiuscole.
	
	È possibile specificare solo un valore *MIXCASEn.
	
	Se è stato specificato un valore *LTRMAXn, il valore n specificato per *LTRMAXn deve essere maggiore o uguale al doppio del valore n specificato per *MIXCASEn.
	Esempi: per *MIXCASE2
	`@12/A78bC  non valido - manca 1 caratt. minusc.`
	`THISONEOK  non valido - mancano 2 caratt. minusc.`
	`ThisIsOkay  valido`
	`Allow-It  valido`

***REQANY3**	Il valore specifica che una parola d'ordine deve contenere caratteri di almeno tre dei seguenti quattro tipi di caratteri.
	• Lettere maiuscole
	• Lettere minuscole
	• Cifre
	• Caratteri speciali
	
	Quando il sistema sta funzionando con QPWDLVL 0 o 1, *REQANY3 ha lo stesso effetto della specifica di *DGTMIN1, *LTRMIN1 e *SPCCHRMIN1.
	Esempi:
	`THISONEOK  non valido - solo 1 tipo`
	`@12/-78  non valido - solo 2 tipi`
	`A1234b1234  valido - maiuscolo, minuscolo, cifra`
	`John.Smith  valido - maiuscolo, minuscolo, spec.`
	`peter(21)  valido - minuscolo, speciale, cifra`

Tabella 44. Valori possibili per il valore di sistema QPWDRULES: (Continua)

***SPCCHRLMTAJC**	Il valore specifica che una parola d'ordine non può contenere 2 o più caratteri speciali adiacenti (consecutivi). Un carattere viene considerato come un carattere speciale se il relativo carattere unicode equivalente dispone della proprietà di non essere né una lettera né una cifra.
	Esempi:
	`Big//Box  non valido`
	`this->way  non valido`
	`@12/A78  valido`
	`John.Smith  valido`

***SPCCHRLMTFST**	Il valore specifica che il primo carattere della parola d'ordine non può essere un carattere speciale. Un carattere viene considerato come un carattere speciale se il relativo carattere unicode equivalente dispone della proprietà di non essere né una lettera né una cifra.
	
	Se sono stati specificati i valori *DGTLMTFST e *LTRLMTFST, non è possibile specificare questo valore. Se il sistema sta funzionando con un valore QPWDLVL 0 o 1, non è possibile specificare sia *LTRLMTFST che *SPCCHRLMTFST.
	Esempi:
	`(2+2equals4)  non valido - (`
	`#fred/#charlie non valido - #`
	`1Good->one12  valido`
	`A1234b1234  valido`

***SPCCHRLMTLST**	Il valore specifica che l'ultimo carattere della parola d'ordine non può essere un carattere speciale. Un carattere viene considerato come un carattere speciale se il relativo carattere unicode equivalente dispone della proprietà di non essere né una lettera né una cifra.
	
	Se sono stati specificati i valori *DGTLMTLST e *LTRLMTLST, non è possibile specificare questo valore.
	Esempi:
	`A1234b123.  non valido - .`
	`>John.Doe<  non valido - <`
	`THISONEOK  valido`
	`@12/A78  valido`

***SPCCHRMAXn**	Il valore specifica il numero massimo di caratteri speciali che possono essere utilizzati nella parola d'ordine. **n** è un numero compreso tra 0 e 9. Un carattere viene considerato come un carattere speciale se il relativo carattere unicode equivalente dispone della proprietà di non essere né una lettera né una cifra.
	
	È possibile specificare solo un valore *SPCCHRMAXn. Se è stato specificato un valore *SPCCHRMINn, il valore n specificato per *SPCCHRMAXn deve essere maggiore o uguale al valore n specificato per *SPCCHRMINn.
	Esempi: per *SPCCHRMAX3
	`@12/A78.b#  non valido - 1 di troppo`
	`!@#$%a1234  non valido - 2 di troppo`
	`THISONEOK  valido`
	`A1234b-234  valido`

Tabella 44. Valori possibili per il valore di sistema QPWDRULES: (Continua)

***SPCCHRMINn**	Il valore specifica il numero minimo di caratteri speciali che devono essere utilizzati nella parola d'ordine. **n** è un numero compreso tra 0 e 9. Un carattere viene considerato come un carattere speciale se il relativo carattere unicode equivalente dispone della proprietà di non essere né una lettera né una cifra.
	
	È possibile specificare solo un valore *SPCCHRMINn. Se è stato specificato un valore *SPCCHRMAXn, il valore n specificato per *SPCCHRMAXn deve essere maggiore o uguale al valore n specificato per *SPCCHRMINn.
	Esempi: per *SPCCHRMIN4
	`Su@us.ibm.com  non valido - 1 in meno`
	`123+45=168     non valido - 2 in meno`
	`A.B@us.ibm.com valido`
	`(24/8=3)       valido`

Programma di approvazione parola d'ordine (QPWDVLDPGM)

È possibile specificare Programma di approvazione parola d'ordine (QPWDVLDPGM) per controllare la convalida delle nuove parole d'ordine.

Se si specifica *REGFAC o un nome programma nel valore di sistema QPWDVLDPGM, il sistema esegue uno o più programmi dopo che la nuova parola d'ordine ha superato le verifiche di convalida specificate nei valori di di sistema di controllo delle parole d'ordine. È possibile utilizzare i programmi per eseguire controlli aggiuntivi sulle parole d'ordine assegnate dall'utente prima che vengano accettate dal sistema.

Un programma di approvazione delle parole d'ordine deve trovarsi nell'ASP (auxiliary storage pool) del sistema o dell'utente di base.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 45. Valori possibili per il valore di sistema QPWDVLDPGM:

***NONE**	Non viene utilizzato alcun programma scritto dall'utente. Sono compresi i programmi di approvazione delle parole d'ordine registrati nella funzione di registrazione dell'uscita.
**REGFAC*	Il programma di convalida viene richiamato dalla funzione di registrazione, punto di uscita QIBM_QSY_VLD_PASSWRD. Nella funzione di registrazione è possibile specificare più di un programma di convalida. Ogni programma verrà richiamato fino a quando uno di essi non indica che la parola d'ordine deve essere rifiutata o fino a quando tutti i programmi non hanno indicato che la parola d'ordine è valida.
nome-programma	Specificare il nome del programma di convalida scritto dall'utente, da 1 a 10 caratteri. Un nome di programma non può essere specificato quando il valore corrente o in sospeso del valore di sistema del livello della parola d'ordine (QPWDLVL) è impostato su 2 o 3.
nome-libreria	Specificare il nome della libreria in cui è posizionato il programma scritto dall'utente. Se il nome della libreria non viene specificato, si utilizza l'elenco delle librerie (*LIBL) dell'utente che modifica il valore di sistema per cercare il programma. QSYS è la libreria consigliata.

Utilizzo di un programma di approvazione della parola d'ordine

Se si specifica *REGFAC o il nome di un programma nel valore di sistema QPWDVLDPGM, uno o più programmi vengono richiamati dal comando Modifica parola d'ordine (CHGPWD) o dalla API Modifica parola d'ordine (QSYCHGPW). I programmi vengono richiamati solo se la nuova parola d'ordine ha superato tutte le altre verifiche specificate nei valori di sistema di controllo della parola d'ordine.

Qualora fosse necessario recuperare il sistema dopo un errore disco, posizionare il programma di approvazione delle parole d'ordine nella libreria QSYS. In questo modo, il programma di approvazione delle parole d'ordine viene caricato quando si ripristina la libreria QSYS.

Se si specifica il nome di un programma nel valore di sistema QPWDVLDPGM, il sistema inoltra i seguenti parametri al programma di approvazione delle parole d'ordine:

Tabella 46. Parametri per il programma di approvazione delle parole d'ordine

Posizione	Tipo	Lunghezza	Descrizione
1	*CHAR	10	La nuova parola d'ordine inserita dall'utente.
2	*CHAR	10	La vecchia parola d'ordine dell'utente.
3	*CHAR	1	Codice di ritorno: 0 per parola d'ordine valida; diverso da 0 per parola d'ordine non corretta.
4 [1]	*CHAR	10	Il nome dell'utente.
1 La posizione 4 è facoltativa.			

Se si specifica *REGFAC nel valore di sistema QPWDVLDPGM, fare riferimento alle informazioni sul Programma di uscita di sicurezza nel manuale dell'API di sistema per dettagli sui parametri trasmessi al programma di convalida.

Se il programma stabilisce che la nuova parola d'ordine non è valida, è possibile inviare il proprio messaggio di eccezione (mediante il comando SNDPGMMSG) o impostare il codice di ritorno su un valore diverso da 0 e consentire al sistema di visualizzare un messaggio di errore. I messaggi di eccezione segnalati dal programma devono essere creati con l'opzione DMPLST(*NONE) del comando Aggiunta descrizione messaggio (ADDMSGD).

La nuova parola d'ordine viene accettata solo se il programma scritto dall'utente termina senza un messaggio di uscita e un codice di ritorno pari a 0. Poiché il codice di ritorno viene impostato inizialmente per le parole d'ordine non valide (diverse da zero), il programma di approvazione deve impostare il codice di ritorno su 0 prima che la parola d'ordine possa essere modificata.

Attenzione: la parola d'ordine corrente e nuova vengono inoltrate al programma di convalida senza codifica. Il programma di convalida può memorizzare le parole d'ordine in un file di database e compromettere la sicurezza sul sistema. Accertarsi che le funzioni del programma di convalida siano riviste dal responsabile della riservatezza e che le modifiche apportate al programma siano severamente controllate.

Il seguente programma CL (control language) è un esempio di un programma di approvazione delle parole d'ordine quando si specifica il nome di un programma per QPWDVLDPGM. Questo esempio si accerta che la parola d'ordine non venga modificata più di una volta nello stesso giorno. È possibile aggiungere ulteriori calcoli al programma per controllare altri criteri per le parole d'ordine:

Nota: utilizzando i codici di esempio, si accettano i termini presenti nel Capitolo 10, "Informazioni sull'esonero di responsabilità e licenza codice", a pagina 329.

```
/*************************************************/
/* NOME:     PWDVALID - Convalida parola d'ordine */
/*                                               */
/* FUNZIONE: Limitare la modifica della parola d'ordine ad  */
/*           una al giorno a meno che la parola d'ordine non sia scaduta   */
/*************************************************/
   PGM (&NEW &OLD &RTNCD &USER)
   DCL VAR(&NEW)       TYPE(*CHAR) LEN(10)
   DCL VAR(&OLD)       TYPE(*CHAR) LEN(10)
   DCL VAR(&RTNCD)     TYPE(*CHAR) LEN(1)
   DCL VAR(&USER)      TYPE(*CHAR) LEN(10)
   DCL VAR(&JOBDATE)   TYPE(*CHAR) LEN(6)
   DCL VAR(&PWDCHGDAT) TYPE(*CHAR) LEN(6)
   DCL VAR(&PWDEXP)    TYPE(*CHAR) LEN(4)
/* Richiamare la data corrente e convertirla nel formato YMD */
   RTVJOBA    DATE(&JOBDATE)
   CVTDAT     DATE(&JOBDATE) TOVAR(&JOBDATE) +
              TOFMT(*YMD)    TOSEP(*NONE)
/* Richiamare la data dell'ultima modifica della parola d'ordine e se     */
/* questa è scaduta dal profilo utente                                    */
   RTVUSRPRF  USRPRF(&USER)  PWDCHGDAT(&PWDCHGDAT)+
     PWDEXP(&PWDEXP)
/* Confrontare due date                        */
/* per verificare che siano uguali e che la parola d'ordine non sia scaduta   */
/* inviare quindi un messaggio *ESCAPE per impedire la modifica */
/* impostare il codice di ritorno per consentire la modifica    */
   IF (&JOBDATE=&PWDCHGDAT *AND &PWDEXP='*NO ') +
       SNDPGMMSG  MSGID(CPF9898) MSGF(QCPFMSG) +
       MSGDTA('Password can be changed only +
               once per day') +
       MSGTYPE(*ESCAPE)
   ELSE  CHGVAR &RTNCD '0'
   ENDPGM
```

Il seguente programma CL (control language) rappresenta un esempio di programma di approvazione delle parole d'ordine quando si specifica *REGFAC per QPWDVLDLVL.

Questo esempio verifica che la nuova parola d'ordine sia in CCSID 37 (oppure, se è in CCSID 13488, converte la nuova parola d'ordine in CCSID 37), che la nuova parola d'ordine non termini con un carattere numerico e che la nuova parola d'ordine non contenga il nome del profilo utente. L'esempio presuppone che un file dei messaggi (PWDERRORS) sia stato creato e che le descrizioni dei messaggi (PWD0001 e PWD0002) siano state aggiunte al file dei messaggi. È possibile aggiungere ulteriori calcoli al programma per controllare altri criteri per le parole d'ordine:

```
/*********************************************************/
/*                                                       */
/*  NOME:   PWDEXITPGM1 - Convalida parola d'ordine uscita 1      */
/*                                                       */
/*  Convalida le parole d'ordine quando si specifica *REGFAC per     */
/*  QPWDVLDPGM. Il programma viene registrato con il comando CL/
/*  ADDEXITPGM* per il punto di uscita QIBM_QSY_VLD_PASSWRD.   */
/*                                                       */
/*                                                       */
/*  PRESUPPOSTI: se si è utilizzato il comando CHGPWD, la */
/*  parola d'ordine CCSID sarà il valore predefinito del lavoro
    (che si presuppone sia CCSID 37).   */
/*  Se si è utilizzata la API QSYCHGPW, la parola
    d'ordine CCSID sarà                                */
/*  UNICODE CCSID 13488.                                 */
/*********************************************************/

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

DCL &UNAME      *CHAR 10
```

```
DCL &NEWPW      *CHAR 256
DCL &NPOFF      *DEC 5 0
DCL &NPLEN      *DEC 5 0
DCL &INDX       *DEC 5 0
DCL &INDX2      *DEC 5 0
DCL &INDX3      *DEC 5 0
DCL &UNLEN      *DEC 5 0

DCL &XLTCHR2    *CHAR 2 VALUE(X'0000')
DCL &XLTCHR     *DEC 5 0
DCL &XLATEU     *CHAR 255 VALUE('............................... +
                               !"#$''()*+,-./0123456789:;<=>?+
                               @ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_+
                               `ABCDEFGHIJKLMNOPQRSTUVWXYZ{|}~.+
                               ................................+
                               ................................+
                               ................................+
                               ................................')

DCL &XLATEC     *CHAR 255 VALUE('................................+
                               ................................+
                               ................................+
                               ................................+
                               .ABCDEFGHI.......JKLMNOPQR......+
                               ..STUVWXYZ......................+
                               ................................+
                               ................................')

/*********************************************************************/
/* FORMATO EXINPUT:                                                  */

/* POSIZIONE  DESCRIZIONE                                            */
/* 001 - 020  NOME PUNTO USCITA                                      */
/* 021 - 028  NOME FORMATO PUNTO USCITA                              */
/* 029 - 032  LIVELLO PAROLA D'ORDINE (binario)                      */
/* 033 - 042  NOME PROFILO UTENTE                                    */
/* 043 - 044  RISERVATO                                              */
/* 045 - 048  SCOSTAMENTO SU PAROLA D'ORDINE VECCHIA (binario)       */
/* 049 - 052  LUNGHEZZA PAROLA D'ORDINE VECCHIA      (binario)       */
/* 053 - 056  CCSID DELLA PAROLA D'ORDINE VECCHIA  (binario)       */
/* 057 - 060  SCOSTAMENTO SU PAROLA D'ORDINE NUOVA   (binario)      */
/* 061 - 064  LUNGHEZZA NUOVA PAROLA D'ORDINE (binario)              */
/* 065 - 068  CCSID NUOVA PAROLA D'ORDINE     (binario)              */
/* ??? - ???  VECCHIA PAROLA D'ORDINE                                */
/* ??? - ???  NUOVA PAROLA D'ORDINE                                  */
/*                                                                   */
/*********************************************************************/


/*********************************************************************/
/*  Stabilire un controllo generico per il programma.                */
/*********************************************************************/

MONMSG     CPF0000
/* Si presupponga che la nuova parola d'ordine sia valida */
CHGVAR &RTN  VALUE('0') /* accept */
/* Richiamare la lunghezza della nuova parola d'ordine,
   lo scostamento e il valore. Ottenere anche il nome
   utente                                          */
CHGVAR &NPLEN VALUE(EXINPUT 61 4))
CHGVAR &NPOFF VALUE(EXINPUT 57 4) + 1)
CHGVAR &UNAME VALUE(EXINPUT 33 10))
CHGVAR &NEWPW VALUE(EXINPUT &NPOFF &NPLEN))
/* Se CCSID è 13488, probabilmente è stata utilizzata la API
   QSYCHGPW che converte */
/* le parole d'ordine in UNICODE CCSID 13488. Convertire in CCSID 37, se */
/* possibile, altrimenti viene restituito un errore */
```

```
IF COND(EXINPUT 65 4) = 13488) THEN(DO)
    CHGVAR &INDX2 VALUE(1)
    CHGVAR &INDX3 VALUE(1)
   CVT1:
    CHGVAR &XLTCHR VALUE(NEWPW &INDX2 2))
    IF COND( (&XLTCHR *LT 1) *OR (&XLTCHR *GT 255) ) THEN(DO)
       CHGVAR &RTN  VALUE('3') /* reject */
       SNDPGMMSG MSG('INVALID CHARACTER IN NEW PASSWORD')
       GOTO DONE
    ENDDO
    CHGVAR NEWPW &INDX3 1) VALUE(XLATEU &XLTCHR 1))
    CHGVAR &INDX2  VALUE(&INDX2 + 2)
    CHGVAR &INDX3  VALUE(&INDX3 + 1)
    IF COND(&INDX2 > &NPLEN) THEN(GOTO ECVT1)
    GOTO CVT1
   ECVT1:
    CHGVAR &NPLEN VALUE(&INDX3 - 1)
    CHGVAR EXINPUT 65 4) VALUE(X'00000025')
 ENDDO

 /* Richiamare il CCSID del valore della nuova parola
    d'ordine - deve essere 37     */
 IF COND(EXINPUT 65 4) *NE 37) THEN(DO)
   CHGVAR &RTN  VALUE('3') /* reject */
   SNDPGMMSG MSG('CCSID OF NEW PASSWORD MUST BE 37')
   GOTO DONE
 ENDDO

 /* UPPERCASE NEW PASSWORD VALUE                      */
 CHGVAR &INDX2 VALUE(1)
 CHGVAR &INDX3 VALUE(1)
 CVT4:
   CHGVAR XLTCHR2 2 1) VALUE(NEWPW &INDX2 1))
   CHGVAR &XLTCHR VALUE(XLTCHR2 1 2))
   IF COND( (&XLTCHR *LT 1) *OR (&XLTCHR *GT 255) ) THEN(DO)
     CHGVAR &RTN  VALUE('3') /* reject */
     SNDPGMMSG MSG('INVALID CHARACTER IN NEW PASSWORD')
     GOTO DONE
   ENDDO
   IF COND(XLATEC &XLTCHR 1) *NE '.') +
   THEN(CHGVAR NEWPW &INDX3 1) VALUE(XLATEC &XLTCHR 1)))
   CHGVAR &INDX2  VALUE(&INDX2 + 1)
   CHGVAR &INDX3  VALUE(&INDX3 + 1)
   IF COND(&INDX2 > &NPLEN) THEN(GOTO ECVT4)
   GOTO CVT4
 ECVT4:

 /* CHECK IF LAST POSITION OF NEW PASSWORD IS NUMERIC */
 IF COND(NEWPW &NPLEN 1) = '0') THEN(GOTO ERROR1)
 IF COND(NEWPW &NPLEN 1) = '1') THEN(GOTO ERROR1)
 IF COND(NEWPW &NPLEN 1) = '2') THEN(GOTO ERROR1)
 IF COND(NEWPW &NPLEN 1) = '3') THEN(GOTO ERROR1)
 IF COND(NEWPW &NPLEN 1) = '4') THEN(GOTO ERROR1)
 IF COND(NEWPW &NPLEN 1) = '5') THEN(GOTO ERROR1)
 IF COND(NEWPW &NPLEN 1) = '6') THEN(GOTO ERROR1)
 IF COND(NEWPW &NPLEN 1) = '7') THEN(GOTO ERROR1)
 IF COND(NEWPW &NPLEN 1) = '8') THEN(GOTO ERROR1)
 IF COND(NEWPW &NPLEN 1) = '9') THEN(GOTO ERROR1)

 /* CHECK IF PASSWORD CONTAINS USER PROFILE NAME        */
 CHGVAR &UNLEN VALUE(1)
 LOOP2:      /* FIND LENGTH OF USER NAME */
  IF COND(UNAME &UNLEN 1) *NE ' ') THEN(DO)
    CHGVAR &UNLEN VALUE(&UNLEN + 1)
    IF COND(&UNLEN = 11) THEN(GOTO ELOOP2)
    GOTO LOOP2
  ENDDO
```

```
ELOOP2:
 CHGVAR &UNLEN VALUE(&UNLEN - 1)


/* CHECK FOR USER NAME IN NEW PASSWORD            */
IF COND(&UNLEN *GT &NPLEN) THEN(GOTO ELOOP3)
CHGVAR &INDX VALUE(1)
LOOP3:
  IF COND(NEWPW &INDX &UNLEN) = UNAME 1 &UNLEN))+
     THEN(GOTO ERROR2)
  IF COND((&INDX + &UNLEN + 1) *LT 128) THEN(DO)
     CHGVAR &INDX VALUE(&INDX + 1)
     GOTO LOOP3
  ENDDO
ELOOP3:

/* La nuova parola d'ordine è valida                    */
GOTO DONE

ERROR1:  /* NEW PASSWORD ENDS IN NUMERIC CHARACTER */
 CHGVAR &RTN  VALUE('3') /* reject */
 SNDPGMMSG TOPGMQ(*PRV) MSGTYPE(*ESCAPE) MSGID(PWD0001) MSGF(QSYS/PWDERRORS)
 GOTO DONE

ERROR2:  /* NEW PASSWORD CONTAINS USER NAME */
 CHGVAR &RTN  VALUE('3') /* reject */
 SNDPGMMSG TOPGMQ(*PRV) MSGTYPE(*ESCAPE) MSGID(PWD0002) MSGF(QSYS/PWDERRORS)
 GOTO DONE

DONE:
ENDPGM
```

Valori di sistema che verificano il controllo

Il controllo dell'attività di sistema è un aspetto importante della sicurezza del sistema in quanto contribuisce a rilevare intrusioni e uso improprio del sistema. È possibile utilizzare valori di sistema specifici per verificare il controllo sul sistema operativo i5/OS .

Panoramica:

Scopo: specificare i valori di sistema che verificano il controllo della sicurezza sul sistema.

Modalità:
WRKSYSVAL *SEC (Comando Gestione valore di sistema)

Autorizzazione:
*AUDIT

Voce di giornale:
SV

Nota: Le modifiche diventano effettive immediatamente. IPL non richiesto.

Questi valori di sistema verificano il controllo sul sistema:

QAUDCTL
Controllo

QAUDENDACN
Azione fine controllo

QAUDFRCLVL
Livello forzatura controllo

QAUDLVL
Livello di controllo

QAUDLVL2
Estensione livello controllo

QCRTOBJAUD
Creazione controllo predefinito

Controllo (QAUDCTL)

valore di sistema controllo (QAUDCTL) stabilisce se viene eseguito il controllo.

Il valore di sistema opera come funzione di attivazione e disattivazione per le seguenti operazioni:

- Valori di sistema QAUDLVL e QAUDLVL2
- Il controllo definito per gli oggetti che utilizzano i comandi CHGOBJAUD (Modifica controllo oggetto), CHGAUD (Modifica valore di controllo) e CHGDLOAUD (Modifica controllo DLO)
- Il controllo definito per gli utenti che utilizzano il comando CHGUSRAUD (Modifica controllo utente)

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

È possibile specificare più di un valore per il valore di sistema QAUDCTL, a meno che non venga specificato *NONE.

Tabella 47. Valori possibili per il valore di sistema QAUDCTL

***NONE**	Non viene eseguito alcun controllo per oggetti e azioni dell'utente.
***NOTAVL**	Questo valore viene visualizzato per indicare che il valore di sistema non è disponibile per l'utente poiché tale utente non dispone dell'autorizzazione speciale *AUDIT o *ALLOBJ. Non è possibile impostare il valore di sistema su questo valore.
***OBJAUD**	Il controllo viene eseguito per gli oggetti che sono stati selezionati utilizzando i comandi CHGOBJAUD, CHGDLOAUD o CHGAUD.
***AUDLVL**	Il controllo viene eseguito per le funzioni selezionate sui valori di sistema QAUDLVL e QAUDLVL2 e sul parametro AUDLVL per i singoli profili utente. Il livello di controllo di un utente viene specificato utilizzando il comando CHGUSRAUD (Modifica controllo utente).
***NOQTEMP**	Il controllo non viene eseguito per la maggior parte delle azioni se l'oggetto si trova nella libreria QTEMP. Consultare il Capitolo 9, "Controllo della sicurezza su System i", a pagina 275 per ulteriori dettagli. È necessario specificare questo valore con *OBJAUD o *AUDLVL.
	Consultare "Pianificazione del controllo sicurezza" a pagina 282 per una descrizione completa del processo di controllo eseguito sul sistema.

Azione fine controllo (QAUDENDACN)

Il valore di sistema QAUDENDACN (Azione fine controllo) determina l'azione che il sistema deve eseguire nel caso in cui il controllo fosse attivo e il sistema non fosse in grado di scrivere le voci sul giornale di controllo.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 48. Valori possibili per il valore di sistema QAUDENDACN:

***NOTAVL**	Questo valore viene visualizzato per indicare che il valore di sistema non è disponibile per l'utente poiché tale utente non dispone dell'autorizzazione speciale *AUDIT o *ALLOBJ. Non è possibile impostare il valore di sistema su questo valore.
***NOTIFY**	Il messaggio CPI2283 viene inviato alle code messaggi QSYSOPR e QSYSMSG (qualora esistano) ogni ora fino a quando il controllo non viene riavviato con esito positivo. Il valore di sistema QAUDCTL è impostato su *NONE per impedire al sistema di tentare di scrivere voci di giornale di controllo aggiuntive. L'elaborazione sul sistema prosegue. Se si esegue un IPL prima di riavviare il controllo, il messaggio CPI2284 viene inviato alle code messaggi QSYSOPR e QSYSMSG durante l'esecuzione dell'IPL.
***PWRDWNSYS**	Se il sistema non è in grado di scrivere una voce di giornale di controllo, il sistema si spegne immediatamente. L'unità di sistema visualizza l'SRC (system reference code) B900 3D10. Una volta riacceso il sistema, questo opera con lo stato limitato. Ciò indica che il sottosistema di controllo si trova nello stato limitato, nessun altro sottosistema è attivo e il collegamento può essere eseguito solo dalla console. Il valore di sistema QAUDCTL è impostato su *NONE. L'utente che si collega alla console per completare l'IPL deve disporre dell'autorizzazione speciale *ALLOBJ e *AUDIT.

Valore consigliato: Per la maggior parte delle installazioni, il valore consigliato è *NOTIFY. Se le normative di sicurezza non richiedono alcuna esecuzione sul sistema senza il controllo, l'utente deve selezionare *PWRDWNSYS.

Il sistema non è in grado di scrivere le voci di giornale di controllo solo in circostanza rare e insolite. Tuttavia, se questo dovesse verificarsi e il valore di sistema QAUDENDACN è *PWRDWNSYS, il sistema si spegne in modo anomalo. Questo potrebbe dare luogo ad un IPL (initial program load) di lunga durata quando si riattiva il sistema.

Livello forzatura controllo (QAUDFRCLVL)

Il valore di sistema livello forzatura controllo (QAUDFRCLVL) determina la frequenza con la quale forzate le nuove voci di giornale di controllo dalla memoria alla memoria ausiliaria. Questo valore di sistema controlla la quantità di dati di controllo che potrebbero andare persa in caso di interruzione anomala del sistema.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 49. Valori possibili per il valore di sistema QAUDFRCLVL

***NOTAVL**	Questo valore viene visualizzato per indicare che il valore di sistema non è disponibile per l'utente poiché tale utente non dispone dell'autorizzazione speciale *AUDIT o *ALLOBJ. Non è possibile impostare il valore di sistema su questo valore.
***SYS**	Il sistema stabilisce quando le voci di giornale vengono scritte sulla memoria ausiliaria in base alle prestazioni del sistema interno.
numero-di-record	Specificare un numero compreso tra 1 e 100 per determinare la quantità di voci di controllo che possono essere accumulate in memoria prima che vengano scritte sulla memoria ausiliaria. Minore è il numero e maggiore è l'effetto sulle prestazioni di sistema.

Valore consigliato: *SYS fornisce le migliori prestazioni di controllo. Tuttavia, se l'installazione richiede che nessuna voce venga persa in caso di interruzione anomala del sistema, è necessario specificare 1. Se si specifica 1, è possibile che le prestazioni ne risentano negativamente.

Livello di controllo (QAUDLVL)

Il valore di sistema livello di controllo (QAUDLVL) insieme al valore di sistema QAUDLVL2 stabilisce quali eventi relativi alla sicurezza registrare sul giornale di controllo della sicurezza (QAUDJRN) per tutti gli utenti del sistema.

È possibile specificare più di un valore per il valore di sistema QAUDLVL, a meno che non venga specificato *NONE.

Affinché il valore di sistema QAUDLVL diventi effettivo, il valore di sistema QAUDCTL deve comprendere *AUDLVL.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 50. Valori possibili per il valore di sistema QAUDLVL

***NONE**	Nessun evento controllato dai valori di sistema QAUDLVL o QAUDLVL2 registrati. Gli eventi vengono registrati per i singoli utenti in base al valore AUDLVL dei profili utente.
***NOTAVL**	Questo valore viene visualizzato per indicare che il valore di sistema non è disponibile per l'utente poiché tale utente non dispone dell'autorizzazione speciale *AUDIT o *ALLOBJ. Non è possibile impostare il valore di sistema su questo valore.
***AUDLVL2**	I valori di sistema QAUDLVL e QAUDLVL2 verranno utilizzati per stabilire le azioni di sicurezza da controllare.
***ATNEVT**	Vengono registrati gli eventi di attenzione.
***AUTFAIL**	Vengono registrati gli eventi di errore dell'autorizzazione.
***CREATE**	Vengono registrate le operazioni di creazione degli oggetti.
***DELETE**	Vengono registrate le operazioni di cancellazione degli oggetti.
***JOBBAS**	Vengono controllate le funzioni di base del lavoro.
***JOBCHGUSR**	Vengono controllate le modifiche apportate al profilo utente attivo di un sottoprocesso o ai relativi profili del gruppo.
***JOBDTA**	Vengono registrate le azioni che coinvolgono un lavoro. *JOBDTA è composto da due valori, *JOBBAS e *JOBCHGUSR, in modo da consentire all'utente di personalizzare al meglio il proprio controllo.Se vengono specificati entrambi i valori, l'utente ottiene lo stesso controllo che se fosse specificato solo *JOBDTA.
***NETBAS**	Vengono controllate le funzioni di base di rete.
***NETCLU**	Vengono controllate le operazioni di gruppi di risorse cluster e del cluster.

Tabella 50. Valori possibili per il valore di sistema QAUDLVL (Continua)

***NETCMN**	Vengono controllare le funzioni di comunicazione e di rete. *NETCMN è composto da diversi valori in modo da consentire all'utente di personalizzare al meglio il proprio controllo. I valori seguenti compongono *NETCMN: *NETBAS *NETCLU *NETFAIL *NETSCK
***NETFAIL**	Vengono controllati gli errori di rete.
***NETSCK**	Vengono controllate le attività socket.
***OBJMGT**	Vengono registrate le operazioni di ridenominazione e di spostamento degli oggetti.
***OFCSRV**	Vengono registrate le modifiche apportate all'indirizzario di distribuzione del sistema e le azioni di posta d'ufficio.
***OPTICAL**	Viene registrato l'utilizzo dei volumi ottici.
***PGMADP**	Viene registrata la ricezione di un'autorizzazione da un programma che adotta l'autorizzazione.
***PGMFAIL**	Vengono registrate le violazioni all'integrità del sistema.
***PRTDTA**	Vengono registrati la stampa di un file di spool, l'invio dell'emissione direttamente ad una stampante e l'invio di una emissione ad una stampante remota.
***SAVRST**	Vengono registrate le operazioni di salvataggio e di ripristino.
***SECCFG**	Viene controllata la configurazione della sicurezza.
***SECDIRSRV**	Vengono controllate le modifiche o gli aggiornamenti durante le funzioni del servizio indirizzario.
***SECIPC**	Vengono controllate le modifiche apportate alle comunicazioni tra processi.
***SECNAS**	Vengono controllate le azioni del servizio di autenticazione della rete.
***SECRUN**	Vengono controllate le funzioni di tempo di esecuzione della sicurezza.
***SECSCKD**	Vengono controllati i descrittori socket.
***SECURITY**	Vengono registrate le funzioni relative alla sicurezza. *SECURITY è composto da diversi valori in modo da consentire all'utente di personalizzare al meglio il proprio controllo. I valori seguenti compongono *SECURITY: *SECCFG *SECDIRSRV *SECIPC *SECNAS *SECRUN *SECSCKD *SECVFY *SECVLDL
***SECVFY**	Vengono controllate le funzioni di utilizzo della verifica.
***SECVLDL**	Vengono controllate le modifiche agli oggetti dell'elenco di convalida.
***SERVICE**	Viene registrato l'utilizzo dei programmi di manutenzione.
***SPLFDTA**	Vengono registrate le azioni eseguite sui file di spool.
***SYSMGT**	Viene registrato l'utilizzo delle funzioni di gestione sistemi.

Riferimenti correlati

"Pianificazione del controllo delle azioni" a pagina 282
I valori di sistema QAUDCTL (controllo), QAUDLVL (livello di controllo), QAUDLVL2 (estensione livello di controllo) e il parametro AUDLVL (controllo azione) nei profili utente collaborano per controllare il controllo azione.

Estensione livello di controllo (QAUDLVL2)

Il valore di sistema estensione livello di controllo (QAUDLVL2) è richiesto quando sono necessari più di sedici valori di controllo.

Specificando *AUDLVL2 come uno dei valori nel valore di sistema QAUDLVL, il sistema controllerà anche i valori di controllo nel valore di sistema QAUDLVL2. È possibile specificare più di un valore per il valore di sistema QAUDLVL2, a meno che non venga specificato *NONE. Affinché il valore di sistema QAUDLVL2 diventi effettivo, il valore di sistema QAUDCTL deve comprendere *AUDLVL e il valore di sistema QAUDLVL deve comprendere *AUDLVL2.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 51. Valori possibili per il valore di sistema QAUDLVL2

***NONE**	Nessun valore di controllo contenuto in questo valore di sistema.
***NOTAVL**	Questo valore viene visualizzato per indicare che il valore di sistema non è disponibile per l'utente poiché tale utente non dispone dell'autorizzazione speciale *AUDIT o *ALLOBJ. Non è possibile impostare il valore di sistema su questo valore.
***ATNEVT**	Vengono registrati gli eventi di attenzione.
***AUTFAIL**	Vengono registrati gli eventi di errore dell'autorizzazione.
***CREATE**	Vengono registrate le operazioni di creazione degli oggetti.
***DELETE**	Vengono registrate le operazioni di cancellazione degli oggetti.
***JOBBAS**	Vengono controllate le funzioni di base del lavoro.
***JOBCHGUSR**	Vengono controllate le modifiche apportate al profilo utente attivo di un sottoprocesso o ai relativi profili del gruppo.
***JOBDTA**	Vengono registrate le azioni che coinvolgono un lavoro. *JOBDTA è composto da due valori, *JOBBAS e *JOBCHGUSR, in modo da consentire all'utente di personalizzare al meglio il proprio controllo.Se vengono specificati entrambi i valori, l'utente ottiene lo stesso controllo che se fosse specificato solo *JOBDTA.
***NETBAS**	Vengono controllate le funzioni di base di rete.
***NETCLU**	Vengono controllate le operazioni di gruppi di risorse cluster e del cluster.
***NETCMN**	Vengono controllare le funzioni di comunicazione e di rete. *NETCMN è composto da diversi valori in modo da consentire all'utente di personalizzare al meglio il proprio controllo. I valori seguenti compongono *NETCMN: *NETBAS *NETCLU *NETFAIL *NETSCK

Tabella 51. Valori possibili per il valore di sistema QAUDLVL2 (Continua)

***NETFAIL**	Vengono controllati gli errori di rete.
***NETSCK**	Vengono controllate le attività socket.
***OBJMGT**	Vengono registrate le operazioni di ridenominazione e di spostamento degli oggetti.
***OFCSRV**	Vengono registrate le modifiche apportate all'indirizzario di distribuzione del sistema e le azioni di posta d'ufficio.
***OPTICAL**	Viene registrato l'utilizzo dei volumi ottici.
***PGMADP**	Viene registrata la ricezione di un'autorizzazione da un programma che adotta l'autorizzazione.
***PGMFAIL**	Vengono registrate le violazioni all'integrità del sistema.
***PRTDTA**	Vengono registrati la stampa di un file di spool, l'invio dell'emissione direttamente ad una stampante e l'invio di una emissione ad una stampante remota.
***SAVRST**	Vengono registrate le operazioni di ripristino.
***SECCFG**	Viene controllata la configurazione della sicurezza.
***SECDIRSRV**	Vengono controllate le modifiche o gli aggiornamenti durante le funzioni del servizio indirizzario.
***SECIPC**	Vengono controllate le modifiche apportate alle comunicazioni tra processi.
***SECNAS**	Vengono controllate le azioni del servizio di autenticazione della rete.
***SECRUN**	Vengono controllate le funzioni di tempo di esecuzione della sicurezza.
***SECSCKD**	Vengono controllati i descrittori socket.
***SECURITY**	Vengono registrate le funzioni relative alla sicurezza. *SECURITY è composto da diversi valori in modo da consentire all'utente di personalizzare al meglio il proprio controllo. I valori seguenti compongono *SECURITY: *SECCFG *SECDIRSRV *SECIPC *SECNAS *SECRUN *SECSCKD *SECVFY *SECVLDL
***SECVFY**	Vengono controllate le funzioni di utilizzo della verifica.
***SECVLDL**	Vengono controllate le modifiche agli oggetti dell'elenco di convalida.
***SERVICE**	Viene registrato l'utilizzo dei programmi di manutenzione.
***SPLFDTA**	Vengono registrate le azioni eseguite sui file di spool.
***SYSMGT**	Viene registrato l'utilizzo delle funzioni di gestione sistemi.

Riferimenti correlati

"Pianificazione del controllo delle azioni" a pagina 282
I valori di sistema QAUDCTL (controllo), QAUDLVL (livello di controllo), QAUDLVL2 (estensione livello di controllo) e il parametro AUDLVL (controllo azione) nei profili utente collaborano per controllare il controllo azione.

Controllo dei nuovi oggetti (QCRTOBJAUD)

Il valore di sistema controllo dei nuovi oggetti (QCRTOBJAUD) si utilizza per stabilire il valore di controllo di un nuovo oggetto, se il valore predefinito del controllo creazione oggetto per la libreria o per l'indirizzario del nuovo oggetto è impostato su *SYSVAL.

Il valore di sistema QCRTOBJAUD rappresenta inoltre il valore di controllo predefinito per i nuovi documenti che non dispongono di una cartella.

Ad esempio, il valore CRTOBJAUD per la libreria CUSTLIB è *SYSVAL. Il valore QCRTOBJAUD è *CHANGE. Se si crea un nuovo oggetto nella libreria CUSTLIB, il relativo valore di controllo dell'oggetto viene impostato automaticamente su *CHANGE. È possibile modificare il valore di controllo dell'oggetto utilizzando il comando CHGOBJAUD o CHGAUD.

Nota: questo valore di sistema è un valore limitato. Consultare Valori di sistema Sicurezza per dettagli su come limitare le modifiche ai valori di sistema di sicurezza e per un elenco completo dei valori di sistema limitati.

Tabella 52. Valori possibili per il valore di sistema QCRTOBJAUD:

***NONE**	Nessun controllo eseguito sull'oggetto.
***NOTAVL**	Questo valore viene visualizzato per indicare che il valore di sistema non è disponibile per l'utente poiché tale utente non dispone dell'autorizzazione speciale *AUDIT o *ALLOBJ. Non è possibile impostare il valore di sistema su questo valore.
***USRPRF**	Il controllo dell'oggetto varia in base al valore nel profilo dell'utente che accede all'oggetto.
***CHANGE**	Un record di controllo viene scritto ogni volta che l'oggetto viene modificato in modo significativo dal punto di vista della sicurezza.
***ALL**	Un record di controllo viene scritto per ogni azione di sicurezza significativa che coinvolge il contenuto dell'oggetto. Un record di controllo viene scritto anche se l'oggetto viene modificato in modo significativo dal punto di vista della sicurezza.

Valore consigliato: il valore selezionato varia in base ai requisiti di controllo dell'installazione. "Pianificazione del controllo dell'accesso agli oggetti" a pagina 308 fornisce maggiori informazioni sui metodi per impostare il controllo dell'oggetto sul sistema. È possibile controllare il valore di controllo a livello dell'indirizzario con il parametro CRTOBJAUD sul comando CRTDIR (Creazione indirizzario) e il valore *CRTOBJAUD sul comando CHGATR (Modifica attributo). Inoltre, è possibili controllare il valore di controllo a livello della libreria con il parametro CRTOBJAUD con il comando CRTLIB e il comando CHGLIB.

Capitolo 4. Profili utente

I profili utente rappresentano uno strumento flessibile e potente. La loro creazione può facilitare notevolmente la protezione e la personalizzazione del sistema per gli utenti.

Panoramica:

Scopo: creare e conservare i profili utente e i profili di gruppo sul sistema.

Modalità:

Comando WRKUSRPRF (gestione profili utente)

Comando CHGUSRAUD (Modifica controllo utente)

Autorizzazione:

Autorizzazione speciale *SECADM

Autorizzazione speciale *AUDIT per modificare il controllo dell'utente

Voce di giornale:

AD per le modifiche al controllo dell'utente

CO per la creazione di un profilo utente

CP per le modifiche ai profili utente

DO per l'eliminazione di un profilo utente

ZC per le modifiche ad un profilo utente non importante ai fini della sicurezza

Concetti correlati

"Profili utente" a pagina 4
Sul sistema operativo i5/OS, ogni profilo utente ha un profilo utente.

Ruoli del profilo utente

Un profilo utente contiene le parole d'ordine di un utente, l'elenco di autorizzazioni speciali assegnate ad un utente e gli oggetti di proprietà dell'utente.

Un profilo utente ricopre diversi ruoli sul sistema:

- Contiene le informazioni relative alla sicurezza che controllano come l'utente si collega al sistema, le operazioni consentite all'utente una volta collegato e come tali operazioni vengono controllate.
- Contiene informazioni create per la personalizzazione del sistema e il relativo adattamento all'utente.
- Si tratta di uno strumento di gestione e di ripristino del sistema operativo. Il profilo utente contiene le informazioni sugli oggetti di proprietà dell'utente e su tutte le autorizzazioni private sugli oggetti.
- Il nome del profilo utente identifica i lavori dell'utente e l'emissione di stampa.

Se il valore di sistema del livello di sicurezza (QSECURITY) sul sistema è 10, il sistema crea automaticamente un profilo utente quando si tenta di collegarsi con un ID utente che ancora non esiste sul sistema. "Valori predefiniti per i profili utente" a pagina 341 in Appendice B, "Profili utente forniti da IBM", a pagina 341 mostra i valori assegnati quando il sistema crea un profilo utente.

Se il valore di sistema QSECURITY sul sistema è 20 o superiore, è necessario che il profilo utente esista già prima che un utente possa collegarsi.

Profili di gruppo

Un profilo di gruppo è un tipo speciale di profilo utente che fornisce la stessa autorizzazione a un gruppo di utenti.

Un profilo di gruppo ha due scopi sul sistema:

Strumento di sicurezza
Un profilo di gruppo fornisce la metodologia per l'organizzazione delle autorizzazioni sul sistema e la loro condivisione tra gli utenti. È possibile definire le autorizzazioni oggetto oppure le autorizzazioni speciali per i profili di gruppo piuttosto che per i singoli profili utente. Un utente può essere un membro di un massimo di 16 profili di gruppo.

Strumento di personalizzazione
Un profilo di gruppo può essere utilizzato come modello per la creazione di singoli profili utente. La maggior parte delle persone appartenenti allo stesso gruppo ha le stesse esigenze di personalizzazione, ad esempio il menu iniziale e la stampante predefinita. È possibile definirle nel profilo di gruppo e copiare quindi il profilo di gruppo per creare profili utente individuali.

L'utente crea profili di gruppo seguendo le stesse procedure utilizzate per la creazione dei singoli profili. Il sistema riconosce un profilo di gruppo quando gli si aggiunge il primo membro. A questo punto, il sistema imposta le informazioni nel profilo che indica che si tratta di un profilo di gruppo. Il sistema, inoltre, genera un numero identificativo gruppo (GID, Group Identification Number) per il profilo. È inoltre possibile definire un profilo come un profilo di gruppo nel momento in cui lo si crea, specificando un valore nel parametro gid. "Pianificazione dei profili di gruppo" a pagina 256 visualizza un esempio su come impostare un profilo di gruppo.

Campi del parametro profilo utente

Questo argomento fornisce informazioni dettagliate sui campi del parametro per profili utente visualizzati sulla richiesta comandi Creazione profilo utente.

Quando si crea un profilo utente, il sistema fornisce al profilo queste autorizzazioni: *OBJMGT, *CHANGE. Queste autorizzazioni sono necessarie alle funzioni del sistema e non dovrebbero essere rimosse.

Molti pannelli del sistema hanno diverse versioni, definite *livelli di assistenza*, per soddisfare le necessità di utenti differenti:

- Livello di assistenza di base; contiene un numero minore di informazioni e non utilizza la terminologia tecnica.
- Livello di assistenza intermedio; visualizza un numero maggiore di informazioni e utilizza termini tecnici.
- Livello di assistenza avanzato; utilizza termini tecnici e visualizza la quantità massima di dati non visualizzando sempre le informazioni relative ai tasti funzione e alle opzioni.

Le sezioni seguenti mostrano quali campi del profili utente vengono richiamati sia sul pannello del livello di assistenza di base che su quello di assistenza intermedio.

Titolo campo
Il titolo della sezione mostra come viene visualizzato il nome del campo sulla richiesta comandi Creazione profilo utente. Il titolo si visualizza quando viene creato un profilo utente con livello di assistenza intermedio o il comando CRTUSRPRF Creazione profilo utente.

Richiesta di aggiunta utente:
Questa opzione mostra come viene visualizzato il nome del campo sul pannello Aggiunta utente ed altri pannelli del profilo utente che utilizzano il livello di assistenza di base. Il pannello del livello di assistenza di base mostra una sottoserie dei campi nel profilo utente. *Non visualizzato*

indica che il campo non appare sul pannello del livello di assistenza di base. Quando si utilizza il pannello Aggiunta utente per creare un profilo utente, i valori predefiniti vengono vengono utilizzati per tutti i campi che non vengono visualizzati.

Parametro CL:
L'utente utilizza il nome del parametro CL per un campo in un programma CL oppure quando si immette un comando del profilo utente senza richiesta.

Lunghezza:
Se si utilizza il comando RTVUSRPRF (Richiamo profilo utente) in un programma CL, questa è la lunghezza che dovrebbe essere utilizzata per definire il campo associato al parametro.

Autorizzazione:
Se un campo fa riferimento a un oggetto separato, come ad esempio una libreria o un programma, all'utente vengono comunicati i requisiti di autorizzazione per l'oggetto. Per specificare l'oggetto quando si crea o si modifica un profilo utente, è necessario disporre dell'autorizzazione corrispondente elencata. Per collegarsi utilizzando il profilo, l'utente necessita dell'autorizzazione elencata. Ad esempio, se si crea il profilo utente USERA con la descrizione lavoro JOBD1, è necessario disporre dell'autorizzazione *USE su JOBD1. USERA deve disporre dell'autorizzazione *USE su JOBD1 per collegarsi con esito positivo con il profilo.

Inoltre, ogni sezione descrive i possibili valori per il campo e un valore consigliato.

Nome profilo utente

Il nome del profilo utente identifica l'utente sul sistema. Questo nome del profilo utente è noto come ID utente. È il nome immesso dall'utente nella richiesta Utente sul pannello Accesso.

Richiesta di aggiunta utente:
Profilo

Parametro CL:
USRPRF

Lunghezza:
10

Il nome del profilo utente può avere una lunghezza massima di 10 caratteri. I caratteri possono essere:

- Lettere (da A a Z)
- Numeri (da 0 a 9)
- Questi caratteri speciali: cancelletto (#), dollaro ($), sottolineatura (_), chiocciola (@).

Il nome del profilo utente non può iniziare con un numero.

Note:

- il pannello Aggiunta utente prevede un nome utente composto da soli otto caratteri.
- è possibile creare un profilo utente in modo che quando un utente si collega, l'ID utente è composto da soli numeri. Per creare un profilo di questo tipo, specificare una Q come primo carattere, ad esempio Q12345. Un utente può quindi collegarsi immettendo 12345 o Q12345 per la richiesta *Utente* sul pannello Accesso.

Per ulteriori informazioni sulla specifica dei nomi sul sistema, consultare l'argomento CL programming.

Suggerimenti per la denominazione dei profili utente: tenere presenti le seguenti considerazioni quando si scelgono i nomi dei profili utente:

- Un nome del profilo utente può essere lungo fino a 10 caratteri. Alcuni metodi delle comunicazioni limitano la lunghezza dell'ID utente a otto caratteri. Anche il pannello Aggiunta utente limita la lunghezza del nome del profilo utente a otto caratteri.

- Utilizzare uno schema di denominazione per faciliti la memorizzazione degli ID utente.
- Il sistema non distingue fra lettere maiuscole e minuscole contenute nel nome del profilo utente. Se si immettono caratteri alfabetici in minuscolo nella stazione di lavoro, il sistema li converte in caratteri maiuscoli.
- I pannelli e gli elenchi utilizzati per gestire i profili utente visualizzano i profili utente in ordine alfabetico in base al nome del profilo utente.
- Evitare l'utilizzo dei caratteri speciali nei nomi dei profili utente. I caratteri speciali potrebbero causare problemi con la correlazione delle tastiere per determinate stazioni di lavoro o con le versioni delle lingue nazionali del programma su licenza i5/OS.

Una tecnica per assegnare i nomi dei profili utente consiste nell'utilizzare i primi sette caratteri del cognome seguiti dal primo carattere del primo nome. Ad esempio:

Nome utente	Nome profilo utente
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Harrisburg, Keith	HARRISBK
Jones, Sharon	JONESS
Jones, Keith	JONESK

Suggerimenti per la denominazione dei profili gruppo: per identificare facilmente i profili gruppo sul sistema, utilizzare una convenzione di denominazione. Iniziare tutti i nomi dei profili gruppo con gli stessi caratteri, ad esempio `GRP` (per gruppo) o `DPT` (per dipartimento).

Parola d'ordine

La parola d'ordine viene utilizzata per verificare l'autorizzazione di un utente per collegarsi al sistema. È necessario specificare un ID utente e una parola d'ordine per collegarsi quando la sicurezza della parola d'ordine è attiva (il valore di sistema QSECURITY è 20 o superiore).

Richiesta di aggiunta utente:
Parola d'ordine

Parametro CL:
PASSWORD

Lunghezza:
128

Le parole d'ordine possono essere composte da un massimo di 10 caratteri quando il valore di sistema QPWDLVL è impostato su 0 o 1. Le parole d'ordine possono essere composte da un massimo di 128 caratteri quando il valore di sistema QPWDLVL è impostato su 2 o 3.

Quando il valore di sistema Livello parola d'ordine (QPWDLVL) è impostato su 0 o 1, le regole per la specifica delle parole d'ordine sono uguali a quelle utilizzate per i nomi dei profili utente. Quando il primo carattere della parola d'ordine è una Q e il secondo carattere è un numero, la lettera Q può essere omessa sul pannello di accesso. Se un utente specifica Q12345 come parola d'ordine sul pannello Modifica parola d'ordine, l'utente può specificare 12345 o Q12345 come parola d'ordine sul pannello di accesso. Quando QPWDLVL è impostato su 2 o 3, l'utente deve specificare la parola d'ordine Q12345 sul pannello di accesso se il profilo utente è stato creato con una parola d'ordine Q12345. Una parola d'ordine composta da soli numeri è concessa quando QPWDLVL è impostato su 2 o 3, ma la parola d'ordine del profilo utente deve essere creata con soli numeri.

Quando il valore di sistema Livello parola d'ordine (QPWDLVL) è impostato su 2 o 3, la parola d'ordine è sensibile al maiuscolo e minuscolo e può contenere qualsiasi caratteri, compresi gli spazi vuoti. Tuttavia, la parola d'ordine non può iniziare con un asterisco ('*') e gli spazi finali vengono eliminati.

Nota: le parole d'ordine possono essere create utilizzando caratteri double-byte. Tuttavia, una parola d'ordine contenente caratteri double-byte non può essere utilizzata per accedere mediante la schermata di accesso del sistema. Le parole d'ordine contenenti caratteri double byte possono essere create dai comandi CRTUSRPRF e CHGUSRPRF e possono essere inoltrate alle API di sistema che supportano il parametro della parola d'ordine.

La codifica a senso unico viene utilizzata per memorizzare la parola d'ordine sul sistema. Se l'utente dimentica la parola d'ordine, il responsabile della riservatezza può utilizzare il comando Modifica profilo utente (CHGUSRPRF) per assegnare una parola d'ordine temporanea e impostare tale parola d'ordine su scaduta, richiedendo all'utente di assegnarne una nuova al successivo accesso.

È possibile impostare i valori di sistema per controllare le parole d'ordine assegnate dagli utenti. I valori di sistema per la composizione della parola d'ordine si applicano solo quando un utente modifica una parola d'ordine utilizzando il comando Modifica parola d'ordine (CHGPWD), l'opzione Modifica parola d'ordine dal menu ASSIST o la API QSYCHGPW. Un utente non può impostare la parola d'ordine uguale al nome del profilo utente utilizzando il comando CHGPWD, il menu ASSIST o l'API QSYCHGPW nelle seguenti condizioni.

- Il valore di sistema QPWDRULES è *PWDSYSVAL e il valore di sistema Lunghezza minima parola d'ordine (QPWDMINLEN) non è 1.
- Il valore di sistema QPWDRULES è *PWDSYSVAL e il valore di sistema Lunghezza massima parola d'ordine (QPWDMAXLEN) non è 10.
- Il valore di sistema QPWDRULES è *PWDSYSVAL e gli altri valori di sistema di composizione della parola d'ordine sono stati modificati dai valori predefiniti.

Consultare l'argomento "Valori di sistema che si applicano alle parole d'ordine" a pagina 50 per informazioni sull'impostazione dei valori di sistema relativi alla composizione della parola d'ordine.

Tabella 53. Valori possibili per PASSWORD:

***USRPRF**	La parola d'ordine per questo utente è uguale al nome del profilo utente. Quando il valore di sistema Livello parola d'ordine (QPWDLVL) è impostato su 2 o 3, la parola d'ordine rappresenta il valore in maiuscolo del nome del profilo utente. Per il profilo JOHNDOE, la parola d'ordine è JOHNDOE e non johndoe.
***NONE**	Nessuna parola d'ordine assegnata a questo profilo utente. L'accesso non è consentito con questo profilo utente. È possibile inoltrare un lavoro batch utilizzando un profilo utente con la parola d'ordine *NONE se si dispone dell'autorizzazione corretta per il profilo utente.
parola d'ordine utente	Una stringa di carattere (128 caratteri o meno).

Suggerimenti per le parole d'ordine:

- Impostare la parola d'ordine per un profilo di gruppo su *NONE. Questo impedisce a chiunque di collegarsi con il profilo gruppo.
- Quando si crea un singolo profilo utente, impostare la parola d'ordine su un valore iniziale e richiedere l'assegnazione di una nuova parola d'ordine all'accesso dell'utente (impostare parola d'ordine scaduta su *YES). La parola d'ordine predefinita quando si crea un profilo utente corrisponde al nome del profilo utente.
- Se si sceglie una parola d'ordine predefinita o banale durante la creazione di un nuovo profilo utente, accertarsi che l'utente intenda collegarsi immediatamente. Se si prevede un ritardo nella connessione

dell'utente, impostare lo stato del nuovo profilo utente su *DISABLED. Modificare lo stato in *ENABLED quando l'utente è pronto all'accesso. Questo consente di proteggere un nuovo profilo utilizzo da parte di utenti non autorizzati.

- Utilizzare i valori di sistema per la composizione della parola d'ordine per impedire agli utenti di assegnare parole d'ordine banali.
- Alcuni metodi di comunicazione inviano le parole d'ordine tra i sistemi e limitano la lunghezza della parola d'ordine e i caratteri contenuti nelle parole d'ordine. Se il sistema comunica con altri sistemi, utilizzare il valore di sistema QPWDMAXLEN o QPWDRULES per limitare la lunghezza delle parole d'ordine. Ai livelli della parola d'ordine 0 e 1, il valore di sistema QPWDLMTCHR può essere utilizzato per specificare caratteri che non possono essere utilizzati nelle parole d'ordine.

Impostazione scadenza parola d'ordine

Il campo *Impostazione scadenza parola d'ordine* consente all'amministratore della riservatezza di indicare nel profilo utente che la parola d'ordine dell'utente è scaduta e deve essere modificata al successivo accesso dell'utente.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
PWDEXP

Lunghezza:
4

Questo valore viene reimpostato su *NO quando si modifica la parola d'ordine. L'utente può modificare la parola d'ordine utilizzando il comando CHGPWD o CHGUSRPRF oppure la API QSYCHGPW o durante il successivo accesso.

Questo campo può essere utilizzato quando un utente non è in grado di ricordare la parola d'ordine e un amministratore della sicurezza deve assegnarne una nuova. Richiedere ad un utente di modificare la parola d'ordine assegnata dall'amministratore della sicurezza, impedisce all'amministratore della sicurezza di conoscere la nuova parola d'ordine e di collegarsi come l'utente.

Quando la parola d'ordine di un utente è scaduta, l'utente riceve un messaggio in fase di accesso (consultare la "Intervallo scadenza parola d'ordine" a pagina 98). L'utente può premere il tasto Invio per assegnare una nuova parola d'ordine oppure premere il tasto F3 (Fine) per annullare il tentativo di accesso senza assegnare una nuova parola d'ordine. Se l'utente sceglie di modificare la parola d'ordine, viene visualizzato il pannello Modifica parola d'ordine e si esegue la convalida della parola d'ordine per la nuova parola d'ordine.

```
                          Informazioni di accesso
                                                              Sistema:
Parola d'ordine scaduta. Modificare la parola d'ordine per proseguire
con la richiesta di accesso.

Accesso precedente . . . . . . . . . . . . . :   10/30/91  14:15:00
```

Figura 1. Messaggio di scadenza della parola d'ordine

Tabella 54. Valori possibili per PWDEXP:

***NO:**	La parola d'ordine non è impostata su scaduta.
***YES:**	La parola d'ordine è impostata su scaduta.

Suggerimenti: impostare la parola d'ordine su scaduta ogni volta che si crea un nuovo profilo utente o si assegna una parola d'ordine temporanea ad un utente.

Stato

Il valore del campo *Stato* indica se il profilo è valido per l'accesso. Se lo stato del profilo è abilitato, il profilo è valido per l'accesso. Se lo stato del profilo è disabilitato, un utente autorizzato deve abilitare nuovamente il profilo per renderlo valido per l'accesso.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
STATUS

Lunghezza:
10

È possibile utilizzare il comando CHGUSRPRF per abilitare un profilo che è stato disabilitato. È necessario disporre dell'autorizzazione speciale *SECADM e dell'autorizzazione *OBJMGT e *USE sul profilo per modificarne lo stato. "Abilitazione di un profilo utente" a pagina 133 visualizza un esempio di un programma di autorizzazione adottato per consentire ad un operatore di sistema di abilitare un profilo.

Il sistema può disabilitare un profilo dopo un determinato numero di tentativi di verifica della parola d'ordine non corretti con quel profilo, a seconda delle impostazioni dei valori di sistema QMAXSIGN e QMAXSGNACN.

È possibile collegarsi sempre con il profilo QSECOFR (responsabile della riservatezza) sulla console, anche se lo stato di QSECOFR è *DISABLED. Se il profilo utente QSECOFR viene disabilitato, collegarsi come QSECOFR sulla console e immettere `CHGUSRPRF QSECOFR STATUS(*ENABLED)`.

Tabella 55. Valori possibili per STATUS:

***ENABLED**	Il profilo è valido per l'accesso.
***DISABLED**	Il profilo non è valido per l'accesso fino a quando un utente autorizzato non lo abilita di nuovo.

Suggerimenti: impostare lo stato su *DISABLED se si desidera impedire l'accesso con un profilo utente. Ad esempio, è possibile disabilitare il profilo di un utente che si assenterà dal lavoro per un periodo di tempo esteso.

Classe utente

La classe utente viene utilizzata per controllare quali opzioni di menu vengono visualizzate all'utente sui menu i5/OS. Ciò consente di controllare l'accesso utente ad alcune funzioni di sistema.

Richiesta di aggiunta utente:
Tipo di utente

Parametro CL:
USRCLS

Lunghezza:
10

Questo non limita necessariamente l'utilizzo dei comandi. Il campo *Possibilità limitate* controlla se l'utente può immettere i comandi. La classe utente potrebbe non coinvolgere le opzioni visualizzate sui menu forniti da altri programmi su licenza.

Se non si specificano autorizzazioni speciali alla creazione di un profilo utente, la classe utente e il valore di sistema livello di sicurezza (QSECURITY) vengono utilizzati per stabilire le autorizzazioni speciali per l'utente.

Valori possibili per USRCLS: la Tabella 56 mostra le possibili classi utente e a cosa servono le autorizzazioni speciali per ciascuna classe utente. Le voci indicano che l'autorizzazione è assegnata solo ai livelli di sicurezza 10 e 20, a tutti i livelli di sicurezza o a nessuno.

Il valore predefinito per la classe utente è ***USER**.

Tabella 56. Autorizzazioni speciali predefinite per classe utente

Autorizzazione speciale	Classi utente				
	***SECOFR**	***SECADM**	***PGMR**	***SYSOPR**	***USER**
*ALLOBJ	Tutto	10 o 20	10 o 20	10 o 20	10 o 20
*SECADM	Tutto	Tutto			
*JOBCTL	Tutto	10 o 20	10 o 20	Tutto	
*SPLCTL	Tutto				
*SAVSYS	Tutto	10 o 20	10 o 20	Tutto	10 o 20
*SERVICE	Tutto				
*AUDIT	Tutto				
*IOSYSCFG	Tutto				

Suggerimenti: la maggior parte degli utenti non deve eseguire le funzioni di sistema. Impostare la classe utente su *USER, a meno che un utente non debba specificatamente utilizzare le funzioni di sistema.

Livello di assistenza

Il campo *Livello di assistenza* nel profilo utente specifica il livello di assistenza predefinito per l'utente quando si crea il profilo. La piattaforma System i fornisce tre livelli di assistenza: base, intermedio e avanzato.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
ASTLVL

Lunghezza:
10

Per ciascun utente, il sistema tiene traccia dell'ultimo livello di assistenza utilizzato per ciascun pannello del sistema con più di un livello di assistenza. Tale livello viene utilizzato la prossima volta che l'utente richiede quel pannello. Durante il lavoro attivo, un utente può modificare il livello di assistenza per un pannello o un gruppo di pannelli correlati premendo il tasto F21 (Selezione livello assistenza). Il nuovo livello di assistenza per quel pannello viene memorizzato con le informazioni utente.

Specificando il parametro del livello di assistenza (ASTLVL) su un comando non si modifica il livello di assistenza memorizzato per l'utente per il pannello associato.

Se il livello di assistenza nel profilo utente viene modificato utilizzando il comando CHGUSRPRF o il comando Modifica profilo (CHGPRF), i livelli di assistenza memorizzati per tutti i pannelli di quell'utente vengono reimpostati sul nuovo valore.

Ad esempio, si presupponga che il profilo utente USERA venga creato con il livello di assistenza predefinito (di base). La Tabella 57 mostra se USERA utilizza il pannello Gestione profili utente o il pannello Gestione iscrizione utente quando si utilizzano opzioni diverse. La tabella inoltre mostra se il sistema modifica la versione del pannello memorizzato con il profilo di USERA.

Tabella 57. Come memorizzare e modificare i livelli di assistenza

Azione eseguita	Versione del pannello visualizzato	Versione del pannello memorizzato
Utilizzare il comando WRKUSRPRF	Pannello Gestione iscrizione utente	Nessuna modifica (livello di assistenza di base)
Dal pannello Gestione iscrizione utente, premere F21 e selezionare livello di assistenza intermedio.	Pannello Gestione profili utente	Modificato in livello di assistenza intermedio
Utilizzare il comando WRKUSRPRF	Pannello Gestione profili utente	Nessuna modifica (intermedio)
Selezionare l'opzione Gestione iscrizione utente dal menu SETUP.	Pannello Gestione profili utente	Nessuna modifica (intermedio)
Immettere CHGUSRPRF USERA ASTLVL(*BASIC)		Modificato in livello di assistenza di base
Utilizzare il comando WRKUSRPRF	Pannello Gestione iscrizione utente	Nessuna modifica (di base)
Immettere `WRKUSRPRF ASTLVL(*INTERMED)`	Pannello Gestione profili utente	Nessuna modifica (di base)

Nota: il campo *opzione Utente* nel profilo utente coinvolge anche la visualizzazione dei pannelli di sistema. Questo campo viene descritto sulla pagina "Opzioni utente" a pagina 116.

Tabella 58. Valori possibili per ASTLVL

***SYSVAL**	Viene utilizzato il livello di assistenza specificato nel valore di sistema QASTLVL.
***BASIC**	Viene utilizzata l'interfaccia utente Operational Assistant.
***INTERMED**	Viene utilizzata l'interfaccia di sistema.
***ADVANCED**	Viene utilizzata l'interfaccia di sistema esperta. Per consentire più voci nell'elenco, i numeri delle opzioni e i tasti funzione non vengono sempre visualizzati. Se il comando non ha associato un livello avanzato (*ADVANCED), viene utilizzato il livello intermedio (*INTERMED).

Libreria corrente

La *libreria corrente* è quella specificata per essere la prima libreria utente in cui effettuare la ricerca degli oggetti richiesti da un utente. Se l'utente crea gli oggetti e specifica *CURLIB, gli oggetti vengono inseriti nella libreria corrente.

Richiesta di aggiunta utente:
Libreria predefinita

Parametro CL:
CURLIB

Lunghezza:
10

speciale
*USE

La libreria corrente viene automaticamente aggiunta all'elenco librerie dell'utente quando questo si collega. Non è necessario che sia incluso nell'elenco iniziale di librerie nella descrizione lavoro dell'utente.

L'utente non può modificare la libreria corrente se il campo *Possibilità limitate* presente nel profilo utente è impostato su *YES o *PARTIAL.

L'argomento "Elenchi librerie" a pagina 222 fornisce maggiori informazioni sull'utilizzo degli elenchi librerie e della libreria corrente.

Tabella 59. Valori possibili per CURLIB:

***CRTDFT**	Questo utente non dispone di una libreria corrente. Se gli oggetti vengono creati utilizzando *CURLIB su un comando di creazione, la libreria QGPL viene utilizzata come libreria corrente predefinita.
nome-libreria-corrente	Il nome di una libreria.

Suggerimenti: utilizzare il campo *Libreria corrente* per controllare l'ubicazione in cui gli utenti possono inserire i nuovi oggetti, come ad esempio i programmi Query. Utilizzare il campo *Possibilità limitate* per impedire agli utenti di modificare la libreria corrente.

Programma iniziale

È possibile specificare il nome di un programma da richiamare nel momento in cui l'utente accede. Tale programma viene definito programma iniziale. Un programma iniziale viene eseguito prima della visualizzazione del menu iniziale, qualora disponibile.

Richiesta di aggiunta utente:
Collegamento al programma

Parametro CL:
INLPGM

Lunghezza:
10 (nome programma) 10 (nome libreria)

Autorizzazione:
*USE per il programma *EXECUTE per la libreria

Se il campo *Possibilità limitate* nel profilo utente è *YES o *PARTIAL, l'utente non può specificare un programma iniziale sul pannello Accesso.

Il programma iniziale viene richiamato solo se il programma di instradamento dell'utente è QCMD o QCL. Consultare "Avvio di un lavoro interattivo" a pagina 213 per maggiori informazioni sulla sequenza dell'elaborazione nel momento in cui l'utente si collega.

I programmi iniziali vengono utilizzati per due scopi principali:

- Limitare l'utente ad una serie specifica di funzioni.
- Eseguire alcune elaborazioni iniziali, come ad esempio aprire i file o stabilire l'elenco di librerei, nel momento in cui l'utente si collega per la prima volta.

I parametri non possono essere inoltrati ad un programma iniziale. Se il programma iniziale non riesce ad avviarsi, l'utente non è in grado di collegarsi.

Tabella 60. Valori possibili per INLPGM:

***NONE**	Nessun programma richiamato nel momento in cui l'utente si collega. Se si specifica il nome di un menu sul parametro del menu iniziale, tale menu viene visualizzato.
nome-programma	Il nome del programma richiamato quando l'utente si collega.

Tabella 61. Valori possibili per la libreria INLPGM:

***LIBL**	L'elenco di librerie viene utilizzato per individuare il programma. Se la descrizione del lavoro per il profilo utente dispone di un elenco di librerie iniziale, tale elenco viene utilizzato. Se la descrizione del lavoro specifica *SYSVAL per l'elenco di librerie iniziale, viene utilizzato il valore di sistema QUSRLIBL.
***CURLIB**	La libreria corrente specificata nel profilo utente viene utilizzata per individuare il programma. Se non si specifica alcuna libreria corrente, viene utilizzata QGPL.
nome-libreria	La libreria in cui è posizionato il programma.

Menu iniziale

È possibile specificare il nome di un menu da visualizzare momento in cui l'utente accede. Il menu iniziale viene visualizzato dopo il programma iniziale dell'utente. Il menu iniziale viene richiamato solo se il programma di instradamento dell'utente è QCMD o QCL.

Richiesta di aggiunta utente:
Primo menu

Parametro CL:
INLMNU

Lunghezza:
10 (nome menu) 10 (nome libreria)

speciale
*USE per il menu *EXECUTE per la libreria

Se si desidera che un utente esegua solo il programma iniziale, è possibile specificare *SIGNOFF per il menu iniziale.

Se il campo Possibilità limitate nel profilo dell'utente è impostato su *YES, l'utente non può specificare un menu iniziale diverso sul pannello Collegamento. Se a un utente viene consentito di specificare un menu iniziale sul pannello Collegamento, il menu specificato sovrascrive il menu nel profilo utente.

Tabella 62. Valori possibili per MENU:

MAIN	Viene visualizzato il menu principale di System i.
***SIGNOFF**	Il sistema scollega l'utente al completamento del programma iniziale. Utilizzare questo valore per limitare gli utenti all'esecuzione di un singolo programma.
nome-menu	Il nome del menu che viene richiamato nel momento in cui l'utente di collega.

Tabella 63. Valori possibili per la libreria MENU:

***LIBL**	Per individuare il menu, si utilizza l'elenco di librerie. Se il programma iniziale aggiunge delle voci all'elenco di librerie, tali voci vengono inserite nella ricerca, poiché il menu viene richiamato una volta completato il programma iniziale.
***CURLIB**	Per individuare il menu, si utilizza la libreria corrente per il lavoro. Se nell'elenco di librerie non esiste alcuna voce della libreria corrente, si utilizza GPL.
nome-libreria	La libreria in cui è ubicato il menu.

Possibilità limitate

È possibile utilizzare il campo Possibilità limitate per limitare la possibilità dell'utente di immettere comandi e di sovrascrivere il programma iniziale, il menu iniziale, la libreria corrente e il programma di gestione dei tasti di attenzione specificati nel profilo utente. Questo campo consente di impedire agli utente di fare esperimenti sul sistema.

Richiesta di aggiunta utente:
Limitare l'utilizzo della riga comandi

Parametro CL:
LMTCPB

Lunghezza:
10

Un utente con possibilità limitate può eseguire solo comandi definiti come utilizzabili da utenti limitati. I seguenti commands da IBM con ALWLMTUSR(*YES):

- Scollegamento (SIGNOFF)
- Invio messaggio (SNDMSG)
- Visualizzazione messaggi (DSPMSG)
- Visualizzazione lavoro (DSPJOB)
- Visualizzazione registrazione lavoro (DSPJOBLOG)
- Avvio PC Organizer (STRPCO)
- Gestione messaggi (WRKMSG)

Il campo Possibilità limitate nel profilo utente e il parametro ALWLMTUSR sui comandi si applicano solo ai comandi eseguiti dalla riga comandi, al pannello Voce comando, FTP, REXEC, utilizzando l'API QCAPCMD o a un'opzione da un menu di raggruppamento dei comandi. Gli utenti possono effettuare le seguenti operazioni:

- Eseguire i comandi in programmi CL che stanno eseguendo un comando come conseguenza dell'esecuzione di un'opzione del menu
- Eseguire comandi remoti mediante le applicazioni

È possibile consentire all'utente con possibilità limitate di eseguire comandi aggiuntivi o eliminare tali comandi dall'elenco, modificando il parametro ALWLMTUSR per un comando. Utilizzare il comando Modifica comando (CHGCMD). Se si creano i propri comandi, è possibile specificare il parametro ALWLMTUSR sul comando Creazione comando (CRTCMD).

Valori possibili: la Tabella 64 mostra i possibili valori per il campo Possibilità limitate e quali funzioni sono consentite per ciascun valore.

Tabella 64. Funzioni consentite per i valori di Possibilità limitate

Funzione	*YES	*PARTIAL	*NO
Modifica programma iniziale	No	No	Sì
Modifica menu iniziale	No	Sì	Sì
Modifica libreria corrente	No	No	Sì
Modifica programma di attenzione	No	No	Sì
Immissione commandi	Pochi valori[1]	Sì	Sì

[1] Per impostazione predefinita sono consentiti i seguenti comandi: SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPJOBLOG, STRPCO, WRKMSG. L'utente non può utilizzare F9 per visualizzare una riga comandi da un qualsiasi menu o pannello.

Suggerimenti: utilizzare un menu iniziale, limitare l'utilizzo della riga comandi e fornire l'accesso al menu consente di impostare un ambiente per un utente che non deve o non vuole accedere alle funzioni del sistema.

Concetti correlati

"Pianificazione dei menu" a pagina 245
I menu sono un ottimo metodo per fornire un accesso controllato sul sistema. È possibile utilizzare i menu per limitare un utente a una serie di funzioni controllate specificando le capacità limitate e un menu iniziale nel profilo utente.

Testo

Il testo nel profilo utente viene utilizzato per descrivere il profilo utente o le sue funzioni.

Richiesta di aggiunta utente:
Descrizione utente

Parametro CL:
TEXT

Lunghezza:
50

Per i profili utente, il testo deve contenere informazioni di identificazione, come ad esempio il nome e il dipartimento dell'utente. Per i profili di gruppo, il testo deve identificare il gruppo, come ad esempio i dipartimenti inclusi nel gruppo.

Tabella 65. Valori possibili per testo:

***BLANK:**	Nessun testo specificato.
descrizione	Specificare non più di 50 caratteri.

Consigli: Il campo *Testo* viene troncato su molti pannelli del sistema. Inserire le informazioni di identificazione più importanti all'inizio del campo.

Autorizzazione speciale

L'autorizzazione speciale viene utilizzata per specificare i tipi di azioni che un utente può eseguire sulle risorse di sistema. Un utente può disporre di una o più autorizzazioni speciali.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
SPCAUT

Lunghezza:
100 (10 caratteri per autorizzazione speciale)

Autorizzazione:
Per fornire un'autorizzazione speciale ad un profilo utente, è necessario disporre di quell'autorizzazione speciale.

Tabella 66. Valori possibili per SPCAUT:

***USRCLS**	Le autorizzazioni speciali vengono concesse a questo utente in base al campo classe utente (USRCLS) nel profilo utente e al valore di sistema del livello di sicurezza (QSECURITY). Se si specifica *USRCLS, non è possibile specificare autorizzazioni speciali per questo utente. Se si specifica *USRCLS quando si crea o si modifica un profilo utente, il sistema inserisce nel profilo le autorizzazioni speciali corrette, come se le avesse immesse l'utente. Quando si visualizzano i profili, l'utente non può indicare se le autorizzazioni speciali sono state immesse individualmente o dal sistema, in base alla classe utente. La Tabella 56 a pagina 86 indica le autorizzazioni speciali predefinite per ogni classe utente.
***NONE**	Nessuna autorizzazione speciale è concessa a questo utente.
nome-autorizzazione-speciale	Specificare una o più autorizzazioni speciali per l'utente.

autorizzazione speciale *ALLOBJ

L'autorizzazione speciale per tutti gli oggetti (*ALLOBJ) consente all'utente di accedere a qualunque risorsa sul sistema se esiste l'autorizzazione privata per l'utente.

Anche se l'utente dispone dell'autorizzazione *EXCLUDE su un oggetto, l'autorizzazione speciale *ALLOBJ consente ancora all'utente di accedere all'oggetto.

Rischi: l'autorizzazione speciale *ALLOBJ fornisce all'utente l'autorizzazione estesa su tutte le risorse sul sistema. L'utente può visualizzare, modificare o cancellare ciascun oggetto. L'utente inoltre può garantire agli altri utenti l'autorizzazione per utilizzare gli oggetti.

Un utente con l'autorizzazione *ALLOBJ non può eseguire direttamente le operazioni che richiedono l'autorizzazione speciale. Ad esempio, l'autorizzazione speciale *ALLOBJ non consente ad un utente di creare un altro profilo utente, poiché la creazione dei profili utente richiede l'autorizzazione speciale *SECADM. Tuttavia, un utente con l'autorizzazione speciale *ALLOBJ può inoltrare un lavoro batch da eseguire utilizzando un profilo che dispone dell'autorizzazione speciale necessaria. L'autorizzazione speciale *ALLOBJ fornisce essenzialmente ad un utente l'accesso a tutte le funzioni sul sistema.

Autorizzazione speciale *SECADM

L'autorizzazione speciale di amministratore della sicurezza (*SECADM) consente ad un utente di creare, modificare e cancellare i profili utente.

Un utente con l'autorizzazione speciale *SECADM può:

- Aggiungere gli utenti all'indirizzario di distribuzione del sistema.
- Visualizzare l'autorizzazione per i documenti o le cartelle.
- Aggiungere ed eliminare i codici di accesso al sistema.
- Fornire e togliere l'autorizzazione al codice di accesso di un utente.
- Fornire e togliere l'autorizzazione agli utenti che possono operare per conto di un altro utente.
- Eliminare i documenti e le cartelle.
- Eliminare gli elenchi dei documenti.
- Modificare gli elenchi di distribuzione creati da altri utenti.

Solo un utente con l'autorizzazione speciale *SECADM e *ALLOBJ può fornire l'autorizzazione speciale *SECADM a un altro utente.

Autorizzazione speciale *JOBCTL

L'autorizzazione speciale controllo lavoro(*JOBCTL) consente all'utente di modificare la priorità dei lavori e di stampa, terminare un lavoro prima che sia terminato oppure cancellare l'emissione prima che venga stampata. L'autorizzazione speciale *JOBCTL inoltre può fornire ad un utente l'accesso all'emissione di spool riservata, se le code di emissione sono state specificate OPRCTL(*YES).

L'autorizzazione speciale al controllo del lavoro (*JOBCTL) consente all'utente di eseguire le seguenti azioni:

- Modificare, cancellare, conservare e rilasciare tutti i file sulle code di emissione specificate come OPRCTL(*YES).
- Visualizzare, inviare e copiare tutti i file sulle code di emissione specificate come DSPDTA(*YES o *NO) e OPRCTL(*YES).
- Conservare, rilasciare e cancellare le code dei lavori specificate come OPRCTL(*YES).
- Conservare, rilasciare e cancellare le code di emissione specificate come OPRCTL(*YES).
- Conservare, rilasciare, modificare e annullare i lavori di altri utenti.
- Avviare, modificare, terminare, conservare e rilasciare i programmi di scrittura se la coda di emissione è specificata come OPRCTL(*YES).
- Modificare gli attributi di esecuzione di un lavoro, come ad esempio la stampante per un lavoro.
- Arrestare i sottosistemi.
- Eseguire l'IPL (Initial Program Load).

La protezione dell'emissione di stampa e delle code di emissione viene trattata in "Stampa" a pagina 225.

È possibile modificare la priorità del lavoro (JOBPTY) e la priorità di emissione (OUTPTY) del proprio lavoro senza l'autorizzazione speciale al controllo del lavoro. È necessario disporre dell'autorizzazione speciale *JOBCTL per modificare la priorità di esecuzione (RUNPTY) del proprio lavoro.

Le modifiche apportate alla priorità dell'emissione e del lavoro di un lavoro vengono limitate dal limite di priorità (PTYLMT) nel profilo dell'utente che apporta le modifiche.

Rischi: Un utente che abusa dell'autorizzazione speciale *JOBCTL può avere un effetto negativo sui singoli lavori e sulle prestazioni generali del sistema.

Autorizzazione speciale *SPLCTL

L'autorizzazione speciale controllo spool (*SPLCTL) consente all'utente di eseguire tutte le funzioni di controllo dello spool, come ad esempio modificare, cancellare, visualizzare, conservare e rilasciare i file di spool.

L'utente può eseguire queste funzioni in tutte le code di emissione, senza tenere conto delle autorizzazioni per la coda di emissione o del parametro OPRCTL per la coda di emissione. L'autorizzazione *SPLCTL consente inoltre ad un utente di gestire le code dei lavori, compresa la conservazione, il rilascio e la cancellazione della coda dei lavori. L'utente può eseguire queste funzioni su tutte le code dei lavori, senza tenere conto delle autorizzazioni per la coda dei lavori o del parametro OPRCTL per la coda dei lavori.

Rischi: l'utente con l'autorizzazione speciale *SPLCTL può eseguire qualsiasi operazione su qualsiasi file di spool nel sistema. I file di spool riservati non possono essere protetti da un utente che dispone dell'autorizzazione speciale *SPLCTL.

Autorizzazione speciale *SAVSYS

L'autorizzazione speciale per il salvataggio del sistema (*SAVSYS) fornisce all'utente l'autorizzazione per salvare, ripristinare e liberare la memoria per tutti gli oggetti sul sistema, senza considerare se l'utente dispone dell'autorizzazione all'esistenza dell'oggetto per gli oggetti.

Rischi: l'utente con l'autorizzazione speciale *SAVSYS può:

- Salvare un oggetto e portarlo su un altro sistema per ripristinarlo.
- Salvare un oggetto e visualizzare il nastro per visualizzare i dati.
- Salvare un oggetto e liberare la memoria, cancellando la parte di dati dell'oggetto.
- Salvare un documento e cancellarlo.

Autorizzazione speciale *SERVICE

L'autorizzazione speciale al servizio (*SERVICE) consente all'utente di avviare i programmi di manutenzione del sistema utilizzando il comando STRSST. Questa autorizzazione speciale consente all'utente di eseguire il debug di un programma con la sola autorizzazione *USE al programma e di eseguire le funzioni di visualizzazione e di modifica del servizio. Inoltre, consente all'utente di eseguire funzioni di traccia.

La funzione dump può essere eseguita senza l'autorizzazione *SERVICE.

Rischi: un utente con l'autorizzazione speciale *SERVICE può visualizzare e modificare le informazioni confidenziali utilizzando le funzioni di sevizio. L'utente deve avere l'autorizzazione speciale *ALLOBJ per modificare le informazioni utilizzando le funzioni di servizio.

Per ridurre il rischio dei comandi di traccia, è possibile fornire gli utenti dell'autorizzazione necessaria per eseguire le tracce senza l'autorizzazione speciale *SERVICE. In questo modo, solo utenti specifici possono eseguire un comando di traccia, che concede loro l'accesso ai dati sensibili. L'utente deve essere autorizzato al comando e disporre dell'autorizzazione speciale *SERVICE o essere autorizzato alla funzione Traccia di servizio di i5/OS mediante Gestione applicazione in System i Navigator. Il comando Modifica utilizzo funzione (CHGFCNUSG), con l'ID funzione QIBM_SERVICE_TRACE, può essere utilizzato anche per modificare l'elenco di utenti abilitati ad eseguire le operazioni di traccia.

I comandi a cui è possibile concedere l'accesso seguendo questa procedura comprendono:

STRCMNTRC	Avvio traccia comunicazioni
ENDCMNTRC	Fine traccia delle comunicazioni
PRTCMNTRC	Stampa traccia delle comunicazioni
DLTCMNTRC	Cancellazione traccia comunicazioni
CHKCMNTRC	Controllo traccia delle comunicazioni
TRCCNN	Connessione traccia (consultare "Concessione accesso alle tracce")
TRCINT	Traccia interna
STRTRC	Avvio traccia lavoro
ENDTRC	Fine traccia lavoro
PRTTRC	Stampa traccia lavoro
DLTTRC	Cancellazione traccia lavoro
TRCTCPAPP	Traccia applicazione TCP/IP
WRKTRC	Gestione tracce

Nota: è necessaria l'autorizzazione *ALLOBJ per modificare i dati utilizzando le funzioni di servizio.

Concessione accesso alle tracce:

I comandi di traccia, come ad esempio TRCCNN (Connessione traccia) sono comandi importanti che non dovrebbero essere concessi a tutti gli utenti che necessitano dell'accesso ad altri strumenti di servizio e di debug.

Attenersi alla seguente procedura per limitare gli utenti che possono accedere a questi comandi di traccia senza disporre dell'autorizzazione *SERVICE:

1. In System i Navigator, aprire Utenti e gruppi.
2. Selezionare **Tutti gli utenti** per visualizzare un elenco dei profili utente.
3. Fare clic col tastino destro del mouse sul profilo utente da modificare.
4. Selezionare **Proprietà**.
5. Fare clic su **Funzioni**.
6. Aprire il separatore Applicazioni.
7. Selezionare **Accesso a**.
8. Selezionare **Applicazioni host**.
9. Selezionare **Sistema operativo**.
10. Selezionare **Servizi**.
11. Utilizzare la casella di spunta per concedere o revocare l'accesso al comando di traccia.

In alternativa, è possibile utilizzare il comando CHGFCNUSG (Modifica utilizzo funzione) per concedere agli utenti l'accesso ai comandi di traccia. Immettere CHGFCNUSG FCNID(QIBM_SERVICE_TRACE) USER(profilo-utente) USAGE(*ALLOWED).

Autorizzazione speciale *AUDIT

L'autorizzazione speciale controllo (*AUDIT) fornisce all'utente la possibilità di visualizzare e modificare le caratteristiche del controllo.

Un utente può effettuare le seguenti attività se dispone dell'autorizzazione speciale *AUDIT:

- Modificare e visualizzare i valori di sistema che controllano il controllo.
- Utilizzare i comandi CHGOBJAUT, CHGDLOAUD e CHGAUD per modificare il controllo degli oggetti.
- Utilizzare il comando CHGUSRAUD per modificare il controllo per un utente.
- Visualizzare i valori di controllo di un oggetto.
- Visualizzare i valori di controllo di un profilo utente.
- Eseguire alcuni dei comandi degli strumenti di sicurezza come PRTADPOBJ.

Rischi: un utente con l'autorizzazione speciale *AUDIT può arrestare e avviare il controllo sul sistema oppure impedire il controllo di azioni particolari. Se si dispone di un record di controllo di eventi relativi alla sicurezza importante per il sistema, prestare attenzione all'utilizzo dell'autorizzazione speciale *AUDIT.

Per evitare che gli utenti generali visualizzino informazioni di controllo, limitare l'accesso degli utenti generali alle seguenti informazioni:

- Il giornale di controllo sicurezza (QAUDJRN)
- Altri giornali che contengono dati di controllo
- File di salvataggio, file esterni, file di spool e emissioni di stampa che contengono informazioni di controllo

Nota: solo un utente che dispone delle autorizzazioni speciali *ALLOBJ, *SECADM e *AUDIT può fornire ad un altro utente l'autorizzazione speciale *AUDIT.

Autorizzazione speciale *IOSYSCFG

L'autorizzazione speciale configurazione di sistema (*IOSYSCFG) fornisce all'utente la possibilità di modificare la configurazione del sistema. Gli utenti che dispongono di questa autorizzazione speciale possono aggiungere o rimuovere informazioni sulla configurazione delle comunicazioni, gestire i server

TCP/IP e configurare l'ICS (internet connection server). La maggior parte dei comandi relativi alla configurazione delle comunicazioni richiede l'autorizzazione speciale *IOSYSCFG.

Suggerimenti per le autorizzazioni speciali: Fornire le autorizzazioni speciali agli utenti rappresenta un rischio per la sicurezza. Per ciascun utente, valutare attentamente le necessità di ciascuna delle autorizzazioni speciali. Tenere traccia degli utenti che dispongono delle autorizzazioni speciali e rivedere periodicamente i loro requisiti per l'autorizzazione.

Inoltre, è necessario controllare le seguenti situazioni dei programmi e dei profili utente:

- Se i profili utente con autorizzazioni speciali possono essere utilizzati per sottomettere i lavori
- Se i programmi creati da questi utenti possono essere eseguiti utilizzando l'autorizzazione del proprietario del programma

I programmi adottano l'autorizzazione speciale *ALLOBJ del proprietario se:

- I programmi vengono creati dagli utente che dispongono dell'autorizzazione speciale *ALLOBJ
- L'utente specifica il parametro USRPRF(*OWNER) sul comando che consente di creare il programma

Ambiente speciale

L'utente può operare in ambiente System i5, System/36 o System/38. Quando l'utente si collega, il sistema utilizza il programma di instradamento e l'ambiente speciale nel profilo utente per stabilire l'ambiente dell'utente.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
SPCENV

Lunghezza:
10

Tabella 67. Valori possibili per SPCENV:

***SYSVAL**	Il valore di sistema QSPCENV viene utilizzato per stabilire l'ambiente al momento dell'accesso da parte dell'utente, se il programma di instradamento dell'utente è QCMD.
***NONE**	L'utente opera in ambiente System i5.
***S36**	L'utente opera in ambiente System/36 se il programma di instradamento dell'utente è QCMD.

Suggerimenti: se l'utente esegue una combinazione di applicazioni System i e System/36, utilizzare il comando Avvia System/36 (STRS36) prima di eseguire le applicazioni System/36 invece che specificare l'ambiente System/36 nel profilo utente. Questo consente di avere prestazioni migliori per le applicazioni System i.

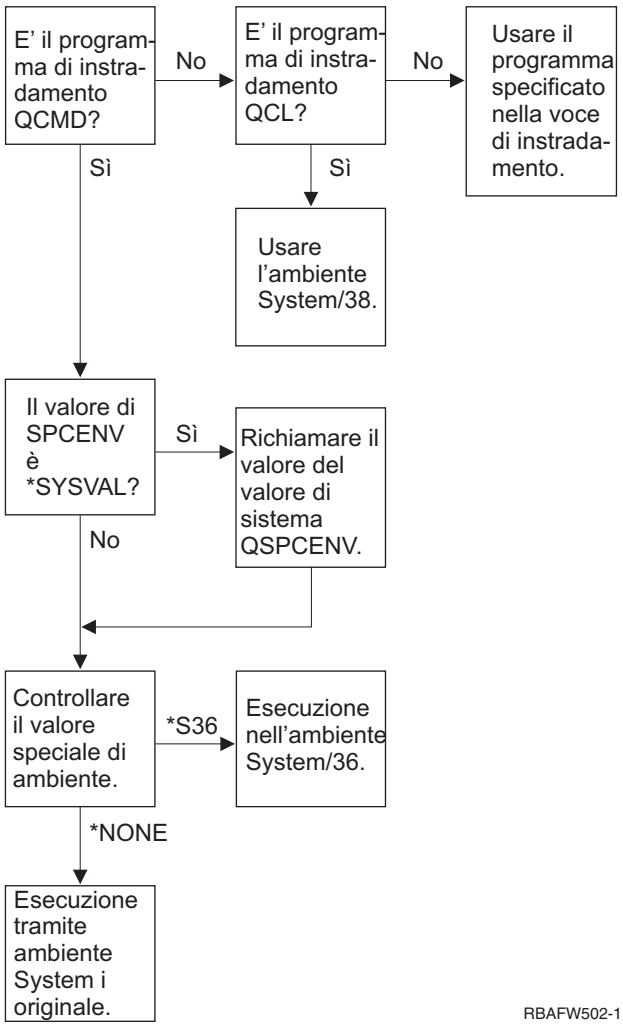


Figura 2. Descrizione dell'ambiente speciale

Descrizione dell'ambiente speciale nella Figura 2

Il sistema determina se il programma di instradamento è QCMD. In caso negativo, il sistema controlla se il programma di instradamento è QCL. In caso affermativo, il sistema utilizzerà l'ambiente speciale System/38. Se il programma di instradamento non è QCL, il sistema utilizza il programma specificato nella voce di instradamento.

Se il programma di instradamento è QCMD, il sistema determina se è stato impostato il valore di sistema SPCENV. In caso affermativo, il sistema richiama il valore per il valore di sistema QSPCENV e il sistema verifica il valore dell'ambiente speciale. Se non è stato impostato il valore di sistema SPCENV, il sistema verifica il valore di ambiente speciale.

Se il valore dell'ambiente speciale è impostato su *S36, il sistema opera nell'ambiente speciale System/36. Se il valore dell'ambiente speciale è impostato su *NONE, il sistema opera nell'ambiente integrato System i.

Visualizza informazioni di accesso

Il pannello Informazioni di accesso è uno strumento che permette agli utenti di controllare i propri profili e di rilevare gli utilizzi errati tentati. Il campo Informazioni di accesso specifica se il pannello Informazioni di accesso viene visualizzato nel momento in cui l'utente effettua l'accesso.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
DSPSGNINF

Lunghezza:
7

La Figura 3 mostra il pannello. Le informazioni sulla scadenza della parola d'ordine vengono visualizzate solo se la parola d'ordine scade entro l'intervallo di avvertenza della scadenza della parola d'ordine.

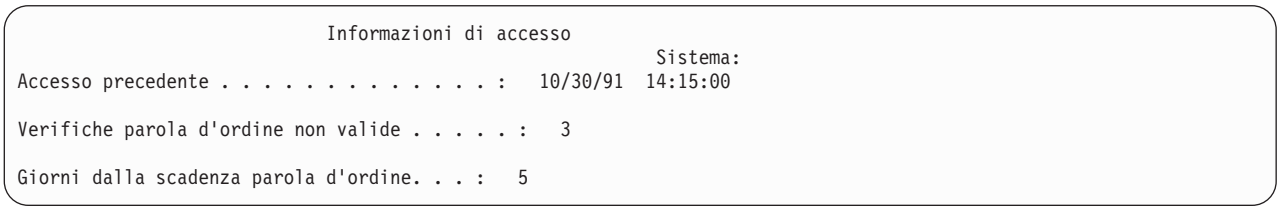


Figura 3. Pannello Informazioni di accesso

Tabella 68. Valori possibili per DSPSGNINF:

***SYSVAL**	Viene utilizzato il valore di sistema QDSPSGNINF.
***NO**	Il pannello Informazioni di accesso non viene visualizzato nel momento in cui l'utente effettua l'accesso.
***YES**	Il pannello Informazioni di accesso viene visualizzato nel momento in cui l'utente effettua l'accesso.

Consigli: si consiglia a tutti gli utenti di consultare questo pannello. Gli utenti con l'autorizzazione speciale o l'autorizzazione sugli oggetti importanti devono essere incoraggiati ad utilizzare il pannello per accertarsi che nessuno tenti di utilizzare il proprio profilo.

Intervallo scadenza parola d'ordine

L'intervallo di scadenza della parola d'ordine controlla il numero di giorni di validità di una parola d'ordine prima che questa debba essere modificata.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
PWDEXPITV

Lunghezza:
5,0

Quando la parola d'ordine di un utente è scaduta, l'utente riceve un messaggio nel momento in cui effettua l'accesso. L'utente può premere il tasto Invio per assegnare una nuova parola d'ordine oppure premere il tasto F3 (Fine) per annullare il tentativo di accesso senza assegnare una nuova parola d'ordine. Se l'utente sceglie di modificare la parola d'ordine, viene visualizzato il pannello Modifica parola d'ordine e si esegue la convalida della parola d'ordine completa per la nuova parola d'ordine. La "Intervallo scadenza parola d'ordine" mostra un esempio del messaggio di scadenza della parola d'ordine.

Tabella 69. Valori possibili per PWDEXPITV:

***SYSVAL**	Viene utilizzato il valore di sistema QPWDEXPITV.
***NOMAX**	Il sistema non richiede che l'utente modifichi la parola d'ordine.
intervallo-scadenza-parola d'ordine	Specificare un numero compreso tra 1 e 366.

Suggerimenti: impostare il valore di sistema QPWDEXPITV su un intervallo appropriato, come ad esempio da 60 a 90 giorni. Utilizzare il campo Intervallo scadenza parola d'ordine nel profilo utente per richiedere che gli utenti con autorizzazioni speciali *SERVICE, *SAVSYS, *SECADM o *ALLOBJ modifichino le parole d'ordine con una frequenza maggiore rispetto agli altri utenti.

Blocco modifica parola d'ordine

Il parametro blocco modifica parola d'ordine specifica il periodo di tempo durante il quale le modifiche ad una parola d'ordine sono bloccate dopo l'ultima operazione di modifica della parola d'ordine riuscita.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
PWDCHGBLK

Lunghezza:
10

Questo valore di parametro non limita le modifiche della parola d'ordine eseguite dal comando CHGUSRPRF (Modifica profilo utente). Inoltre, questo valore di parametro non viene forzato se il campo relativo all'impostazione della scadenza della parola d'ordine (PWDEXP) nel profilo utente ha un valore *YES. Ciò consente ad un amministratore della sicurezza di creare un profilo utente con una parola d'ordine scaduta e di permettere all'utente di accedere e di modificare la parola d'ordine (una volta) senza essere limitato dal valore di sistema di blocco modifica parola d'ordine.

Tabella 70. Valori possibili per PWDCHGBLK:

***SYSVAL**	Viene utilizzato il valore di sistema QPWDCHGBLK.
***NONE**	È possibile modificare la parola d'ordine in qualsiasi momento.
1 - 99	Non è possibile modificare una parola d'ordine entro il numero di ore specificato dopo la precedente operazione di modifica della parola d'ordine riuscita.

Suggerimento: impostare il parametro su *SYSVAL a meno che non venga notata un'attività di modifica della parola d'ordine anomala per un utente specifico. In questo caso, è possibile utilizzare un valore, come ad esempio 2, per limitare la frequenza di modifica della parola d'ordine.

Gestione parola d'ordine locale

Il parametro LCLPWDMGT (Gestione parola d'ordine locale) controlla se la parola d'ordine del profilo utente viene gestita in locale. Quando la parola d'ordine non è gestita in locale, gli utenti non possono accedere al sistema tramite accesso diretto ma tramite altre piattaforme.

Se la parola d'ordine viene gestita in locale, la parola d'ordine viene memorizzata in locale con il profilo utente. Questo è il metodo tradizionale per la memorizzazione della parola d'ordine.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
LCLPWDMGT

Lunghezza:
10

Se la parola d'ordine non viene gestita in locale, la parola d'ordine i5/OS locale viene impostata su *NONE. Il valore della parola d'ordine specificato nel relativo parametro verrà inviato ad altri prodotti IBM che eseguono la sincronizzazione della parola d'ordine, quali ad esempio IBM i5/OS Integration for Windows Server. Gli utenti non saranno in grado di modificare la propria parola d'ordine con il comando CHGPWD (Modifica parola d'ordine). Inoltre, non saranno in grado di accedere direttamente al sistema. La specifica di questo valore interesserà altri prodotti IBM che eseguono la sincronizzazione della parola d'ordine, quali ad esempio IBM i5/OS Integration for Windows Server.

Questo parametro non dovrebbe essere impostato su *NO a meno che l'utente non debba solo accedere al sistema mediante altre piattaforme, come ad esempio Windows Server.

Tabella 71. Valori possibili per LCLPWDMGT:

***YES**	La parola d'ordine viene gestita in locale.
***NO**	La parola d'ordine non viene gestita in locale.

Limite sessioni unità

Il campo limite sessioni unità controlla se il numero di sessioni unità consentite per un utente è limitato. Il valore non limita l'utilizzo del menu Richiesta sistema o un secondo collegamento dalla stessa unità.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
LMTDEVSSN

Lunghezza:
7

Tabella 72. Valori possibili per LMTDEVSSN:

***SYSVAL**	Viene utilizzato il valore di sistema QLMTDEVSSN.
***NO**	L'utente può essere collegato a più di una unità contemporaneamente.
***YES**	L'utente non può essere collegato a più di una unità contemporaneamente.
0	L'utente non è limitato a un numero specifico di sessioni unità. Questo valore ha lo stesso significato di *NO.
1	L'utente è limitato a una singola sessione unità. Questo valore ha lo stesso significato di *YES.
2 - 9	L'utente è limitato al numero specificato di sessioni unità.

Suggerimenti: limitare gli utenti ad una stazione di lavoro alla volta è uno dei metodi per scoraggiare la condivisione dei profili utente. Impostare il valore di sistema QLMTDEVSSN su 1 (YES). Se alcuni utenti devono necessariamente collegarsi a più stazioni di lavori, utilizzare il campo Limite sessioni unità nel profilo utente per quegli utenti.

Buffer della tastiera

Questo parametro specifica il valore del buffer della tastiera utilizzato quando un lavoro viene inizializzato per questo profilo utente. Il nuovo valore ha effetto al successivo collegamento dell'utente.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
KBDBUF

Lunghezza:
10

Il campo Buffer della tastiera controlla due funzioni:

Type-ahead:
Invia i dati del tipo di utente più rapidamente di quanto possano essere inviati al sistema.

Memorizzazione in buffer del tasto di attenzione:
Se tale funzione è attiva, il tasto di Attenzione viene trattato come un qualsiasi altro tasto. Se la Memorizzazione in buffer del tasto di attenzione non è attiva, premendo il tasto di attenzione si inviano le informazioni al sistema anche quando l'inserimento di altri stazioni di lavoro è impedito.

Tabella 73. Valori possibili per KBDBUF:

***SYSVAL**	Viene utilizzato il valore di sistema QKBDBUF.
***NO**	La funzione type-ahead e l'opzione di Memorizzazione in buffer del tasto di attenzione non sono attive per questo profilo utente.
***TYPEAHEAD**	La funzione type-ahead è attiva per questo profilo utente.
***YES**	La funzione type-ahead e l'opzione di Memorizzazione in buffer del tasto di attenzione sono attive per questo profilo utente.

Memoria massima

È possibile specificare la quantità massima di memoria ausiliaria che il sistema utilizza per memorizzare gli oggetti permanenti di proprietà del profilo utente. Ciò include gli oggetti che il sistema inserisce nella libreria temporanea (QTEMP) durante un lavoro.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
MAXSTG

Lunghezza:
11,0

Se la memoria necessaria è maggiore della quantità massima specificata quando l'utente tenta di creare un oggetto, l'oggetto non viene creato.

Il valore della memoria massima viene applicato indipendentemente ad ogni ASP (Auxiliary Storage Pool) indipendente sul sistema. Per questo motivo, specificare un valore 5000 indica che il profilo utente può utilizzare la seguente dimensione di memoria ausiliaria:

- 5000 KB di memoria ausiliaria nell'ASP di sistema e negli ASP utente di base.
- 5000 KB di memoria ausiliaria nell'APS indipendente 00033 (se presente).
- 5000 KB di memoria ausiliaria nell'ASP indipendente 00034 (se presente).

In totale vengono forniti 15.000 KB di memoria ausiliaria dall'intero sistema.

Quando si pianifica la memoria massima per i profili utente, è opportuno considerare le seguenti funzioni di sistema, che possono coinvolgere la memoria massima necessaria all'utente:

- Un'operazione di ripristino assegna innanzitutto la memoria all'utente che esegue l'operazione di ripristino e trasferisce in seguito gli oggetti a OWNER. Gli utenti che eseguono un numero elevato di operazioni di ripristino dovrebbero disporre di MAXSTG(*NOMAX) nei rispettivi profili utente.
- Al profilo utente che possiede un ricevitore di giornale viene assegnata la memoria non appena la dimensione del ricevitore aumenta. Se vengono creati nuovi ricevitori, la memoria continua ad essere assegnata al profilo utente che possiede il ricevitore di giornale attivo. Gli utenti che possiedono i ricevitori di giornale attivi dovrebbero disporre di MAXSTG(*NOMAX) nei rispettivi profili utente.
- Se un profilo utente specifica OWNER(*GRPPRF), la proprietà di ciascun oggetto creato dall'utente viene trasferito al profilo di gruppo una volta creato l'oggetto. Tuttavia, l'utente che crea l'oggetto deve avere una memoria adeguata per contenere ogni oggetto creato prima che la proprietà dell'oggetto venga trasferita al profilo gruppo.
- Il sistema assegna la memoria per le descrizioni degli oggetti inseriti in una libreria al proprietario di tale libreria. Ciò si verifica anche se gli oggetti sono di proprietà di un altro profilo utente. Esempi di tali descrizioni sono riferimenti testo e programma.
- Il sistema assegna memoria al profilo utente per oggetti temporanei che vengono utilizzati durante l'elaborazione del lavoro. Esempi di tali oggetti sono i blocchi di controllo di sincronizzazione, gli spazi di modifica dei file e i documenti.

Tabella 74. Valori possibili per MAXSTG:

***NOMAX**	È possibile assegnare a questo profilo tutta la memoria richiesta.
KB massimi	Specificare la quantità massima di memoria in kilobyte (1 kilobyte equivale a 1024 byte) che può essere assegnata a questo profilo utente.

Limite priorità

Il limite priorità nel profilo utente determina le proprietà massime di pianificazione (priorità del lavoro e di emissione) consentite per ciascun lavoro inoltrato dall'utente. Il limite priorità controlla la priorità del lavoro quando viene inoltrato. Esso controlla anche le modifiche apportate alla priorità del lavoro quando il lavoro è in attesa nella coda o quando viene eseguito.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
PTYLMT

Lunghezza:
1

Un lavoro batch dispone di tre valori di priorità differenti:

Priorità di esecuzione:
Determina come il lavoro può competere per le risorse del computer quando il lavoro è in esecuzione. La priorità di esecuzione viene determinata dalla classe dell'oggetto.

Priorità lavoro:
Determina la priorità di pianificazione per un lavoro batch quando il lavoro si trova nella coda lavori. È possibile impostare la priorità del lavoro nella descrizione lavoro oppure utilizzando il comando di inoltro.

Priorità di emissione:
Determina la priorità pianificazione per l'emissione creata dal lavoro sulla coda di emissione. È possibile impostare la priorità di emissione nella descrizione lavoro oppure quando si utilizza il comando di inoltro.

Il limite di priorità limita inoltre le modifiche che un utente con l'autorizzazione speciale *JOBCTL può apportare al lavoro di un altro utente. Non è possibile fornire al lavoro di un altro utente una priorità più alta rispetto al limite specificato nel proprio profilo utente.

Se un lavoro batch viene eseguito in un profilo utente diverso rispetto all'utente che ha inoltrato il lavoro, i limiti di priorità per il lavoro batch vengono stabiliti dal profilo in cui viene eseguito il lavoro. Se una priorità di pianificazione richiesta in un lavoro inoltrato supera il limite di priorità nel profilo utente, la priorità del lavoro viene ridotta al livello concesso dal profilo utente.

Tabella 75. Valori possibili per PTYLMT:

3	Il limite di priorità predefinito per i profili utente è 3. La priorità predefinita per la priorità del lavoro e di emissione sulle descrizioni del lavoro è 5. Impostare il limite di priorità per il profilo utente impostato su 3 consente all'utente di spostare alcuni lavori avanti ad altri nelle code.
limite priorità	Specificare un valore, compreso tra 1 e 9. La priorità più alta è 1; quella più bassa è 9.

Suggerimenti: l'utilizzo dei valori di priorità nelle descrizioni lavoro e sui comandi di inoltro lavoro si rivela spesso la soluzione migliore per la gestione dell'uso delle risorse di sistema rispetto alla modifica del limite di priorità nei profili utente.

Utilizzare il limite di priorità nel profilo utente per controllare le modifiche che gli utenti possono apportare ai lavori inoltrati. Ad esempio, gli operatori di sistema possono aver bisogno di un limite di priorità maggiore in modo da poter spostare gli oggetti nelle code.

Descrizione lavoro

La descrizione di un lavoro contiene una serie specifica di attributi lavoro, vale a dire la coda lavori da utilizzare, la priorità di pianificazione, i dati di instradamento, la severità della coda messaggi, le informazioni sull'emissione e sull'elenco librerie. Gli attributi determinano la modalità di esecuzione di ciascun lavoro sul sistema.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
JOBD

Lunghezza
10 (nome descrizione lavoro) 10 (nome libreria)

Autorizzazione:
*USE per descrizione lavoro, *READ e *EXECUTE per la libreria

Quando un utente effettua un collegamento, il sistema blocca la voce relativa alla stazione di lavoro nella descrizione del sottosistema per stabilire la descrizione lavoro da utilizzare per il lavoro interattivo. Se la voce della stazione di lavoro specifica *USRPRF per la descrizione del lavoro, verrà utilizzata la descrizione lavoro specificata nel profilo utente.

La descrizione lavoro per un lavoro batch viene specificata all'avvio del lavoro. Tale descrizione può essere specificata da un nome o potrebbe essere la descrizione lavoro del profilo utente sotto il quale viene eseguito il lavoro.

Consultare l'argomento Work management per ulteriori informazioni sulle descrizioni dei lavori e i relativi utilizzi.

Tabella 76. Valori possibili per JOBD:

QDFTJOBD	Viene utilizzata la descrizione del lavoro fornita dal sistema e rilevata nella libreria QGPL. È possibile utilizzare il comando Visualizzazione descrizione lavoro (DSPJOBD) per consultare gli attributi contenuti in questa descrizione lavoro.
nome- descrizione- lavoro	Specificare il nome della descrizione lavoro, 10 caratteri o meno.

Tabella 77. Valori possibili per la libreria JOBD:

***LIBL**	L'elenco librerie viene utilizzato per individuare la descrizione del lavoro.
***CURLIB**	La libreria corrente per il lavoro viene utilizzata per individuare la descrizione del lavoro. Se nell'elenco di librerie non esiste alcuna voce della libreria corrente, si utilizza GPL.
nome- libreria	Specificare la libreria in cui è posizionata la descrizione del lavoro, 10 caratteri o meno.

Suggerimenti: per i lavori interattivi, la descrizione del lavoro costituisce un metodo efficace per il controllo dell'accesso alle librerie. È possibile utilizzare una descrizione lavoro per un utente che deve specificare un elenco librerie univoco, invece che utilizzare il valore di sistema QUSRLIBL (elenco librerie utente).

Profilo di gruppo

Il parametro profilo di gruppo (GRPPRF) specifica se l'utente è un membro di un profilo di gruppo. Il profilo gruppo può fornire all'utente l'autorizzazione necessaria per utilizzare gli oggetti sui quali l'utente non dispone dell'autorizzazione specifica. È possibile specificare fino a 15 gruppi aggiuntivi per l'utente nel parametro Profilo di gruppo supplementare (SUPGRPPRF).

Richiesta di aggiunta utente:
Gruppo di utenti

Parametro CL:
GRPPRF

Lunghezza:
10

Autorizzazione:
Per specificare un gruppo durante la creazione o la modifica di un profilo utente, è necessario disporre delle autorizzazioni *OBJMGT, *OBJOPR, *READ, *ADD, *UPD e *DLT sul profilo gruppo.

Nota: L'autorizzazione adottata non viene utilizzata per controllare l'autorizzazione *OBJMGT sul profilo gruppo. Per ulteriori informazioni sull'autorizzazione adottata, consultare "Oggetti che adottano l'autorizzazione del proprietario" a pagina 160.

Quando si specifica un profilo di gruppo in un profilo utente, all'utente vengono automaticamente concesse le autorizzazioni *OBJMGT, *OBJOPR, *READ, *ADD, *UPD e *DLT al profilo di gruppo, se questo non è già compreso nei profili di gruppo utente. Queste autorizzazioni sono necessarie alle funzioni del sistema e non dovrebbero essere rimosse.

Se un profilo specificato nel parametro GRPPRF non è già un profilo di gruppo, il sistema imposta le informazioni nel profilo contrassegnandolo come profilo di gruppo. Il sistema inoltre crea un gid per il profilo di gruppo, qualora non ne abbia già uno.

Quando si modifica il valore GRPPRF, la modifica diventa effettiva al successivo collegamento dell'utente o al successivo passaggio, da parte del lavoro, all'utente del profilo tramite un handle o un token del profilo, che è stato ottenuto una volta che si è verificata la modifica.

Consultare "Pianificazione dei profili di gruppo" a pagina 256 per ulteriori informazioni sull'utilizzo dei profili di gruppo.

Tabella 78. Valori possibili per GRPPRF

***NONE**	Non viene utilizzato alcun profilo utente per questo profilo utente.
nome-profilo-utente	Specificare il nome di un profilo di gruppo di cui questo profilo utente è un membro.

Proprietario

Se l'utente è un membro di un gruppo, è possibile utilizzare il parametro proprietario nel profilo utente per specificare chi possiede i nuovi oggetti creati dall'utente. Gli oggetti possono essere di proprietà dell'utente o del primo gruppo dell'utente (il valore del parametro GRPPRF). È possibile specificare il campo Proprietario solo se è stato specificato un valore diverso da *NONE per il campo Profilo gruppo.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
OWNER

Lunghezza:
10

Quando si modifica il valore Proprietario, la modifica diventa effettiva al successivo accesso dell'utente o al successivo passaggio, da parte del lavoro, all'utente del profilo tramite un handle o un token del profilo, ottenuto una volta che si è verificata la modifica.

Tabella 79. Valori possibili per Proprietario:

***USRPRF**	Questo profilo utente è il proprietario degli oggetti che crea.
***GRPPRF**	Il profilo di gruppo diviene il proprietario degli oggetti creati dall'utente e ottiene l'autorizzazione (*ALL) su tutti gli oggetti. Il profilo utente non ottiene tutte le autorizzazioni specifiche sui nuovi oggetti che crea. Se si specifica *GRPPRF, è necessario specificare il nome di un profilo di gruppo nel parametro GRPPRF e il parametro GRPAUT deve essere *NONE. **Note:** 1. Se si fornisce la proprietà al gruppo, tutti i membri del gruppo possono modificare, sostituire e cancellare l'oggetto. 2. Il parametro *GRPPRF viene ignorato per tutti i file system, tranne QSYS.LIB. Nei casi in cui il parametro viene ignorato, l'utente conserva la proprietà dell'oggetto.

Autorizzazione gruppo

Se il profilo utente è un membro di un gruppo ed è stato specificato OWNER(*USRPRF), il campo Autorizzazione gruppo controlla quale autorizzazione viene fornita al profilo di gruppo per gli oggetti creati da questo utente.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
GRPAUT

Lunghezza:
10

L'autorizzazione gruppo può essere specificata solo quando GRPPRF non è *NONE e OWNER è *USRPRF. L'autorizzazione gruppo si applica al profilo specificato nel parametro GRPPRF. Non si applica ai profili di gruppo supplementari specificati nel parametro SUPGRPPRF.

Quando si modifica il valore GRPAUT, la modifica diventa effettiva al successivo collegamento dell'utente o al successivo passaggio, da parte del lavoro, all'utente del profilo tramite un handle o un token del profilo, ottenuto una volta che si è verificata la modifica.

Tabella 80. Valori possibili per GRPAUT:

***NONE**	Nessuna autorizzazione specifica viene concessa al profilo di gruppo quando questo utente crea gli oggetti.
***ALL**	Al profilo di gruppo vengono concesse tutte le autorizzazioni per la gestione e i dati sui nuovi oggetti creati dall'utente.
***CHANGE**	Al profilo di gruppo viene fornita l'autorizzazione alla modifica degli oggetti creati dall'utente.
***USE**	Al profilo di gruppo viene fornita l'autorizzazione per la visualizzazione degli oggetti creati dall'utente.
***EXCLUDE**	Al profilo gruppo viene negato specificatamente l'accesso ai nuovi oggetti creati dall'utente.

Riferimenti correlati

"Definizione della modalità di accesso alle informazioni" a pagina 142
È possibile definire quali operazioni possono essere eseguite su oggetti, dati e campi.

Tipo autorizzazione gruppo

Quando un utente crea un nuovo oggetto, il parametro Tipo autorizzazione gruppo nel profilo utente determina il tipo di autorizzazione che il gruppo di utenti riceve sul nuovo oggetto.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
GRPAUTTYP

Lunghezza:
10

Il parametro GRPAUTTYP gestisce i parametri OWNER, GRPPRF e GRPAUT per determinare l'autorizzazione del gruppo su un nuovo oggetto.

Quando si modifica il valore GRPAUTTYP, la modifica diventa effettiva al successivo collegamento dell'utente o al successivo passaggio, da parte del lavoro, all'utente del profilo tramite un handle o un token del profilo, ottenuto una volta che si è verificata la modifica.

Tabella 81. Valori possibili per GRPAUTTYP: [1]

***PRIVATE**	L'autorizzazione definita nel parametro GRPAUT viene assegnata al profilo di gruppo come autorizzazione privata.
***PGP**	Il profilo di gruppo definito nel parametro GRPPRF è il gruppo principale per l'oggetto appena creato. L'autorizzazione del gruppo principale per l'oggetto è l'autorizzazione specificata nel parametro GRPAUT. Questo valore può essere specificato solo quando GRPAUT non è *NONE.

Tabella 81. Valori possibili per GRPAUTTYP: [1] (Continua)

[1]	L'autorizzazione privata e l'autorizzazione del gruppo principale forniscono lo stesso accesso all'oggetto per membri del gruppo, ma con caratteristiche di prestazioni diverse. "Gruppo principale per un oggetto" a pagina 155 spiega come opera l'autorizzazione del gruppo principale.

Suggerimenti: specificare *PGP consente di iniziare ad utilizzare l'autorizzazione al gruppo principale. È opportuno considerare di utilizzare GRPAUTTYP(*PGP) per gli utenti che creano nuovi oggetti con una certa frequenza a cui devono accedere i membri del profilo del gruppo.

Gruppi supplementari

È possibile specificare gruppi supplementari durante la creazione o la modifica di un profilo utente. L'utente non può disporre di profili di gruppo supplementare se il parametro GRPPRF è *NONE.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
SUPGRPPRF

Lunghezza:
150

Autorizzazione:
Per specificare i gruppi supplementari durante la creazione o la modifica di un profilo utente, è necessario disporre dell'autorizzazione *OBJMGT, *OBJOPR, *READ, *ADD, *UPD e *DLT su ciascun profilo di gruppo.

Nota: L'autorizzazione *OBJMGT non può derivare dall'autorizzazione adottata. Per ulteriori informazioni, consultare "Oggetti che adottano l'autorizzazione del proprietario" a pagina 160.

È possibile specificare un massimo di 15 nomi di profili dai quali l'utente deve ricevere l'autorizzazione. L'utente diventa un membro di ciascun profilo di gruppo supplementare.

Quando i profili di gruppo supplementari vengono specificati in un profilo utente, all'utente vengono automaticamente concesse le autorizzazioni *OBJMGT, *OBJOPR, *READ, *ADD, *UPD e *DLT su ciascun profilo di gruppo, se questo non è già compreso nei profili di gruppo utente. Queste autorizzazioni sono necessarie alle funzioni del sistema e non dovrebbero essere rimosse. Se un profilo specificato nel parametro SUPGRPPRF non è già un profilo di gruppo, il sistema lo contrassegna come un profilo di gruppo. Il sistema inoltre crea un numero gid (group identification) per il profilo di gruppo, qualora non ne abbia già uno.

Quando si modifica il valore SUPGRPPRF, la modifica diventa effettiva al successivo accesso dell'utente o al successivo passaggio, da parte del lavoro, all'utente del profilo tramite un handle o un token del profilo, ottenuto una volta che si è verificata la modifica.

Consultare "Pianificazione dei profili di gruppo" a pagina 256 per ulteriori informazioni sull'utilizzo dei profili di gruppo.

Tabella 82. Valori possibili per SUPGRPPRF

***NONE**	Non vengono utilizzati gruppi supplementari con questo profilo utente.
nome- profilo- gruppo	Specificare fino ad un massimo di 15 nomi di profili di gruppo da utilizzare con questo profilo utente. Questi profili, insieme al profilo specificato nel parametro GRPPRF, vengono utilizzati per fornire all'utente l'accesso agli oggetti. È anche possibile specificare il nome profilo per GRPPRF come uno dei 15 profili gruppo supplementari.

Codice account

La specifica del codice account consente all'utente di raccogliere informazioni sulle risorse del sistema utilizzate da un lavoro.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
ACGCDE

Lunghezza:
15

L'account lavoro è una funzione facoltativa utilizzata per raccogliere le informazioni sull'utilizzo delle risorse di sistema. Il valore di sistema del livello di account (QACGLVL) determina se l'account del lavoro è attivo. Il codice account per un lavoro deriva dalla descrizione del lavoro o dal profilo utente. Il codice account può inoltre essere specificato quando un lavoro è in esecuzione mediante il comando Modifica codice account (CHGACGCDE).

Quando si modifica il valore del *codice account*, la modifica diventa effettiva al successivo collegamento dell'utente o al successivo avvio di un lavoro, che viene eseguito tramite il codice account del profilo utente.

Consultare l'argomento Work management per maggiori informazioni sull'account del lavoro.

Tabella 83. Valori possibili per ACGCDE:

***BLANK**	A questo profilo utente viene assegnato un codice account di 15 spazi vuoti.
codice account	Specificare un codice account di 15 caratteri. Se si specificano meno di 15 caratteri, la stringa viene riempita sulla destra con spazi vuoti.

Parola d'ordine documento

La parola d'ordine documento controlla l'accessibilità e la distribuzione della posta personale quando viene visualizzata da persone che lavorano per conto dell'utente. La parola d'ordine documento viene supportata da alcuni prodotti DIA (Document Interchange Architecture), quali ad esempio Displaywriter.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
DOCPWD

Tabella 84. Valori possibili per DOCPWD:

***NONE**	Nessuna parola d'ordine documento viene utilizzata da questo utente.
parola d'ordine- documento	Specificare una parola d'ordine documento per questo utente. La parola d'ordine deve essere composta da 1 a 8 caratteri (lettere da A a Z e numeri da 0 a 9). Il primo carattere della parola d'ordine documento deve essere alfabetico; i caratteri restanti possono essere alfanumerici. Gli spazi vuoti incorporati, quelli iniziali e i caratteri speciali non sono consentiti.

Coda messaggi

Una *coda messaggi* è un oggetto su cui i messaggi vengono inseriti quando vengono inviati ad una persona o ad un programma. Una coda messaggi viene utilizzata quando un utente invia o riceve i messaggi.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
MSGQ

Lunghezza:
10 (nome coda messaggi) 10 (nome libreria)

Autorizzazione:
*USE per la coda messaggi, se presente. *EXECUTE per la libreria della coda messaggi.

Se la coda messaggi non esiste, viene creata quando il profilo viene creato o modificato. La coda messaggi è di proprietà del profilo creato o modificato. All'utente che crea il profilo viene fornita l'autorizzazione *ALL alla coda messaggi.

Se la coda messaggi per un profilo utente viene modificata utilizzando il comando Modifica profilo utente (CHGUSRPRF), la coda messaggi precedente non viene cancellata automaticamente dal sistema.

Tabella 85. Valori possibili per MSGQ:

***USRPRF**	Una coda messaggi con lo stesso nome del profilo utente viene utilizzata come coda messaggi per questo utente. Se la coda messaggi non esiste, viene creata nella libreria QUSRSYS.
nome coda-messaggi	Specificare il nome della coda messaggi utilizzato per questo utente. Se si specifica il nome di una coda messaggi, è necessario specificare il parametro della libreria.

Tabella 86. Valori possibili per la libreria MSGQ:

***LIBL**	L'elenco librerie viene utilizzato per individuare la coda messaggi. Se la coda messaggi non esiste, non è possibile specificare *LIBL.
***CURLIB**	La libreria corrente per il lavoro viene utilizzata per individuare la coda messaggi. Se nell'elenco di librerie non esiste alcuna voce della libreria corrente, si utilizza GPL. Se la coda messaggi non esiste, viene creata nella libreria corrente o in QGPL.
nome- libreria	Specificare la libreria in cui è posizionata la coda messaggi. Se la coda messaggi non esiste, viene creata in questa libreria.

| **Suggerimenti:** fornire a ciascun profilo utente una coda messaggi univoca, preferibilmente con lo stesso
| nome del profilo utente.

Consegna

La modalità di consegna di una coda messaggi stabilisce se l'utente viene interrotto all'arrivo di un nuovo messaggio sulla coda.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
DLVRY

Lunghezza:
10

La modalità di consegna specificata nel profilo utente si applica alla coda messaggi personale dell'utente. Se si modifica la consegna della coda messaggi nel profilo utente e l'utente ha effettuato l'accesso, la modifica avrà luogo al successivo ha effettuato l'accesso da parte dell'utente. È possibile inoltre modificare la consegna di una coda messaggi con il comando Modifica coda messaggi (CHGMSGQ).

Tabella 87. Valori possibili per DLVRY:

***NOTIFY**	Il lavoro a cui è assegnata la coda messaggi viene informato dell'arrivo di un messaggio nella coda messaggi. Per i lavori interattivi in una stazione di lavoro, l'allarme audio e la luce di messaggio in attesa sono attivi. Il tipo di consegna non può essere modificato in *NOTIFY se la coda messaggi viene utilizzata anche da un altro utente.
***BREAK**	Il lavoro a cui è assegnata la coda messaggi viene interrotto all'arrivo di messaggio nella coda messaggi. Se il lavoro è un lavoro interattivo, l'allarme audio è attivo (se l'allarme è installato). Il tipo di consegna non può essere modificato in *BREAK se la coda messaggi viene utilizzata anche da un altro utente.
***HOLD**	I messaggi vengono conservati nella coda messaggi fino a quando non vengono richiesti dall'utente o dal programma.
***DFT**	I messaggi che richiedono risposta ricevono una risposta predefinita; i messaggi puramente informativi vengono ignorati.

Severità

Se una coda messaggi è in modalità *BREAK o *NOTIFY, il codice di severità stabilisce i messaggi con livello più basso inviati all'utente. I messaggi con severità inferiore rispetto al codice di severità vengono conservati nella coda messaggi senza che l'utente venga informato.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
SEV

Lunghezza:
2,0

Se si modifica la severità della coda messaggi nel profilo utente e l'utente è collegato, la modifica avrà luogo al successivo accesso da parte dell'utente. È possibile inoltre modificare la severità di una coda messaggi con il comando CHGMSGQ.

Tabella 88. Valori possibili per SEV:

00:	Se non si specifica un codice severità, si utilizza il valore 00. L'utente viene informato di tutti i messaggi, se la coda messaggi è in modalità *NOTIFY o *BREAK.
codice- severità	Specificare un valore, compreso tra 00 e 99, per il codice di severità più basso che provoca l'invio della notifica all'utente. È possibile specificare un qualsiasi valore composto da 2 cifre, anche se non è stato definito alcun codice di severità (definito dal sistema o dall'utente).

Unità di stampa

È possibile specificare la stampante utilizzata per stampare l'emissione per questo utente. I file di spool sono inseriti in una coda di emissione con lo stesso nome della stampante quando la coda di emissione (OUTQ) viene specificata come unità di stampa (*DEV).

Richiesta di aggiunta utente:
Stampante predefinita

Parametro CL:
PRTDEV

Lunghezza:
10

L'unità di stampa e le e informazioni sulla coda di emissione provenienti dal profilo utente vengono utilizzate se il file di stampa specifica *JOB e se la descrizione del lavoro specifica *USRPRF. Per ulteriori informazioni sull'indirizzamento dell'emissione di stampa, consultare l'argomento Basic printing.

Tabella 89. Valori possibili per PRTDEV:

***WRKSTN**	Viene utilizzata la stampante assegnata alla stazione di lavoro dell'utente (nella descrizione dell'unità).
***SYSVAL**	Viene utilizzata la stampante di sistema predefinita specificata nel valore di sistema QPRTDEV.
nome- unità- stampa	Specificare il nome della stampante utilizzata per stampare l'emissione per questo utente.

Coda di emissione

Sia l'elaborazione interattiva che quella in batch possono restituire file di spool da inviare ad una stampante. I file di spool vengono inseriti in una coda di emissione. Il sistema può disporre di numerose e differenti code di emissione.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
OUTQ

Lunghezza:
10 (nome coda di emissione) 10 (nome libreria)

Autorizzazione:
*USE per la coda di emissione *EXECUTE per la libreria

Non è necessario che una coda di emissione sia collegata ad una stampante per ricevere i nuovi file di spool.

L'unità di stampa e le e informazioni sulla coda di emissione provenienti dal profilo utente vengono utilizzate se il file di stampa specifica *JOB e se la descrizione del lavoro specifica *USRPRF. Per ulteriori informazioni sull'indirizzamento dell'emissione di stampa, consultare l'argomento Advanced Function Presentation.

Tabella 90. Valori possibili per OUTQ:

***WRKSTN**	Viene utilizzata la coda di emissione assegnata alla stazione di lavoro dell'utente (nella descrizione dell'unità).
***DEV**	Viene utilizzata una coda di emissione con lo stesso nome dell'unità di stampa specificato sul parametro PRTDEV.
nome- coda- emissione	Specificare il nome della coda di emissione da utilizzare. La coda di emissione deve essere già esistente. Se è stata specificata una coda di emissione, è necessario specificare anche la libreria.

Tabella 91. Valori possibili per la libreria OUTQ:

***LIBL**	L'elenco di librerie viene utilizzato per rilevare la coda di emissione.
***CURLIB**	La libreria corrente per il lavoro viene utilizzata per rilevare la coda di emissione. Se nell'elenco di librerie non esiste alcuna voce della libreria corrente, si utilizza GPL.
nome- libreria	Specificare la libreria in cui è posizionata la coda di emissione.

Programma di gestione tasto di attenzione

Il Programma di gestione tasto di attenzione (ATNPGM) è il programma che viene richiamato quando l'utente seleziona il tasto Attenzione (ATTN) durante un lavoro interattivo.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
ATNPGM

Lunghezza:
10 (nome programma) 10 (nome libreria)

Autorizzazione:
*USE per il programma

*EXECUTE per la libreria

ATNPGM viene attivato solo se il programma di instradamento dell'utente è QCMD. ATNPGM viene attivata prima di richiamare il programma iniziale. Se il programma iniziale modifica ATNPGM, il nuovo ATNPGM rimane attivo solo fino a quando non termina il programma iniziale. Se il comando Impostazione programma di gestione tasto di attenzione (SETATNPGM) viene eseguito da una riga comandi o da un'applicazione, il nuovo ATNPGM specificato sovrascrive ATNPGM dal profilo utente.

Nota: consultare "Avvio di un lavoro interattivo" a pagina 213 per maggiori informazioni sulla sequenza dell'elaborazione nel momento in cui l'utente si collega.

Il campo *Possibilità limitate* determina se l'utente con il comando Modifica profilo (CHGPRF) può specificare un programma di gestione tasto di attenzione diverso.

Tabella 92. Valori possibili per ATNPGM:

***SYSVAL**	Viene utilizzato il valore di sistema QATNPGM.
***NONE**	Questo utente non utilizza alcun programma di gestione tasto di attenzione.
***ASSIST**	Viene utilizzato il programma di attenzione Operational Assistant (QEZMAIN).
nome- programma	Specificare il nome del programma di gestione tasto di attenzione. Se viene specificato il nome di un programma, è necessario specificare una libreria.

Tabella 93. Valori possibili per la libreria ATNPGM:

***LIBL**	L'elenco di librerie viene utilizzato per individuare il Programma di gestione tasto di attenzione.
***CURLIB**	La libreria corrente per il lavoro viene utilizzata per individuare il Programma di gestione tasto di attenzione. Se nell'elenco di librerie non esiste alcuna voce della libreria corrente, si utilizza GPL.
nome- libreria:	Specificare la libreria in cui è ubicato il programma di gestione tasto di attenzione.

Sequenza di ordinamento

La sequenza di ordinamento viene utilizzata per l'emissione di questo utente. È possibile utilizzare le tabelle di ordinamento fornite dal sistema oppure crearne di proprie. Una tabella di ordinamento può essere associata ad un particolare identificativo lingua sul sistema.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
SRTSEQ

Lunghezza:
10 (nome tabella o valore) 10 (nome libreria)

Autorizzazione:
*USE per la tabella *EXECUTE per la libreria

Tabella 94. Valori possibili per SRTSEQ:

***SYSVAL**	Viene utilizzato il valore di sistema QSRTSEQ.
***HEX**	Per questo utente viene utilizzata la sequenza di ordinamento esadecimale standard.
***LANGIDSHR**	Viene utilizzata la tabella della sequenza di ordinamento associata all'identificativo lingua dell'utente. La tabella può contenere lo stesso peso per più caratteri.
***LANGIDUNQ**	Viene utilizzata la tabella della sequenza di ordinamento associata all'identificativo lingua dell'utente. La tabella deve contenere un peso univoco per ciascun carattere nella code page.
nome-tabella	Specificare il nome della tabella della sequenza di ordinamento per questo utente.

Tabella 95. Valori possibili per la libreria SRTSEQ:

***LIBL**	L'elenco di librerie viene utilizzato per individuare la tabella specificata per il valore SRTSEQ.
***CURLIB**	La libreria corrente per il lavoro viene utilizzata per individuare la tabella specificata per il valore SRTSEQ. Se nell'elenco di librerie non esiste alcuna voce della libreria corrente, si utilizza GPL.
nome- libreria	Specificare la libreria in cui è posizionata la tabella della sequenza di ordinamento.

Identificativo lingua

È possibile specificare l'identificativo lingua che il sistema deve utilizzare per l'utente.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
LANGID

Lunghezza:
10

Per consultare un elenco di identificativi lingua, premere F4 (Richiesta) sul parametro identificativo lingua dal pannello Creazione profilo utente o dal pannello Modifica profilo utente.

Tabella 96. Valori possibili per LANGID:

***SYSVAL:**	Il valore di sistema QLANGID viene utilizzato per determinare l'identificativo lingua.
identificativo- lingua	Specificare l'identificativo lingua per questo utente.

Identificativo paese o regione

È possibile specificare l'identificativo paese o regione che il sistema deve utilizzare per l'utente.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
CNTRYID

Lunghezza:
10

Per consultare un elenco di identificativi paese o regione, premere F4 (Richiesta) sul parametro identificativo paese o regione dal pannello Creazione profilo utente o dal pannello Modifica profilo utente.

Tabella 97. Valori possibili per CNTRYID:

***SYSVAL**	Il valore di sistema QCNTRYID viene utilizzato per stabilire l'identificativo paese o regione.
identificativo paese o regione	Specificare l'identificativo paese o regione per questo utente.

CCSID (Coded character set identifier)

È possibile specificare il CCSID (coded character set identifier) che il sistema deve utilizzare per l'utente.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
CCSID

Lunghezza:
5,0

Per consultare un elenco di CCSID (coded character set identifiers) premere F4 (Richiesta) sul parametro relativo CCSID dal pannello Creazione profilo utente o dal pannello Modifica profilo utente.

Tabella 98. Valori possibili per CCSID:

***SYSVAL**	Il valore di sistema QCCSID viene utilizzato per stabilire il CCSID (coded character set identifier).
coded-character- set-identifier	Specificare il CCSID (coded character set identifier) per questo utente.

Controllo identificativo carattere

L'attributo *CHRIDCTL* controlla il tipo di conversione serie di caratteri codificati per i file di visualizzazione, stampate e i gruppi di pannelli.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
CHRIDCTL

Lunghezza:
10

Le informazioni sul controllo dell'identificativo carattere provenienti dal profilo utente vengono utilizzate solo se è stato specificato il valore speciale *CHRIDCTL sul parametro del comando CHRID sui comandi di creazione, modifica o sovrascrittura per i file di visualizzazione, stampate e i gruppi di pannelli.

Tabella 99. Valori possibili per CHRIDCTL:

***SYSVAL**	Il valore di sistema QCHRIDCTL viene utilizzato per determinare il controllo identificativo carattere.

Tabella 99. Valori possibili per CHRIDCTL: (Continua)

***DEVD**	Il CHRID dell'unità viene utilizzato per rappresentare il CCSID dei dati. Non viene eseguita alcuna conversione, poiché il CCSID dei dati è sempre identico al CHRID dell'unità.
***JOBCCSID**	La conversione dei caratteri avviene quando esiste una differenza tra i valori dell'unità CHRID, del lavoro CCSID o dei dati CCSID. In fase di immissione, i dati dei caratteri vengono convertiti dall'unità CHRID al CCSID del lavoro, quando necessario. In fase di emissione, i dati dei caratteri vengono convertiti dal CCSID del lavoro nell'unità CHRID, quando necessario. In fase di emissione, i dati dei caratteri vengono convertiti dal CCSID del gruppo di pannelli o del file nell'unità CHRID, quando necessario.

Attributi del lavoro

Il campo SETJOBATR specifica gli attributi del lavoro da utilizzare nel momento in cui ha inizio il lavoro dalla locale specificata nel parametro LOCALE.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
SETJOBATR

Lunghezza:
160

Tabella 100. Valori possibili per SETJOBATR:

***SYSVAL**	Il valore di sistema QSETJOBATR viene utilizzato per stabilire gli attributi del lavoro da utilizzare dalla locale.
***NONE**	Nessun attributo del lavoro deve essere utilizzato dalla locale.
***CCSID**	Viene utilizzato il CCSID (coded character set identifier) dalla locale. Il valore CCSID dalla locale sovrascriverà il CCSID del profilo utente.
***DATFMT**	Viene utilizzato il formato della data della locale.
***DATSEP**	Viene utilizzato il separatore data della locale.
***DECFMT**	Viene utilizzato il formato decimale della locale.
***SRTSEQ**	Viene utilizzata la sequenza di ordinamento della locale. La sequenza di ordinamento della locale sovrascriverà la sequenza di ordinamento del profilo utente.
***TIMSEP**	Viene utilizzato il separatore ora della locale.

È possibile specificare qualsiasi combinazione dei seguenti valori:

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

Locale

Il campo Locale specifica il nome del percorso della locale assegnata alla variabile di ambiente LANG per questo utente.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
LOCALE

Tabella 101. Valori per LOCALE:

***SYSVAL**	Il valore di sistema QLOCALE viene utilizzato per stabilire il nome del percorso della locale da assegnare per questo utente.
***NONE**	Nessuna locale assegnata per questo utente.
***C**	La locale C è assegnata a questo utente.
***POSIX**	La locale POSIX è assegnata a questo utente.
nome percorso locale	Il nome del percorso della locale da assegnare a questo utente.

Opzioni utente

Il campo Opzioni utente consente di personalizzare alcuni pannelli e funzioni del sistema per l'utente. È possibile specificare più valori per il parametro dell'opzione utente.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
USROPT

Lunghezza:
240 (10 caratteri ognuno)

Tabella 102. Valori possibili per USROPT:

***NONE**	Non viene utilizzata alcuna opzione speciale per questo utente. Viene utilizzata l'interfaccia di sistema standard.
***CLKWD**	Le parole chiave vengono visualizzate al posto dei possibili valori dei parametri quando si richiede il comando CL (control language). Ciò equivale a selezionare il tasto F11 dal normale comando CL (control language) che richiede la visualizzazione.
***EXPERT**	Quando l'utente visualizza pannelli che elencano le autorizzazioni dell'oggetto, come ad esempio il pannello Editazione autorizzazione oggetto o il pannello Editazione elenco di autorizzazioni, vengono visualizzate le informazioni dettagliate sull'autorizzazione senza che l'utente debba premere il tasto F11 (Visualizzazione dettagli). "Pannelli autorizzazioni" a pagina 166 mostra un esempio della versione esperta del pannello.
***HLPFULL**	L'utente visualizza le informazioni di aiuto a schermo intero, invece di visualizzare una finestra.
***PRTMSG**	Quando un file di spool viene stampato per questo l'utente, un messaggio viene inviato alla coda messaggi dell'utente.
***ROLLKEY**	Le azioni dei tasti Pag. Su e Pag. Giù vengono invertite.
***NOSTSMSG**	I messaggi di stato in genere visualizzati nella parte inferiore del pannello non vengono presentati all'utente.
***STSMSG**	I messaggi di stato vengono visualizzati quando vengono inviati all'utente.

Numero uid (user identification)

L'IFS (integrated file system) utilizza il numero uid (user identification) per identificare un utente e verificarne l'autorizzazione. Ogni utente sul sistema deve avere un uid univoco.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
UID

Lunghezza:
10,0

Tabella 103. Valori possibili per UID:

***GEN**	Il sistema genera un uid univoco per questo utente. L'uid generato sarà superiore a 100.
uid	Un valore compreso tra 1 e 4294967294 da assegnare come uid per questo utente. L'uid non deve essere già stato assegnato a un altro utente.

Suggerimenti: per la maggior parte delle installazioni, consentire al sistema di generare un uid per i nuovi utenti specificando UID(*GEN). Tuttavia, se il sistema fa parte di una rete, è possibile che sia necessario assegnare uid in modo che corrispondano a quelli assegnati su altri sistemi nella rete. Consultare l'amministratore di rete.

Numerto gid (Group identification)

L'IFS (integrated file system) utilizza il numero gid (group identification) per identificare questo profilo come profilo gruppo. Un profilo utilizzato come profilo gruppo deve disporre di un gid.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
GID

Lunghezza:
10,0

Tabella 104. Valori possibili per GID:

***NONE**	Questo profilo non dispone di un gid. È necessario specificare questo valore se il profilo utente è un membro di un gruppo (GRPPRF non è *NONE).
***GEN**	Il sistema genera un gid univoco per questo profilo. Il gid creato sarà superiore a 100.
gid	Un valore compreso tra 1 e 4294967294 da assegnare come gid per questo profilo. Il gid non deve essere già stato assegnato ad un altro profilo.

Suggerimenti: per la maggior parte delle installazioni, consentire al sistema di generare un gid per i nuovi profili di gruppo, specificando GID(*GEN). Tuttavia, se il sistema fa parte di una rete, è probabile che l'utente debba assegnare i gid in modo che corrispondano a quelli assegnati su altri sistemi nella rete. Consultare l'amministratore di rete.

Non assegnare un gid a un profilo utente che non si intende utilizzare come profilo di gruppo. In alcuni ambienti, ad un utente che ha effettuato l'accesso e dispone di un gid viene impedito di eseguire alcune funzioni.

Indirizzario principale

L'indirizzario principale è l'indirizzario di lavoro iniziale dell'utente per l'IFS (integrated file system). L'indirizzario principale è l'indirizzario corrente dell'utente se non è stato specificato un indirizzario corrente e diverso.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
HOMEDIR

Se l'indirizzario principale specificato nel profilo non esiste nel momento in cui l'utente si collega, l'indirizzario principale dell'utente è l'indirizzario ″root″ (/).

Tabella 105. Valori possibili per HOMEDIR:

***USRPRF**	L'indirizzario principale assegnato all'utente è `/home/xxxxx`, dove `xxxxx` rappresenta il nome del profilo utente.
indirizzario-principale	Il nome dell'indirizzario principale da assegnare a questo utente.

Associazione EIM

L'Associazione EIM specifica se è necessario aggiungere un'associazione EIM (Enterprise Identity Mapping) ad un identificativo EIM per questo utente. Facoltativamente, l'identificativo EIM può essere creato solo se non esiste già.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
EIMASSOC

Note:

1. le informazioni sull'associazione EIM non sono memorizzate nel profilo utente. Queste informazioni non vengono salvate o ripristinate con il profilo utente.
2. Se il sistema non è configurato per EIM, non viene eseguita alcuna elaborazione. L'impossibilità di eseguire le operazioni EIM non implica la non riuscita del comando.

Tabella 106. Valori possibili per EIMASSOC, valori singoli:

Valori singoli	
***NOCHG**	Non verrà aggiunta l'associazione EIM.

Tabella 107. Valori possibili per EIMASSOC, elemento 1:

Elemento 1: Identificativo EIM Specifica l'identificativo EIM per questa associazione.	
***USRPRF**	Il nome dell'identificativo EIM è lo stesso del profilo utente.
valore-carattere	Specifica il nome dell'identificativo EIM.

Tabella 108. Valori possibili per EIMASSOC, elemento 2:

Elemento 2: Tipo di associazione Specifica il tipo di associazione. Si consiglia di aggiungere un'associazione di destinazione per un utente i5/OS. Le associazioni di destinazione vengono utilizzate principalmente per proteggere i dati esistenti. Vengono rilevate come risultato di un'operazione di ricerca delle corrispondente (ad esempio, eimGetTargetFromSource()), ma non possono essere utilizzate come identità origine per un'operazione di ricerca delle corrispondenze. Le associazioni di origine vengono utilizzate principalmente a scopi di autenticazione. Possono essere utilizzate come identità origine di un'operazione di ricerca delle corrispondenze, ma non verranno rilevate come destinazione di un'operazione di ricerca delle corrispondenze. Le associazioni amministrative vengono utilizzate per dimostrare che un'identità viene associata ad un identificativo EIM ma che non può essere utilizzata come origine, e non verrà trovata come destinazione, di un'operazione di ricerca delle corrispondenze.	
***TARGET**	Elabora un'associazione di destinazione.
***SOURCE**	Elabora un'associazione origine.
***TGTSRC**	Elabora un'associazione di destinazione e origine.
***ADMIN**	Elabora un'associazione amministrazione.
***ALL**	Elabora tutti i tipi di associazione.

Tabella 109. Valori possibili per EIMASSOC, elemento 3:

Elemento 3: Azione associazione	
***REPLACE**	Le associazioni del tipo specificato verranno eliminate da tutti gli identificativi EIM che dispongono di un'associazione per questo profilo utente e il registro EIM locale. Una nuova associazione verrà aggiunta all'identificativo EIM specificato.
***ADD**	Aggiunge un'associazione.
***REMOVE**	Elimina un'associazione.

Tabella 110. Valori possibili per EIMASSOC, elemento 4:

Elemento 4: Creazione identificativo EIM Specifica se l'identificativo EIM deve essere creato qualora non esista già.	
***NOCRTEIMID**	L'identificativo EIM non viene creato.
***CRTEIMID**	L'identificativo EIM viene creato qualora non esista.

speciale

Il campo Autorizzazione specifica l'autorizzazione pubblica per il profilo utente.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
AUT

L'autorizzazione su un profilo controlla molte funzioni associate al profilo, come ad esempio:

- Modifica del profilo
- Visualizzazione del profilo
- Cancellazione del profilo
- Inoltro di un lavoro utilizzando il profilo

- Specifica del profilo in una descrizione lavoro
- Trasferimento proprietà oggetto al profilo
- Aggiunta dei membri, se il profilo è un profilo di gruppo

Tabella 111. Valori possibili per AUT:

***EXCLUDE**	L'accesso al profilo utente viene specificatamente negato agli utenti.
***ALL**	Agli utenti vengono concesse tutte le autorizzazioni dati e gestione sul profilo utente.
***CHANGE**	Agli utenti viene concessa l'autorizzazione per modificare il profilo utente.
***USE**	Agli utenti viene concessa l'autorizzazione per visualizzare il profilo utente.

Consultare "Definizione della modalità di accesso alle informazioni" a pagina 142 per una spiegazione completa delle autorizzazioni che possono essere concesse.

Suggerimenti: per impedire l'uso improprio dei profili utente che dispongono l'autorizzazione agli oggetti critici, accertarsi che l'autorizzazione pubblica per i profili sia *EXCLUDE. I possibili usi impropri di un profilo comprendono l'inoltro di un lavoro eseguito in quel profilo utente o la modifica di un programma che adotta l'autorizzazione di quel profilo utente.

Controllo oggetto

Il valore del controllo dell'oggetto per un profilo utente gestisce il valore di controllo dell'oggetto per un oggetto per stabilire se l'accesso di un oggetto da parte dell'utente viene controllato o meno.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
OBJAUD

Lunghezza:
10

Il controllo dell'oggetto per un profilo utente non può essere specificato su tutti i comandi del profilo utente. Utilizzare il comando CHGUSRAUD per specificare il controllo dell'oggetto per un utente. Solo un utente che dispone dell'autorizzazione speciale *AUDIT può utilizzare il comando CHGUSRAUD.

Tabella 112. Valori possibili per OBJAUD:

***NONE**	Il valore OBJAUD per gli oggetti stabilisce se il controllo dell'oggetto viene eseguito o meno per questo utente.
***ALL**	Se il valore OBJAUD per un oggetto specifica *USRPRF, quando questo utente modifica o legge l'oggetto viene scritto un record di controllo.
***CHANGE**	Se il valore OBJAUD per un oggetto specifica *USRPRF, quando questo utente modifica l'oggetto viene scritto un record di controllo.
***NOTAVL**	Questo valore viene visualizzato per indicare che il valore del parametro non è disponibile per l'utente poiché tale utente non dispone dell'autorizzazione speciale *AUDIT o *ALLOBJ. Non è possibile impostare il valore del parametro su questo valore.

La Tabella 113 mostra come i valori OBJAUD per l'utente e l'oggetto operano insieme:

Tabella 113. Controllo eseguito per l'accesso oggetto

Valore OBJAUD per l'oggetto	**Valore OBJAUD per l'utente**		
	***NONE**	***CHANGE**	***ALL**
*ALL	Modifica e utilizzo	Modifica e utilizzo	Modifica e utilizzo
*CHANGE	Modifica	Modifica	Modifica
*NONE	Nessuna	Nessuna	Nessuna
*USRPRF	Nessuna	Modifica	Modifica e utilizzo

Attività correlate

"Pianificazione del controllo dell'accesso agli oggetti" a pagina 308
Il sistema operativo i5/OS fornisce un metodo per registrare gli accessi a un oggetto nel giornale di controllo della sicurezza tramite valori di sistema e valori di controllo dell'oggetto per utenti e oggetti. Questa operazione viene denominata *controllo oggetto*.

Controllo azione

Per un singolo utente, è possibile specificare le azioni relative alla sicurezza da registrare nel giornale di controllo. Le azioni specificate per un singolo utente si applicano in aggiunta alle azioni specificate per tutti gli utenti dai valori di sistema QAUDLVL e QAUDLVL2.

Richiesta di aggiunta utente:
Non visualizzato

Parametro CL:
AUDLVL

Lunghezza:
640

Il controllo dell'azione per un profilo utente non può essere specificato su tutti i pannelli del profilo utente. Viene definito mediante il comando CHGUSRAUD. Solo un utente che dispone dell'autorizzazione speciale *AUDIT può utilizzare il comando CHGUSRAUD.

Tabella 114. Valori possibili per AUDLVL:

***NONE**	Il valore di sistema QAUDLVL verifica il controllo delle azioni per questo utente. Non viene eseguito alcun controllo aggiuntivo.
***NOTAVL**	Questo valore viene visualizzato per indicare che il valore di parametro non è disponibile per l'utente poiché tale utente non dispone dell'autorizzazione speciale *AUDIT o *ALLOBJ. Non è possibile impostare il valore del parametro su questo valore.
***AUTFAIL**	Vengono controllati gli errori di autorizzazione.
***CMD**	Vengono registrate le stringhe del comando. *CMD può essere specificato solo per i singoli utenti. Il controllo della stringa del comando non è disponibile come opzione sull'interno sistema mediante il valore di sistema QAUDLVL.
***CREATE**	Vengono registrate le operazioni di creazione degli oggetti.
***DELETE**	Vengono registrate le operazioni di cancellazione degli oggetti.
***JOBBAS**	Vengono controllate le funzioni di base del lavoro.
***JOBCHGUSR**	Vengono controllate le modifiche apportate al profilo utente attivo di un sottoprocesso o ai relativi profili del gruppo.
***JOBDTA**[1]	Vengono registrate le modifiche al lavoro.

Tabella 114. Valori possibili per AUDLVL: (Continua)

***OBJMGT**	Vengono registrate le operazioni di ridenominazione e di spostamento degli oggetti.
***OFCSRV**	Vengono registrate le modifiche apportate all'indirizzario di distribuzione del sistema e le azioni di posta d'ufficio.
***NETBAS**	Vengono controllate le funzioni di base di rete.
***NETCLU**	Vengono controllate le operazioni di gruppi di risorse cluster e del cluster.
***NETCMN** [3]	Vengono controllate le funzioni di rete e di comunicazione.
***NETFAIL**	Vengono controllati gli errori di rete.
***NETSCK**	Vengono controllate le attività socket.
***OPTICAL**	Vengono controllate tutte le funzioni dell'unità ottica.
***PGMADP**	Viene registrata la ricezione di un'autorizzazione ad un oggetto mediante un programma che adotta l'autorizzazione.
***PGMFAIL**	Vengono controllati gli errori di programma.
***PRTDTA**	Vengono controllate le funzioni di stampa con parametro SPOOL(*NO).
***SAVRST**	Vengono registrate le operazioni di salvataggio e di ripristino.
***SECCFG**	Viene controllata la configurazione della sicurezza.
***SECDIRSRV**	Vengono controllate le modifiche o gli aggiornamenti durante le funzioni del servizio indirizzario.
***SECIPC**	Vengono controllate le modifiche apportate alle comunicazioni tra processi.
***SECNAS**	Vengono controllate le azioni del servizio di autenticazione della rete.
***SECRUN**	Vengono controllate le funzioni di tempo di esecuzione della sicurezza.
***SECSCKD**	Vengono controllati gli descrittori socket.
***SECURITY**[2]	Vengono registrate le funzioni relative alla sicurezza.
***SECVFY**	Vengono controllate le funzioni di utilizzo della verifica.
***SECVLDL**	Vengono controllate le modifiche agli oggetti dell'elenco di convalida.
***SERVICE**	Viene registrato l'utilizzo dei programmi di manutenzione.
***SPLFDTA**	Vengono registrate le azioni eseguite sui file di spool.
***SYSMGT**	Viene registrato l'utilizzo delle funzioni di gestione sistemi.

Tabella 114. Valori possibili per AUDLVL: (Continua)

[1]	*JOBDTA include i due valori *JOBBAS e *JOBCHGUSR, che abilitano l'utente a personalizzare al meglio il proprio controllo. Se vengono specificati entrambi i valori, l'utente ottiene lo stesso controllo che se fosse specificato solo *JOBDTA.
[2]	*SECURITY è composto da diversi valori in modo da consentire all'utente di personalizzare al meglio il proprio controllo. Se vengono specificati tutti i valori, l'utente ottiene lo stesso controllo che se fosse specificato solo *SECURITY. Tali valori sono riportati di seguito. • *SECCFG • *SECDIRSRV • *SECIPC • *SECNAS • *SECRUN • *SECSCKD • *SECVFY • *SECVLDL
[3]	*NETCMN è composto da diversi valori in modo da consentire all'utente di personalizzare al meglio il proprio controllo. Se vengono specificati tutti i valori, l'utente ottiene lo stesso controllo che se fosse specificato solo *NETCMN. Tali valori sono riportati di seguito. • *NETBAS • *NETCLU • *NETFAIL • *NETSCK

Riferimenti correlati

"Pianificazione del controllo delle azioni" a pagina 282
I valori di sistema QAUDCTL (controllo), QAUDLVL (livello di controllo), QAUDLVL2 (estensione livello di controllo) e il parametro AUDLVL (controllo azione) nei profili utente collaborano per controllare il controllo azione.

Informazioni aggiuntive associate a un profilo utente

Questo argomento discute le autorizzazioni private, informazioni sull'oggetto posseduto e informazioni sull'oggetto del gruppo principale associate al profilo utente.

Riferimenti correlati

"Come memorizzare le informazioni sulla sicurezza" a pagina 264
Per pianificare procedure adeguate per la copia di riserva e il ripristino per le informazioni sulla sicurezza è necessario conoscere il modo in cui le informazioni vengono memorizzate e salvate.

Autorizzazioni private

Tutte le autorizzazioni private sugli oggetti di cui dispone un utente vengono memorizzate con il profilo utente. Quando un utente necessita di un'autorizzazione su un oggetto, è possibile effettuare le ricerche nelle autorizzazioni private dell'utente.

"Diagramma di flusso 3: Come viene controllata l'autorizzazione utente su un oggetto" a pagina 187
fornisce maggiori informazioni sul controllo delle autorizzazioni.

È possibile visualizzare le autorizzazioni private dell'utente su oggetti basati sulla libreria utilizzando il comando Visualizzazione profilo utente:

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

È possibile gestire le autorizzazioni private di un utente per oggetti basati su libreria e indirizzario tramite il comando WRKOBJPVT (Gestione oggetti per autorizzazione privata). Per modificare le autorizzazioni private di un utente, è possibile utilizzare i comandi che gestiscono le autorizzazioni sugli oggetti, come ad esempio Editazione autorizzazione oggetto (EDTOBJAUT).

È possibile copiare tutte le autorizzazioni private da un profilo utente su un altro mediante il comando GRTUSRAUT (Concessione autorizzazione utente). Consultare "Copia autorizzazione da un utente" a pagina 177 per ulteriori informazioni.

Autorizzazioni del gruppo principale

I nomi di tutti gli oggetti per cui il profilo rappresenta il gruppo principale vengono memorizzati con il profilo di gruppo.

È possibile visualizzare gli oggetti basati sulla libreria, per i quali il profilo rappresenta il gruppo principale, utilizzando il comando DSPUSRPRF:

```
DSPUSRPRF nome-profilo-gruppo TYPE(*OBJPGP)
```

È possibile inoltre utilizzare il comando Gestione oggetti per gruppo primario (WRKOBJPGP).

Informazioni sull'oggetto posseduto

Poiché la dimensione di un profilo utente può influire sulle prestazioni, si consiglia di non assegnare tutti (o quasi tutti) gli oggetti ad un solo profilo di società.

Le informazioni sull'autorizzazione privata per un oggetto vengono memorizzate con il profilo utente proprietario dell'oggetto. Queste informazioni vengono utilizzate per costruire i pannelli del sistema che gestiscono l'autorizzazione sull'oggetto. Se un profilo possiede un vasto numero di oggetti che dispongono di diverse autorizzazioni private, le prestazioni della creazione dei pannelli dell'autorizzazione sugli oggetti potrebbero venire compromesse. 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. È 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.

Autenticazione ID digitali

I certificati digitali consentono agli utenti di proteggere le comunicazione e di garantire l'integrità dei messaggi. L'infrastruttura della sicurezza di System i consente l'utilizzo dei certificati digitali x.509 per l'identificazione.

Le API dell'ID digitale creano, distribuiscono e gestiscono i certificati digitali associati ai profili utente. Consultare Digital certificate management APIs per dettagli sulle seguenti API:

- Aggiunta certificato utente (QSYADDUC)
- Eliminazione certificato utente (QSYRMVUC)
- Elenco certificato utente (QSYLSTUC)
- Rilevazione utente certificato (QSYFNDUC)
- Aggiunta certificato elenco di convalida (QSYADDVC)
- Eliminazione certificato elenco di convalida (QSYRMVVC)
- Elenco certificato elenco di convalida (QSYLSTVC)
- Controllo certificato elenco di convalida (QSYCHKVC)
- Analisi certificato (QSYPARSC)

Gestione profili utente

Questo argomento descrive i comandi ed i pannelli utilizzati dal cliente per creare, modificare e cancellare i profili utente sul sistema operativo i5/OS.

È necessario disporre dell'autorizzazione speciale *SECADM per creare, modificare o cancellare i profili utente.

Creazione profili utente

È possibile creare un profilo utente utilizzando il pannello elenco WRKUSRPRF (Gestione profili utente), il comando CRTUSRPRF (Creazione profilo utente), l'opzione Gestione iscrizione utente dal menu SETUP oppure utilizzando System i Navigator .

L'utente che crea il profilo utente ne è anche il proprietario e dispone dell'autorizzazione *ALL. Il profilo utente dispone dell'autorizzazione *OBJMGT e *CHANGE. Queste autorizzazioni sono necessarie per le normali operazioni e non dovrebbero essere rimosse.

Un profilo utente non può essere creato con un numero maggiore di autorizzazioni o possibilità rispetto all'utente che crea il profilo.

Nota: Non è possibile utilizzare il comando CRTUSRPRF (Creazione profilo utente) per creare un profilo utente in un lotto dischi indipendente. Tuttavia, quando un utente dispone di un'autorizzazione privata per un oggetto nel lotto dischi indipendente, è il proprietario di un oggetto in un lotto dischi indipendente o è il gruppo principale di un oggetto in un lotto dischi indipendente, il nome del profilo viene memorizzato nel lotto dischi indipendente. Se il lotto dischi indipendente viene spostato su un altro sistema, l'autorizzazione privata, la proprietà dell'oggetto e le voci del gruppo principali verranno collegate al profilo con lo stesso nome sul sistema di destinazione. Se un profilo non esiste sul sistema di destinazione, verrà creato un profilo. L'utente non disporrà di alcuna autorizzazione speciale e la parola d'ordine verrà impostata su *NONE.

Utilizzo del comando Gestione profili utente

È possibile immettere un nome profilo specifico, una serie di profili generici o *ALL sul comando WRKUSRPRF (Gestione profili utente).

Il livello di assistenza determina il pannello di elenco visualizzato dall'utente. Quando si utilizza il comando WRKUSRPRF con il livello di assistenza *BASIC, l'utente accederà al pannello Gestione iscrizione utente. Se è stato specificato il livello di assistenza *INTERMED, l'utente accederà al pannello Gestione profili utente.

È possibile specificare il parametro ASTLVL (livello di assistenza) sul comando. Se non si specifica ASTLVL, il sistema utilizza il livello di assistenza memorizzato con il profilo utente.

Nel pannello Gestione profili utente, immettere 1 e il nome del profilo che si desidera creare:

```
                          Gestione profili utente

Immettere le opzioni e premere Invio.
  1=Creaz. 2=Modifica   3=Copia   4=Eliminaz. 5=Visualiz.
  12=Gestione oggetti per proprietario

     Profilo
Opz  utente         Testo
1      NEWUSER
__   DPTSM       Reparto Vendite e Marketing
__   DPTWH       Reparto Magazzino
```

L'utente visualizza il pannello Creazione profilo utente:

```
                      Creazione profilo utente (CRTUSRPRF)

Immettere le scelte e premere Invio.

Profilo utente . . . . . .   NEWUSER        Nome
Parola d'ordine utente . . . . . .   *NONE         Valore carattere, *USRPRF...
Impostazione scadenza parola d'ordine  . . . .   *YES          *NO, *YES
Stato . . . . . .   *ENABLED      *ENABLED, *DISABLED
Classe utente . . . . . .   *USER         *USER, *SYSOPR, *PGMR...
Livello di assistenza . . . . . .   *SYSVAL       *SYSVAL, *BASIC, *INTERMED...
Libreria corrente . . . . . .   *CRTDFT       Nome, *CRTDFT
Progr. iniziale da richiamare  . . . .   *NONE         Nome, *NONE
  Libreria. . . . . .                 Nome, *LIBL, *CURLIB
Menu iniziale . . . . . .   MAIN          Nome, *SIGNOFF
  Libreria. . . . . .   QSYS          Nome, *LIBL, *CURLIB
Possibilità limitate . . . . . .   *NO           *NO, *PARTIAL, *YES
Testo 'descrizione'. . . . . .   *BLANK
```

Il pannello Creazione profilo utente mostra tutti i campi contenuti nel profilo utente. Utilizzare F10 (Parametri aggiuntivi) e pag giù per immettere più informazioni. Utilizzare F11 (Visualizzazione parole chiave) per visualizzare i nomi dei parametri.

Il pannello Creazione profilo utente non aggiunge l'utente all'indirizzario di sistema.

Utilizzo del comando Creazione profilo utente

È possibile utilizzare il comando CRTUSRPRF (Creazione profilo utente) per creare un profilo utente. È possibile immettere i parametri con il comando oppure è possibile premere il tasto F4 e visualizzare il pannello Creazione profilo utente.

Utilizzo dell'opzione Gestione iscrizione utente

È possibile utilizzare l'opzione Gestione iscrizione utente per aggiungere utenti al sistema.

Selezionare l'opzione Gestione iscrizione utente dal menu SETUP. Il livello di assistenza memorizzato con il proprio profilo utente determina se l'utente può visualizzare il pannello Gestione profili utente o Gestione iscrizione utente. L'utente può utilizzare F21 (Selezione livello di assistenza) per modificare i livelli.

Sul pannello Gestione iscrizione utente, utilizzare l'opzione 1 (Aggiunta) per aggiungere un nuovo utente al sistema.

```
                         Gestione iscrizione utente

Immettere le seguenti opzioni e quindi premere Invio.
1=Aggiunta  2=Modifica  3=Copia  4=Elimin.  5=Visualiz.

Opz     Utente            Descrizione
1       NEWUSER
_       DPTSM          Reparto Vendite e Marketing
_       DPTWH          Reparto Magazzino
```

L'utente visualizza il pannello Aggiunta utente:

```
                                Aggiunta utente

Immettere le seguenti scelte e quindi premere Invio.

Utente . . . . . .   NEWUSER        Nome
Descrizione utente. . . .
Par. d'ord . . . . . .   NEWUSER
Tipo di utente  . . . . . .   *USER          Tipo, F4 per elenco
Gruppo di utenti. . . . .   *NONE          Nome, F4 per elenco

Limitazioni uso riga comandi   N              Y=Sì, N=No

Libreria predefinita  . .                   Nome
Stampante predefinita . . . . .   *WRKSTN        Nome, *WRKSTN, F4 per elenco
Programma di accesso . . . . .   *NONE          Nome, *NONE
  Libreria  . . . . . .                       Nome

Primo menu  . . . . . .                     Nome
  Libreria  . . . . . .                       Nome

F1=Aiuto  F3=Fine   F5=Rivisual. F12=Annullamento
```

Il pannello Aggiunta utente è stato creato per l'amministratore della sicurezza senza un background tecnico. Non visualizza tutti i campi contenuti nel profilo utente. I valori predefiniti vengono utilizzati per tutti i campi che non sono visualizzati.

Nota: se si utilizza il pannello Aggiunta utente, è necessario utilizzare nomi del profilo utente con una lunghezza massima di otto caratteri.

Pag. giù per visualizzare il secondo pannello:

```
                                Aggiunta utente

Immettere le seguenti scelte e quindi premere Invio.

Prog. tasto attenzione . .   *SYSVAL
  Libreria  . . . . . .
```

Il pannello Aggiunta utente aggiunge automaticamente una voce nell'indirizzario di sistema con lo stesso ID utente del nome del profilo utente (i primi otto caratteri) e un indirizzo del nome del sistema.

Copia profili utente

È possibile creare un profilo utente copiando un altro profilo utente o un profilo di gruppo.

È possibile voler impostare un profilo in un gruppo come modello. Copiare il primo profilo nel gruppo per creare profili aggiuntivi.

È possibile copiare un profilo in modalità interattiva dal pannello Gestione iscrizione utente o dal pannello Gestione profili utente. Non esiste un comando per copiare un profilo utente.

Concetti correlati

"Profili di gruppo" a pagina 5
Un *profilo di gruppo* è un tipo speciale di profilo utente. Piuttosto che fornire l'autorizzazione a ciascun utente singolarmente, è possibile utilizzare un profilo di gruppo per definire l'autorizzazione per un gruppo di utenti.

Copia dal pannello Gestione profili utente

È possibile copiare le informazioni di un profilo utente dal pannello Gestione profili utente.

Sul pannello Gestione profili utente, immettere 3 prima del profilo che si desidera copiare. L'utente visualizza il pannello Creazione profilo utente:

```
                      Creazione profilo utente (CRTUSRPRF)

Immettere le scelte e premere Invio.

Profilo utente . . . . . .                Nome
Parola d'ordine utente. . . . . > *USRPRF       Nome
Impost. par. l'ordine come scad . . . > *NO           *NO, *YES
Stato. . . . . > *ENABLED      *ENABLED,
Classe utente. . . . . > *USER         *USER,
Livello di assistenza. . . . . > *SYSVAL       *SYSVAL,
Libreria corrente . . . . . > DPTWH         Nome,
Progr. iniziale da richiamare. . . . > *NONE         Nome,
Libreria. . . . . .                Nome,
Menu iniziale. . . . . > ICMAIN        Nome,
Libreria. . . . . > ICPGMLIB      Nome,
Possibilità limitate . . . . . > *NO           *NO,
Testo 'descrizione'. . . . . > 'Reparto Magazzino'
```

Tutti i valori del profilo utente da cui si è effettuata la copia vengono visualizzati sul pannello Creazione profilo utente, tranne i seguenti campi:

Profilo utente
Campo vuoto. Da riempire.

Parola d'ordine
Valore predefinito comando CRTUSRPRF

Parola d'ordine documento
*NONE

Coda messaggi
*USRPRF

Attributi lavoro locale
*SYSVAL

Locale *SYSVAL

Numero identificativo utente
*GEN

Numero identificativo gruppo
*NONE

Indirizzario principale
*USRPRF

Associazione EIM
*NOCHG

speciale
*EXCLUDE

È possibile modificare i campi sul pannello Creazione profilo utente. Le autorizzazioni private del profilo dal quale si è effettuata la copia non vengono copiate. Inoltre, gli oggetti interni contenenti preferenze utente e altre informazioni sull'utente non verranno copiati.

Copia dal pannello Gestione iscrizione utente

È inoltre possibile copiare profili utente dal pannello Gestione iscrizione utente.

Sul pannello Gestione iscrizione utente, immettere 3 prima del profilo che si desidera copiare. L'utente visualizza il pannello Copia utente:

```
                                Copia utente

Copia da utente  . . . . :   DPTWH

Immettere le seguenti scelte e quindi premere Invio.

Utente . . . . . .
Descrizione utente. . . .   Reparto Magazzino
Par. d'ord . . . . . .
Tipo di utente. . . . . .   USER
Gruppo di utenti. . . . .

Limit. utiliz. riga comandi  N

Libreria predefinita  . .   DPTWH
Stampante predefinita  . . . .   PRT04
Programma di accesso . . . .   *NONE
  Libreria  . . . . . .
```

Tutti i valori dal profilo dal quale si esegue la copia vengono visualizzati sul pannello Aggiunta utente, ad eccezione dei seguenti valori:

Profilo
Campo vuoto. Da riempire. Fino a 8 caratteri.

Parola d'ordine
Campo vuoto. Se non si immette un valore, il profilo viene creato con la parola d'ordine uguale al valore predefinito specificato per il parametro PASSWORD del comando CRTUSRPRF.

È possibile modificare tutti i campi sul pannello Copia utente. I campi del profilo utente che non appaiono nella versione livello di assistenza di base vengono ancora copiati dal profilo dal quale si esegue la copia, con le seguenti eccezioni:

Coda messaggi
*USRPRF

Parola d'ordine documento
*NONE

Numero identificativo utente
*GEN

Numero identificativo gruppo
*NONE

Associazione EIM
*NOCHG

speciale
*EXCLUDE

Le autorizzazioni private del profilo dal quale si è effettuata la copia non vengono copiate.

Copia delle autorizzazioni private

È possibile copiare le autorizzazioni private da un profilo utente ad un altro utilizzando il comando Concessione autorizzazione utente (GRTUSRAUT).

Ciò non deve essere utilizzato al posto dei profili di gruppo o degli elenchi autorizzazioni. La copia delle autorizzazioni non faciliterà la gestione delle autorizzazioni simili in futuro e può causare dei problemi alle prestazioni sul sistema.

Concetti correlati

"Copia autorizzazione da un utente" a pagina 177
È possibile copiare tutte le autorizzazioni private da un profilo utente su un altro mediante il comando Concessione autorizzazione utente (GRTUSRAUT).

Modifica profili utenti

È possibile modificare un profilo utente utilizzando l'opzione 2 (Modifica) dal pannello Gestione profili utente o dal pannello Gestione iscrizione utente. È inoltre possibile utilizzare il comando CHGUSRPRF (Modifica profilo utente).

Gli utenti che possono immettere i comandi possono modificare alcuni parametri dei propri profili utilizzando il comando CHGPRF (Modifica profilo).

Un utente non può modificare un profilo utente per disporre di più autorizzazioni speciali o possibilità rispetto all'utente che modifica il profilo.

Cancellazione profili utente

L'utente non può cancellare un profilo utente che possiede gli oggetti. Prima che sia possibile cancellare tali profili utente, è necessario cancellare gli oggetti di proprietà del profilo o trasferire la proprietà di quegli oggetti su un altro profilo.

Non è possibile cancellare un profilo utente se è il gruppo principale degli oggetti. Quando si utilizza il livello di assistenza intermedio per cancellare un profilo utente, è possibile modificare o rimuovere il gruppo principale per gli oggetti. L'utente può utilizzare il comando WRKOBJPGP per elencare gli oggetti per i quali un profilo rappresenta il gruppo principale.

Quando si cancella un profilo utente, l'utente viene rimosso da tutti gli elenchi di distribuzione e dall'indirizzo di sistema.

Non è necessario modificarne la proprietà o cancellare la coda messaggi dell'utente. Il sistema cancella automaticamente la coda messaggi quando si cancella il profilo.

Non è possibile cancellare un profilo di gruppo contenente dei membri. Per elencare i membri di un profilo di gruppo, immettere `DSPUSRPRF` *`nome-profilo-gruppo`* `*GRPMBR`. Modificare il campo GRPPRF o SUPGRPPRF in ciascun profilo membro prima di eliminare il profilo di gruppo.

Utilizzo del comando Cancellazione profilo utente

Per cancellare un profilo utente, è possibile immettere il comando DLTUSRPRF (Cancellazione profilo utente) direttamente oppure utilizzare l'opzione 4 (Cancellazione) dal pannello Gestione profili utente.

Il comando DLTUSRPRF dispone di parametri che consentono di gestire:

- Tutti gli oggetti di proprietà del profilo
- Tutti gli oggetti per i quali il profilo rappresenta il gruppo principale
- Associazioni EIM

```
                      Cancellazione profilo utente (DLTUSRPRF)

Immettere le scelte e premere Invio.

Profilo utente . . . . . . . . . . > HOGANR        Nome
Opzione oggetto posseduto:
  Valore oggetto posseduto . . . .   *CHGOWN       *NODLT, *DLT, *CHGOWN
  Nome profilo utente se *CHGOWN     WILLISR       Nome
Opzione gruppo principale:
  Valore gruppo principale . . . .   *NOCHG        *NOCHG, *PGP
  Nuovo gruppo principale . . . .
  Autorizzazione nuovo gruppo principale  .
Associazione EIM  . . . . . . . .   *DLT          *DLT, *NODLT
```

È possibile cancellare tutti gli oggetti posseduti o trasferirli ad un nuovo proprietario. Se si desidera gestire singolarmente gli oggetti posseduti, è possibile utilizzare il comando Gestione oggetti per proprietario (WRKOBJOWN). È possibile modificare il gruppo principale per tutti gli oggetti per i quali il profilo di gruppo rappresenta il gruppo principale. Se si desidera gestire gli oggetti singolarmente, è possibile utilizzare il comando Gestione oggetti per gruppo primario (WRKOBJPGP). I pannelli per entrambi i comandi sono simili:

```
                        Gestione oggetti per proprietario

Profilo utente . . . . . . :   HOGANR

Immettere le opzioni e premere Invio.
  2=Modifica autorizzazione  4=Eliminaz.   5=Visualizzaz. autore
  8=Visualizzazione descrizione   9=Modifica proprietario
                                                          Unità
Opz    Oggetto    Libreria   Tipo    Attributo   ASP
 4   HOGANR        QUSRSYS       *MSGQ                   *SYSBAS
 9   QUERY1        DPTWH         *PGM                    *SYSBAS
 9   QUERY2        DPTWH         *PGM                    *SYSBAS
```

Utilizzo dell'opzione Rimozione utente

È possibile utilizzare l'opzione Rimozione utente sul pannello Gestione iscrizione utente per cancellare un profilo utente.

Dal pannello Gestione iscrizione utente, immettere 4 (Rimozione) prima del profilo che si desidera cancellare. L'utente visualizza il pannello Rimozione utente:

```
                              Eliminazione utente

Utente . . . . . . . . . . :   HOGANR
Descrizione utente . . . . . :   Reparto vendite e marketing


Per eliminare l'utente inserire una delle seguenti opz. e premere Invio.

     1. Fornire tutti gli oggetti di proprietà dell'utente ad un nuovo prop.
     2. Cancel. o cambiare il propr. di ogg. specifici di prop. dell'utente.
```

Per modificare la proprietà di tutti gli oggetti prima di cancellare il profilo, selezionare l'opzione 1. L'utente visualizza un pannello che richiede di inserire il nuovo proprietario.

Per gestire singolarmente gli oggetti, selezionare l'opzione 2. L'utente visualizza il pannello Rimozione utente con i dettagli:

```
                              Eliminazione utente

Utente . . . . . :   HOGANR
Descrizione utente . . . . :   Hogan, Richard - Reparto Magazzino

Nuovo proprietario  . . . . . .     Nome, F4 per el.

Per eliminare l'utente, cancellare o cambiare il proprietario
di tutti gli oggetti.
Immettere le opzioni e premere Invio.
  2=Modifica in nuovo utente   4=Cancellaz.   5=Visualizzaz. dettagli


Opz  Oggetto   Libreria     Descrizione
 4   HOGANR    QUSRSYS      Coda messaggi HOGANR
 2   QUERY1    DPTWH        Query inventario, prospetto a disposiz.
 2   QUERY2    DPTWH        Query inventario, prospetto su ordinaz.
```

Utilizzare le opzioni sul pannello per cancellare gli oggetti o trasferirli a un nuovo proprietario. Quando tutti gli oggetti sono stati rimossi dal pannello, è possibile cancellare il profilo.

Note:

1. È possibile utilizzare il tasto F13 per cancellare tutti gli oggetti di proprietà del profilo utente.
2. I file di spool non vengono visualizzati sul pannello Gestione oggetti per proprietario. È possibile cancellare un profilo utente anche se quel profilo ancora possiede i file di spool. Una volta cancellato un profilo utente, utilizzare il comando Gestione file di spool (WRKSPLF) per individuare e cancellare i file di spool di proprietà del profilo utente, se non sono più necessari.
3. Gli oggetti per i quali il profilo utente cancellato rappresentava il gruppo principale disporre di un gruppo principale *NONE.

Gestione oggetti per autorizzazioni private

È possibile utilizzare il comando Gestione oggetti per autorizzazioni private (WRKOBJPVT) per visualizzare e gestire gli oggetti per i quali un profilo dispone di un'autorizzazione privata.

Gestione oggetti per gruppo primario

È possibile utilizzare il comando Gestione oggetti per gruppo primario (WRKOBJPGP) per visualizzare e gestire gli oggetti per i quali un profilo rappresenta il gruppo principale.

È possibile utilizzare questo pannello per modificare un gruppo principale dell'oggetto su un altro profilo o impostare il gruppo principale relativo su *NONE.

```
                    Gestione oggetti per gruppo primario

Gruppo primario . . . . . :   DPTAR

Immettere le opzioni e premere Invio.
  2=Modifica autorizz.  4=Cancell. 5=Visualizz. autorizzazione
  8=Visualizzazione descrizione    9=Modifica gruppo primario
                                             Unità
Opz    Oggetto    Libreria   Tipo    Attributo   ASP
       CUSTMAST   CUSTLIB    *FILE               *SYSBAS
       CUSTWRK    CUSTLIB    *FILE               *SYSBAS
       CUSTLIB    QSYS       *LIB                *SYSBAS
```

Abilitazione di un profilo utente

Se i valori di sistema QMAXSIGN e QMAXSGNACN sul sistema sono impostati in modo da disabilitare un profilo utente dopo un numero troppo elevato di tentativi di verifica della parola d'ordine, potrebbe essere necessario abilitare il profilo modificando lo stato del profilo in *ENABLED.

Per abilitare un profilo utente, è necessario disporre dell'autorizzazione speciale *SECADM, e delle autorizzazioni *OBJMGT e *USE al profilo utente. Solitamente, un operatore di sistema non dispone dell'autorizzazione speciale *SECADM. Una soluzione è data dall'utilizzo di un programma di esempio che adotta l'autorizzazione:

1. Creare un programma CL di proprietà di un utente con l'autorizzazione speciale *SECADM, e le autorizzazioni *OBJMGT e *USE ai profili utenti sul sistema. Adottare l'autorizzazione del proprietario durante la creazione del programma specificando USRPRF(*OWNER).
2. Utilizzare il comando EDTOBJAUT per creare l'autorizzazione pubblica sul programma *EXCLUDE e fornire agli operatori di sistema l'autorizzazione *USE.
3. L'operatore abilita il profilo immettendo il *nome-profilo* `CALL ENABLEPGM` .
4. La parte principale del programma ENABLEPGM appare così:

```
PGM &PROFILE
DCL VAR(&PROFILE) TYPE(*CHAR) LEN(10)
CHGUSRPRF USRPRF(&PROFILE) STATUS(*ENABLED)
ENDPGM
```

Elenco profili utente

È possibile visualizzare e stampare le informazioni sui profili utente in diversi formati.

Visualizzazione di un singolo profilo

Per visualizzare i valori di un singolo profilo utente, utilizzare l'opzione 5 (visualizzazione) dal pannello Gestione iscrizione utente o dal pannello Gestione profili utente. In alternativa, è possibile utilizzare il comando DSPUSRPRF (Visualizzazione profilo utente).

Elenco di tutti i profili

È possibile utilizzare il comando DSPAUTUSR (Visualizzazione utenti autorizzati)per stampare o visualizzare tutti i profili utente presenti sul sistema.

Il parametro sequenza (SEQ) sul comando consente di ordinare l'elenco in base al nome del profilo o al profilo di gruppo.

```
                          Visualizzazione utenti autorizzati

                        Ultima
Profilo     Profilo     modifica  Nessuna
gruppo      utente      par. ord. par. ord. Testo
DPTSM
            ANDERSR     08/04/0x            Anders, Roger
            VINCENT     09/15/0x            Vincent, Mark
DPTWH
            ANDERSR     08/04/0x            Anders, Roger
            HOGANR      09/06/0x            Hogan, Richard
            QUINN       09/06/0x            Quinn, Rose
QSECOFR
            JONESS      09/20/0x            Jones, Sharon
            HARRISON    08/29/0x            Harrison, Ken
*NO GROUP
            DPTSM       09/05/0x     X      Vendite e MKTG
            DPTWH       09/18/0x     X      Magazzino
```

Premendo F11, l'utente è in grado di visualizzare i profili utente con parole d'ordine definite da utilizzare nei diversi livelli di parola d'ordine.

```
                       Visualizzazione utenti autorizzati

                     Par. ord. Livello    Livello                Locale
Utente    Gruppo     Ultimo    0 o 1      2 o 3      Netserver   Parola d'ordine
Profilo   Profilo    Modificato Par.ord.   Par.ord.   Par.ord.    Gestione
ANGELA               04/21/0x   *YES       *NO        *YES        *YES
ARTHUR               07/07/0x   *YES       *YES       *YES        *YES
CAROL1               05/15/0x   *YES       *YES       *YES        *YES
CAROL2               05/15/0x   *NO        *NO        *NO         *NO
CHUCKE               05/18/0x   *YES       *NO        *YES        *YES
DENNISS              04/20/0x   *YES       *NO        *YES        *YES
DPORTER              03/30/0x   *YES       *NO        *YES        *YES
GARRY                08/04/0x   *YES       *YES       *YES        *YES
JANNY                03/16/0x   *YES       *NO        *YES        *YES
```

Tipi di visualizzazione del profilo utente

Il comando DSPUSRPRF (Visualizzazione profilo utente) fornisce diversi tipi di visualizzazione ed elenchi.

- Alcune visualizzazioni ed elenchi sono disponibili solo per i profili individuali. Altri possono essere stampati per tutti i profili o una serie di profili generici.
- È possibile creare un file di emissione da alcune visualizzazioni specificando l'emissione (*OUTFILE). Utilizzare un programma o uno strumento di query per produrre prospetti personalizzati dal file di emissione. "Analisi profili utente" a pagina 324 fornisce suggerimenti per i prospetti.

Tipi di prospetti del profilo utente

È possibile generare prospetti del profilo utente utilizzando il comando PRTUSRPRF (Stampa profilo utente) o il comando ANZDFTPWD (Analisi parola d'ordine predefinita).

- Stampa profilo utente (PRTUSRPRF)

  Questo comando genera prospetti che contengono informazioni relative ai profili utente sul sistema. È possibile stampare quattro differenti variazioni di questo prospetto. Uno contiene le informazioni sul tipo di autorizzazione, uno contiene le informazioni sul tipo di ambiente, uno contiene le informazioni sul tipo di parola d'ordine e uno contiene le informazioni sul tipo di livello di parola d'ordine.
- Analisi parola d'ordine predefinita (ANZDFTPWD)

Questo comando genera un prospetto riguardante tutti i profili utente sul sistema che dispongono di una parola d'ordine predefinita e consente di eseguire delle azioni sui profili. Un profilo dispone di una parola d'ordine predefinita quando il nome del profilo utente corrisponde alla parola d'ordine del profilo.

I profili utente sul sistema che dispongono di una parola d'ordine predefinita possono essere disabitati e le rispettive parole d'ordine possono essere impostate su scadute.

Ridenominazione di un profilo utente

Il sistema non fornisce un metodo diretto per la ridenominazione di un profilo utente. È possibile creare un nuovo profilo con le stesse autorizzazioni per un utente con un nuovo nome.

Alcune informazioni, tuttavia, non possono essere trasferite al nuovo profilo. Di seguito vengono riportati degli esempi di informazioni che non possono essere trasferite:

- File di spool.
- Oggetti interni contenenti preferenze utente e altre informazioni sull'utente andranno persi.
- I certificati digitali che contengono il nome utente verranno invalidati.
- Le informazioni sull'uid e sul gid conservate dall'IFS non possono essere modificate.
- L'utente non è in grado di modificare le informazioni memorizzate dalle applicazioni contenenti il nome utente.

Le applicazioni eseguite dall'utente possono disporre di profili di applicazioni. La creazione di un nuovo profilo utente i5/OS per ridenominare un utente non implica la ridenominazione dei profili delle applicazioni di cui un utente può disporre. Un profilo Lotus Notes è un esempio di un profilo delle applicazioni.

Il seguente esempio mostra come creare un nuovo profilo per un utente con un nuovo nome e le stesse autorizzazioni. Il vecchio nome del profilo è SMITHM, mentre il nuovo nome del profilo utente è JONESM:

1. Copiare il vecchio profilo (SMITHM) su un nuovo profilo (JONESM) utilizzando l'opzione di copia dal pannello Gestione iscrizione utente.
2. Fornire a JONESM tutte le autorizzazioni private di SMITHM utilizzando il comando GRTUSRAUT (Concessione autorizzazione utente):

   ```
   GRTUSRAUT JONESM REFUSER(SMITHM)
   ```

3. Modificare il gruppo principale di tutti gli oggetti di cui SMITHM è il gruppo principale utilizzando il comando WRKOBJPGP (Gestione oggetti per gruppo principale):

   ```
   WRKOBJPGP PGP(SMITHM)
   ```

   Immettere l'opzione 9 su tutti gli oggetti che devono modificare il proprio gruppo principale e immettere NEWPGP (JONESM) sulla riga comandi.

   Nota: è necessario assegnare un gid a JONESM mediante il parametro GID sul comando CRTUSRPRF o CHGUSRPRF (Creazione o Modifica profilo utente).
4. Visualizzare il profilo utente SMITHM utilizzando il comando DSPUSRPRF (Visualizzazione profilo utente):

   ```
   DSPUSRPRF USRPRF(SMITHM)
   ```

   Annotare l'uid
   e il gid per SMITHM.
5. Trasferire a JONESM la proprietà di tutti gli altri oggetti posseduti e rimuovere il profilo utente SMITHM, utilizzando l'opzione (Rimozione) dal pannello Gestione iscrizione utente.
6. Modificare l'uid e il gid di JONESM nell'uid e nel gid appartenenti a SMITHM utilizzando il comando CHGUSRPRF (Modifica profilo utente):

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

Se JONESM possiede gli oggetti contenuti in un indirizzario, il comando CHGUSRPRF non può essere utilizzato per modificare l'uid e il gid. Utilizzare la API QSYCHGID per modificare l'uid e il gid del profilo utente JONESM.

Gestione controllo utente

È possibile utilizzare il comando CHGUSRAUD (Modifica controllo utente) per impostare le caratteristiche di controllo per gli utenti.

Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *AUDIT.

```
          Modifica controllo
utente (CHGUSRAUD)

Immettere le scelte e premere Invio.

Profilo utente . . . . . .   HOGANR
               + per altri valori   JONESS
Valore di controllo oggetto . . . . .   *SAME
Controllo azione utente . . . . . .   *CMD
               + per altri valori   *SERVICE
```

È possibile specificare le caratteristiche di controllo per più di un utente alla volta, elencando i nomi dei profili utente.

Il parametro AUDLVL (controllo azione utente) può disporre di più di un valore. I valori specificati non vengono aggiunti ai valori AUDLVL correnti per gli utenti ma sostituiscono i valori AUDLVL correnti.

Se si dispone dell'autorizzazione speciale *ALLOBJ o *AUDIT, è possibile utilizzare il comando Visualizzazione profilo utente (DSPUSRPRF) per vedere le caratteristiche di controllo per un utente.

Gestione profili nei programmi CL

È possibile gestire profili utente all'interno di un programma CL.

È possibile voler richiamare le informazioni sul profilo utente da un programma CL. È possibile utilizzare il comando Richiamo profilo utente (RTVUSRPRF) nel programma CL. Il comando restituisce gli attributi richiesti del profilo alle variabili che l'utente associa ai nomi del campo dei profili utente. Le descrizioni dei campi dei profili utente in questa sezione mostrano le lunghezze del campo previste dal comando RTVUSRPRF. In alcuni casi, un campo decimale può disporre anche di un valore non numerico. Ad esempio, il campo della memoria massima (MAXSTG) viene definito come campo decimale, ma può disporre di un valore *NOMAX. Le informazioni in linea per il comando RVTUSRPRF descrive i valori restituiti in un campo decimale per i valori non numerici.

Il programma di esempio in "Utilizzo di un programma di approvazione della parola d'ordine" a pagina 66 mostra un esempio su come utilizzare il comando RTVUSRPRF.

È possibile inoltre voler utilizzare il comando CRTUSRPRF o CHGUSRPRF all'interno di un programma CL. Se si utilizzano le variabili per i parametri di questi comandi, definire le variabili come campi di carattere in modo da corrispondere al pannello di richiesta Creazione profilo utente. Non è necessario che le dimensioni delle variabili corrispondano alle dimensioni del campo.

Non è possibile richiamare la parola d'ordine dell'utente, poiché la parola d'ordine viene memorizzata con una codifica a senso unico. Se si desidera che l'utente inserisca nuovamente la parola d'ordine prima di accedere alle informazioni critiche, è possibile utilizzare il comando Controllo parola d'ordine

(CHKPWD) nel programma. Il sistema confronta la parola d'ordine immessa come parola d'ordine dell'utente e invia un messaggio di uscita al programma se la parola d'ordine non è corretta.

Punti di uscita del profilo utente

È possibile scrivere i propri programmi di uscita per eseguire funzioni specifiche del profilo utente. Quando si registrano i programmi di uscita con uno qualsiasi dei punti di uscita del profilo utente, l'utente viene informato della creazione, della modifica, della cancellazione o del ripristino del profilo utente.

Nel momento della notifica, il programma di uscita può eseguire una delle seguenti operazioni:

- Richiamare le informazioni sul profilo utente.
- Iscrivere il profilo utente appena creato nell'indirizzario di sistema.
- Creare gli oggetti necessari per il profilo utente.

Nota: tutte le autorizzazioni adottate verranno soppresse prima di richiamare i programmi di uscita. Ciò indica che il programma di uscita non può avere l'autorizzazione per accedere all'oggetto del profilo utente.

Informazioni correlate

Exit programs

profili utente forniti da IBM

Un numero di profili utente viene fornito con il software di sistema. Questi profili utente forniti da IBM vengono utilizzati come proprietari dell'oggetto per diverse funzioni di sistema. Alcune funzioni di sistema vengono anche eseguite tramite specifici profili utente forniti da IBM.

Per consentire all'utente di installare il sistema la prima volta, la parola d'ordine per il profilo del responsabile della riservatezza (QSECOFR) è la stessa per ogni sistema fornito. Tuttavia, la parola d'ordine per QSECOFR viene fornita come scaduta. Per i nuovi sistemi, all'utente viene richiesto di modificare la parola d'ordine la prima volta che si collega come QSECOFR.

Quando si installa un nuovo release del sistema operativo, le parole d'ordine per i profili forniti da IBM non vengono modificati. Se i profili quali QPGMR e QSYSOPR dispongono di parola d'ordine, queste non vengono impostate su *NONE automaticamente.

Appendice B, "Profili utente forniti da IBM", a pagina 341 contiene un elenco completo di tutti i profili utente forniti da IBM e di tutti i valori campo relativi a ciascun profilo.

Nota: Tutti i profili utente forniti da IBM, tranne QSECOFR vengono forniti con una parola d'ordine *NONE e non sono concepiti per l'accesso. Tali profili vengono utilizzati dal sistema operativo IBM i5/OS . Per questo motivo, l'accesso a tali profili o l'utilizzo dei profili per possedere gli oggetti utente (non forniti da IBM) non è consigliato.

Concetti correlati

"Profili utente forniti da IBM" a pagina 276
È possibile eseguire attività di controllo sui profili utente forniti da IBM tramite la verifica delle relative parole d'ordine.

Modifica delle parole d'ordine per i profili utente forniti da IBM

Qualora fosse necessario accedere ad uno dei profili forniti da IBM, è possibile modificare la parola d'ordine utilizzando il comando CHGUSRPRF. È possibile inoltre modificare queste parole d'ordine utilizzando un'opzione dal menu SETUP.

Per proteggere il sistema, è opportuno lasciare la parola d'ordine impostata su *NONE per tutti i profili forniti da IBM, tranne QSECOFR. Non consentire l'utilizzo di parole d'ordine banali per il profilo

QSECOFR.

```
                  Modifica par. d'ord. per uten. forniti da IBM

Inserire la nuova par. d'ord. per l'uten. fornito da IBM,
inserirla nuovamente per verificare la modifica, quindi
premere Invio.

Nuova parola d'ordine resp. sicurezza (QSECOFR)  . .
  Nuova parola d'ordine (da verificare) . . . . . .

Nuova parola d'ordine oper. sistema (QSYSOPR)  . . .
  Nuova parola d'ordine (da verificare) . . . . . .

Nuova parola d'ordine programmatore (QPGMR)  . . . .
  Nuova parola d'ordine (da verificare) . . . . . .

Nuova parola d'ordine utente (QUSER)  . . . . . .
  Nuova parola d'ordine (da verificare) . . . . . .

Nuova parola d'ordine servizio (QSRV)  . . . . . .
  Nuova parola d'ordine (da verificare) . . . . . .
```

Pag. giù per modificare altre parole d'ordine:

```
                  Modifica par. d'ord. per uten. forniti da IBM

Inserire nuova par. d'ord. per l'utente fornito da IBM,
immettere la modifica e premere quindi Invio.

Nuova parola d'ordine servizio di base (QSRVBAS) . .
  Nuova parola d'ordine (da verificare) . . . . . .
```

Gestione ID utente programmi di manutenzione

Sono disponibili diversi miglioramenti e aggiunte ai programmi di manutenzione di manutenzione che ne facilitano l'utilizzo e la comprensione.

- **SST (System service tools)**

  È possibile ora gestire e creare gli ID utente dei programmi di manutenzione dagli SST (system service tools) selezionando l'opzione 8 (Gestione ID utente programmi di manutenzione) dal pannello SST principale. L'utente non ha più bisogno di entrare nel DST (Dedicated service tools) per reimpostare le parole d'ordine, garantire o revocare i privilegi oppure creare gli ID utente dei programmi di manutenzione. **Nota**: le informazioni relative ai programmi di manutenzione sono state spostate nell'information center.

- **Miglioramenti gestione parole d'ordine**

  Il server viene fornito con la possibilità limitata di modificare le parole d'ordine predefinite e scadute. Ciò indica che non è possibile modificare gli ID utente con parole d'ordine predefinite e scadute utilizzando la API Modifica ID utente programmi di manutenzione (QSYCHGDS) e non è possibile neanche modificare le relative parole d'ordine mediante SST. L'utente, mediante il DST, può solo modificare un ID utente del programma di manutenzione con associata una parola d'ordine predefinita e scaduta. Inoltre, è possibile modificare l'impostazione per consentire la modifica delle parole d'ordine predefinite e scadute. Inoltre, è possibile utilizzare il nuovo privilegio Modifica programmi di manutenzione (STRSST) per creare un ID utente del programma di manutenzione in grado di accedere al DST, ma può essere limitato nell'accedere all'SST.

- **Modifiche terminologiche**

I dati di testo e altre documentazioni sono stati modificati per rispecchiare la terminologia del nuovo programma di manutenzione. Nello specifico, il termine ID utente programma di manutenzione sostituisce i termini precedenti, quali profili utente DST, ID utente DST, profili utente dei programmi di manutenzione o le variazioni di questi nomi.

Concetti correlati

"Profili utente forniti da IBM" a pagina 276
È possibile eseguire attività di controllo sui profili utente forniti da IBM tramite la verifica delle relative parole d'ordine.

Informazioni correlate

Gestione degli ID utente dei programmi di manutenzione

Parola d'ordine del sistema

La parola d'ordine del sistema viene utilizzata per autorizzare le modifiche del modello di sistema, determinate condizioni di servizio e le modifiche alle proprietà. Se queste modifiche sono state eseguite sul sistema, è possibile che all'utente venga richiesta la parola d'ordine del sistema quando si esegue un IPL.

Capitolo 5. Sicurezza delle risorse

Questa sezione descrive ognuno dei componenti della sicurezza delle risorse e spiega come partecipino alla protezione delle informazioni sul sistema. Inoltre, questo capitolo spiega come utilizzare i comandi CL e i pannelli per impostare la sicurezza delle risorse sul sistema.

La sicurezza delle risorse definisce quali utenti sono abilitati all'utilizzo degli oggetti sul sistema e quali operazioni possono eseguire su quegli oggetti.

Capitolo 7, "Progettazione sicurezza", a pagina 235 tratta le tecniche per la creazione della sicurezza delle risorse, compreso il modo in cui influisce sulla creazione delle applicazioni e sulle prestazioni del sistema.

L'argomento "Controllo dell'autorizzazione da parte del sistema" a pagina 182 fornisce diagrammi di flusso e note dettagliati sulla modalità di controllo delle autorizzazioni da parte del sistema. La consultazione di tali informazioni può risultare particolarmente utile man mano che si leggono le spiegazioni riportate di seguito.

Concetti correlati

"Sicurezza delle risorse" a pagina 5
La capacità di accedere ad un oggetto viene chiamata *autorizzazione*. La sicurezza delle risorse sul sistema operativo i5/OS consente di controllare le autorizzazioni oggetto definendo chi può utilizzare gli oggetti e in che modo è possibile utilizzarli.

"Consigli generali per la struttura della sicurezza" a pagina 236
Se la struttura della sicurezza è semplice risulterà più facile gestirla e controllarla. Inoltre, in questo modo miglioreranno le prestazioni dell'applicazione e delle procedure per la copia di riserva.

Definizione degli utenti che possono accedere alle informazioni

È possibile fornire l'autorizzazione ai singoli utenti, a gruppi di utenti e al pubblico.

Nota: in alcuni ambienti, l'autorizzazione di un utente viene considerata come **privilegio**.

L'utente definisce chi può utilizzare un oggetto in diversi modi:

Autorizzazione pubblica:
L'**autorizzazione pubblica** è composta da tutti coloro che sono autorizzati ad accedere al sistema. L'autorizzazione pubblica viene definita per ogni oggetto sul sistema, sebbene l'autorizzazione pubblica di un oggetto può essere *EXCLUDE. L'autorizzazione pubblica ad un oggetto viene utilizzata qualora non venisse rilevata un'altra autorizzazione specifica per l'oggetto.

Autorizzazione privata:
È possibile definire l'autorizzazione specifica per utilizzare (o meno) un oggetto. È possibile concedere l'autorizzazione ad un profilo utente individuale o ad un profilo di gruppo. Un oggetto dispone dell'**autorizzazione privata** se una qualsiasi autorizzazione diversa da quella pubblica, la proprietà dell'oggetto o l'autorizzazione al gruppo principale viene definita per l'oggetto.

Autorizzazione utente:
I singoli profili utente possono disporre dell'autorizzazione all'utilizzo degli oggetti sul sistema. Questo è un tipo di autorizzazione privata.

Autorizzazione gruppo:
I profili di gruppo possono disporre dell'autorizzazione all'utilizzo degli oggetti sul sistema. Un membro del gruppo ottiene l'autorizzazione del gruppo a meno che non sia stata definita specificatamente un'autorizzazione per tale utente. Anche l'autorizzazione del gruppo viene considerata come autorizzazione privata.

Proprietà oggetto:
Ogni oggetto sul sistema dispone di un proprietario. Il proprietario dispone dell'autorizzazione *ALL sull'oggetto, per impostazione predefinita. Tuttavia, l'autorizzazione del proprietario sull'oggetto può essere modificata o rimossa. L'autorizzazione del proprietario sull'oggetto non è considerata come autorizzazione privata.

Autorizzazione gruppo principale:
È possibile specificare un gruppo principale per un oggetto e l'autorizzazione che il gruppo principale dispone sull'oggetto. L'autorizzazione del gruppo principale viene memorizzata con l'oggetto e può fornire prestazioni migliori rispetto all'autorizzazione privata concessa ad un profilo di gruppo. Solo un profilo utente con un numero gid (group identification number) può essere il gruppo principale per un oggetto. L'autorizzazione del gruppo principale non è considerata come autorizzazione privata.

Definizione della modalità di accesso alle informazioni

È possibile definire quali operazioni possono essere eseguite su oggetti, dati e campi.

Autorizzazione indica il tipo di accesso consentito ad un oggetto. Le diverse operazioni richiedono tipi differenti di autorizzazione.

Nota: in alcuni ambienti, l'autorizzazione associata ad un oggetto viene definita la **modalità di accesso** dell'oggetto.

L'autorizzazione ad un oggetto si divide in tre categorie:

1. **Autorizzazione oggetto** definisce le operazioni che possono essere effettuate sull'oggetto nel suo intero.
2. **Autorizzazione dati** definisce le operazioni che possono essere effettuate sul contenuto dell'oggetto.
3. **Autorizzazione campo** definisce le operazioni che possono essere effettuate sui campi di dati.

La Tabella 115 descrive i tipi di autorizzazione disponibili ed elenca alcuni esempi di come vengono utilizzate le autorizzazioni. Nella maggior parte dei casi, l'accesso ad un oggetto richiede una combinazione di autorizzazioni oggetto, dati e campo. Appendice D, "Autorizzazione richiesta per gli oggetti utilizzati dai comandi", a pagina 361 fornisce informazioni sull'autorizzazione richiesta per eseguire una funzione specifica.

Tabella 115. Descrizione dei tipi di autorizzazione

speciale	Nome	Funzioni consentite
Autorizzazioni oggetto:		
*OBJOPR	Operativo oggetto	Controllare la descrizione di un oggetto. Utilizzare l'oggetto come stabilito dalle autorizzazioni dati dell'utente.
*OBJMGT	Gestione oggetto	Specificare la sicurezza per l'oggetto. Spostare o rinominare l'oggetto. Tutte le funzioni definite per *OBJALTER e *OBJREF.
*OBJEXIST	Esistenza oggetto	Cancellare l'oggetto. Liberare la memoria dell'oggetto. Eseguire le operazioni di salvataggio e ripristino per l'oggetto [1]. Trasferire la proprietà dell'oggetto.
*OBJALTER	Modifica oggetto	Aggiungere, eliminare, inizializzare e riorganizzare i membri dei file di database. Modificare e aggiungere gli attributi dei file di database: aggiungere e rimuovere i trigger. Modificare gli attributi dei pacchetti SQL.

Tabella 115. Descrizione dei tipi di autorizzazione (Continua)

speciale	Nome	Funzioni consentite
*OBJREF	Riferimento oggetto	Specificare un file di database come principale in un limite di riferimento. Ad esempio, si desidera definire una regola secondo la quale un record del cliente deve esistere nel file CUSMAS prima che un ordine per il cliente possa essere aggiunto al file CUSORD. È necessaria l'autorizzazione *OBJREF al file CUSMAS per poter definire questa regola.
*AUTLMGT	Gestione elenco autoriz.	Aggiungere e rimuovere gli utenti e le relative autorizzazioni dall'elenco di autorizzazioni [2].
Autorizzazioni dati:		
*READ	Lettura	Visualizzare il contenuto dell'oggetto, come ad esempio la visualizzazione dei record in un file.
*ADD	Aggiunta	Aggiungere le voci ad un oggetto, come ad esempio l'aggiunta dei messaggi ad una coda messaggi o l'aggiunta dei record ad un file.
*UPD	Aggiornam.	Modificare le voci in un oggetto, come ad esempio la modifica dei record in un file.
*DLT	Cancellazione	Rimuovere le voci da un oggetto, come ad esempio la rimozione dei messaggi da una coda messaggi o la cancellazione dei record da un file.
*EXECUTE	Esecuz.	Eseguire un programma, programma di manutenzione o pacchetto SQL. Individuare un oggetto in una libreria o in un indirizzario.
Autorizzazioni campo:		
*MGT	Gestione	Specificare la sicurezza per il campo.
*ALTER	Modifica	Modificare gli attributi del campo.
*REF	Riferimento	Specificare il campo come parte della chiave principale in un limite di riferimento.
*READ	Lettura	Accedere al contenuto del campo. Ad esempio, visualizzare il contenuto del campo.
*ADD	Aggiunta	Aggiungere le voci ai dati, come ad esempio aggiungere le informazioni ad un campo specifico.
*UPDATE	Aggiornam.	Modificare il contenuto delle voci esistenti nel campo.

[1] Se un utente dispone dell'autorizzazione speciale al sistema di salvataggio (*SAVSYS), non è necessaria l'autorizzazione all'esistenza dell'oggetto per l'esecuzione delle operazioni di salvataggio e ripristino sull'oggetto.

[2] Consultare l'argomento "Gestione elenco autorizzazioni" a pagina 149 per ulteriori informazioni.

Attività correlate

"Passaggio al livello 30 da un livello inferiore" a pagina 13
Quando si passa al livello di sicurezza 30 da un livello di sicurezza inferiore, il sistema modifica tutti i profili utente per aggiornare le autorizzazioni speciali la prossima volta che si esegue un IPL (initial program load).

Riferimenti correlati

"Autorizzazione gruppo" a pagina 105
Se il profilo utente è un membro di un gruppo ed è stato specificato OWNER(*USRPRF), il campo Autorizzazione gruppo controlla quale autorizzazione viene fornita al profilo di gruppo per gli oggetti creati da questo utente.

Autorizzazioni comunemente utilizzate

È possibile specificare alcune serie di autorizzazioni oggetti e dati.

Determinate serie di autorizzazioni dati e oggetti vengono comunemente richieste per eseguire le operazioni sugli oggetti. È possibile specificare queste serie di autorizzazioni definite dal sistema (*ALL, *CHANGE, *USE) invece di definire singolarmente le autorizzazioni necessarie per un oggetto. L'autorizzazione *EXCLUDE è diversa rispetto al non disporre di alcuna autorizzazione. L'autorizzazione *EXCLUDE nega, nello specifico, l'accesso all'oggetto. Non disporre di alcuna autorizzazione significa che l'utente utilizza l'autorizzazione pubblica definita per l'oggetto. La Tabella 116 mostra le autorizzazioni definite dal sistema disponibili utilizzando i comandi e i pannelli dell'autorizzazione sull'oggetto.

Tabella 116. Autorizzaz. definita dal sistema

speciale	***ALL**	***CHANGE**	***USE**	***EXCLUDE**
Autorizzazioni oggetto				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
Autorizzazioni dati				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X		
*DLT	X	X		
*EXECUTE	X	X	X	

La Tabella 117 mostra le autorizzazioni aggiuntive definite dal sistema, disponibili utilizzando i comandi WRKAUT e CHGAUT:

Tabella 117. Autorizzaz. definita dal sistema

speciale	***RWX**	***RW**	***RX**	***R**	***WX**	***W**	***X**
Autorizzazioni oggetto							
*OBJOPR	X	X	X	X	X	X	X
*OBJMGT							
*OBJEXIST							
*OBJALTER							
*OBJREF							
Autorizzazioni dati							
*READ	X	X	X	X			
*ADD	X	X			X	X	
*UPD	X	X			X	X	
*DLT	X	X			X	X	
*EXECUTE	X		X		X		X

Il programma su licenza LAN Server utilizza gli elenchi di controllo agli accessi per gestire l'autorizzazione. Le autorizzazioni di un utente vengono definite **permessi**. La Tabella 118 a pagina 145

mostra come i permessi Server LAN corrispondano alle autorizzazioni oggetti e dati:

Tabella 118. Autorizzazioni Server LAN

Autorizzazione	**Autorizzazioni Server LAN**
*EXCLUDE	Nessuna
Autorizzazioni oggetto	
*OBJOPR	Consultare nota 1
*OBJMGT	Autorizzazione
*OBJEXIST	Creazione, Cancellazione
*OBJALTER	Attributo
*OBJREF	Nessun equivalente
Autorizzazioni dati	
*READ	Lettura
*ADD	Creazione
*UPD	Scrittura
*DLT	Cancellazione
*EXECUTE	Esecuz.

1 A meno che non sia specificato NONE per un utente nell'elenco di controllo dell'accesso, all'utente viene implicitamente fornito *OBJOPR.

Definizione delle informazioni a cui è possibile accedere

È possibile definire la sicurezza delle risorse per i singoli oggetti sul sistema. Inoltre, è possibile definire la sicurezza per i gruppi di oggetti utilizzando la sicurezza delle librerie o un elenco di autorizzazioni.

Sicurezza libreria

È possibile utilizzare la sicurezza libreria per proteggere le informazioni.

La maggior parte degli oggetti sul sistema risiede nelle librerie. Per accedere ad un oggetto, è necessario disporre dell'autorizzazione sia sull'oggetto stesso che sulla libreria nella quale risiede l'oggetto. Per la maggior parte delle operazioni, compresa la cancellazione di un oggetto, l'autorizzazione *USE sulla libreria dell'oggetto è sufficiente (oltre all'autorizzazione richiesta per l'oggetto). La creazione di un nuovo oggetto richiede l'autorizzazione *ADD sulla libreria dell'oggetto. Appendice D, "Autorizzazione richiesta per gli oggetti utilizzati dai comandi", a pagina 361 mostra che l'autorizzazione è richiesta dai comandi CL per gli oggetti e le librerie degli oggetti.

Utilizzare la sicurezza delle librerie è una tecnica che consente di proteggere le informazioni conservando nel contempo uno schema della sicurezza semplice. Ad esempio, per proteggere le informazioni riservate per una serie di applicazioni, è possibile eseguire le operazioni elencate di seguito:

- Utilizzare una libreria per memorizzare tutti i file confidenziali per un particolare gruppo di applicazioni.
- Assicurarsi che l'autorizzazione pubblica sia sufficiente per tutti gli oggetti (nella libreria) che vengono utilizzati dalle applicazioni (*USE o *CHANGE).
- Limitare l'autorizzazione pubblica alla libreria stessa (*EXCLUDE).
- Fornire ai gruppi selezionati o agli individui l'autorizzazione alla libreria (*USE o *ADD se le applicazioni la richiedono).

Sebbene la sicurezza delle librerie rappresenti un metodo semplice ma efficace nella protezione delle informazioni, potrebbe rivelare inadeguata per i dati con elevati requisiti di sicurezza. Gli oggetti estremamente sensibili dovrebbero essere protetti individualmente o con un elenco di autorizzazioni, piuttosto che basarsi sulla sicurezza delle librerie.

Concetti correlati

"Pianificazione delle librerie" a pagina 241
Una libreria è come un indirizzario utilizzato per individuare gli oggetti nella libreria. Molti fattori influenzano la scelta su come raggruppare le informazioni relative all'applicazione in librerie e su come gestire queste librerie.

Sicurezza libreria ed elenchi di librerie

Quando una libreria viene aggiunta ad un elenco di librerie dell'utente, l'autorizzazione di cui dispone l'utente sulla libreria viene memorizzata con le informazioni dell'elenco di librerie.

L'autorizzazione dell'utente sulla libreria rimane per l'intero lavoro, anche se l'autorizzazione dell'utente sulla libreria viene revocata mentre il lavoro è ancora attivo.

Quando viene richiesto l'accesso ad un oggetto ed è stato specificato *LIBL per l'oggetto stesso, le informazioni dell'elenco librerie vengono utilizzate per controllare l'autorizzazione per la libreria. Se si specifica un nome qualificato, l'autorizzazione per la libreria viene specificatamente controllata, anche se la libreria viene inserita nell'elenco di librerie dell'utente.

Attenzione: se un utente sta utilizzando un'autorizzazione adottata quando si aggiunge una libreria all'elenco di librerie, l'utente conserva l'autorizzazione sulla libreria anche quando questo non sta più utilizzando l'autorizzazione adottata. Questo rappresenta un rischio per la sicurezza. Le voci aggiunte ad un elenco di librerie dell'utente da un programma che utilizza l'autorizzazione adottata dovrebbero essere rimosse prima che termini il programma con l'autorizzazione adottata.

Inoltre, le applicazioni che utilizzano gli elenchi delle librerie piuttosto che i nomi qualificati delle librerie corrono un rischio maggiore in materia di sicurezza. Un utente autorizzato all'utilizzo dei comandi per la gestione degli elenchi di librerie può potenzialmente utilizzare una versione differente di un programma.

Riferimenti correlati

"Elenchi librerie" a pagina 222
L'**elenco librerie** per un lavoro indica le librerie in cui effettuare le ricerche e l'ordine in cui le ricerche devono essere effettuate.

Autorizzazioni campo

È possibile specificare autorizzazioni campo per file di database.

Le autorizzazioni campo sono supportate per i file di database. le autorizzazione supportate sono Gestione, Modifica, Riferimento, Lettura, Aggiunta e Aggiornamento. È possibile amministrare queste autorizzazioni solo mediante le istruzioni SQL, GRANT e REVOKE. È possibile visualizzare queste autorizzazioni mediante i comandi Visualizzazione autorizzazione oggetto (DSPOBJAUT) e Editazione autorizzazione oggetto (EDTOBJAUT). Con il comando EDTOBJAUT è possibile solo visualizzare le autorizzazioni campo e non modificarle.

```
                          Visualizzazione autorizzazione oggetto

Oggetto . . . . . :   PLMITXT     Proprietario. . . . . :   PGMR1
  Libreria . . . . :   RLN         Gruppo principale  . . . :   DPTAR
Tipo di oggetto. :   *FILE       Unità ASP  . . . . . :   *SYSBAS

L'oggetto protetto dall'elenco di autorizzazioni  . . :   *NONE
                       Autorizz.  ---------------Dati---------------
Utente     Gruppo      oggetto   Lett. Agg. Aggior. Canc.   Esecuz.
*PUBLIC                *CHANGE     X     X     X       X       X
PGMR1                  *ALL        X     X     X       X       X
USER1                  *USE        X                           X
USER2                  USER DEF    X           X               X
USER3      USER DEF               X    X



Premere Invio per continuare


F3=Fine  F11=Non visual. dettagli F12=Annullamento F16=Visualizzazione
autorizzazione campo
```

Figura 4. Pannello Visualizzazione autorizzazione oggetto che riporta F16=Visualizzazione autorizzazione campo. Questo tasto funzione verrà visualizzato quando un file di database dispone di autorizzazioni campo.

```
                          Visualizzazione autorizzazione campo

Oggetto . . . . . :   PLMITXT     Proprietario. . . . . :   PGMR1
  Libreria  . . . . :   RLN         Gruppo principale  . . . :   *NONE
Tipo oggetto  . . . . :   *FILE

                        Oggetto   -----Autorizzazioni campo-----------
Campo        Utente     Autoriz.   Mgt  Modif Rif  Let.  Agg. Aggiorn.
Campo3       PGMR1      *ALL        X      X   X    X     X      X
             USER1      *Use                        X
             USER2      USER DEF                    X            X
             USER3      USER DEF                X   X
             *PUBLIC    *CHANGE                     X     X      X
Campo4       PGMR1      *ALL        X      X        X     X      X
             USER1      *Use                        X
             USER2      USER DEF                    X
             USER3      USER DEF                    X
             *PUBLIC    *CHANGE                     X     X      X
                                                                Altro
Premere Invio per continuare.

F3=Fine F5=Rivis. F12=Annull. F16=Rip. inizio elen. da F17=In. elen. da
```

Figura 5. Pannello Visualizzazione autorizzazione campo. Quando si seleziona "F17=Inizio elenco da" verrà visualizzata la richiesta Inizio elenco da. Se si preme il tasto F16, l'operazione precedente di inizio elenco da verrà ripetuta.

Le autorizzazioni campo comprendono le seguenti opzioni:

- Il comando Stampa autorizzazioni private (PRTPVTAUT) dispone di un campo che indica quando un file dispone di autorizzazioni campo.
- Il comando Visualizzazione autorizzazione oggetto (DSPOBJAUT) dispone di un parametro Autorizzazione tipo per consentire la visualizzazione delle autorizzazioni oggetto, autorizzazioni campo o di tutte le autorizzazioni. Se il tipo di oggetto non è *FILE, è possibile visualizzare solo le autorizzazioni oggetto.
- Le informazioni fornite dalla API Elenco utenti autorizzati sull'oggetto (QSYLUSRA) indicano se un file dispone di autorizzazioni campo.

- Il comando Concessione autorizzazione utente (GRTUSRAUT) non concederà le autorizzazioni campo dell'utente.
- Quando si esegue una concessione con oggetto di riferimento utilizzando il comando GRTOBJAUT ed entrambi gli oggetti (quello a cui viene fatta la concessione e quello di riferimento) sono file di database, verranno concesse tutte le autorizzazioni campo dove si verifica una corrispondenza dei nomi campo.
- Se l'autorizzazione di un utente su un file di database viene rimossa, verranno rimosse anche tutte le autorizzazioni campo per l'utente.

Sicurezza e ambiente System/38

Questa sezione fornisce informazioni sulla sicurezza nell'ambiente System/38.

L'ambiente System/38 e i programmi CL di tipo CLP38 rappresentano un potenziale rischio per la sicurezza. Quando un comando qualificato non relativo alla libreria viene immesso dal pannello Immissione comando System/38 o richiamato da un qualsiasi programma CL CLP38, la libreria QUSER38 (qualora esista) è la prima libreria in cui si effettua la ricerca di quel comando. La libreria QSYS38 è la seconda libreria in cui si effettua la ricerca. Un programmatore o un qualsiasi utente esperto potrebbe collocare un altro comando CL nell'una o l'altra di queste librerie e fare in modo che il comando venga utilizzato al posto di un comando proveniente da una libreria presente nell'elenco di librerie.

La libreria QUSER38 non viene fornita con il sistema operativo. Tuttavia, può essere creata da chiunque possieda un'autorizzazione sufficiente per la creazione di una libreria.

Informazioni correlate


System/38 Environment Programming

Suggerimento per l'ambiente System/38

Questo argomento include un elenco di suggerimenti per l'ambiente System/38.

Utilizzare queste misure per proteggere il sistema per l'Ambiente System/38 e i programmi CL di tipo CLP38:

- Controllare l'autorizzazione pubblica della libreria QSYS38 e, se è *ALL o *CHANGE, modificarla in *USE.
- Controllare l'autorizzazione pubblica della libreria QUSER38 e, se è *ALL o *CHANGE, modificarla in *USE.
- Se le librerie QUSER38 e QSYS38 non esistono, crearle e impostarle sull'autorizzazione pubblica *USE. Ciò impedirà a chiunque altro di crearla in seguito e di fornire agli utente o al pubblico un'autorizzazione troppo estesa su tale libreria.

Sicurezza dell'indirizzario

È possibile utilizzare la sicurezza dell'indirizzario per proteggere le informazioni.

Quando si accede ad un oggetto in un indirizzario, è necessario disporre dell'autorizzazione su tutti gli indirizzari nel percorso contenente l'oggetto. È necessario inoltre disporre dell'autorizzazione necessaria sull'oggetto per eseguire l'operazione richiesta.

È possibile desiderare di utilizzare la sicurezza dell'indirizzario allo stesso modo in cui si utilizza la sicurezza della libreria. Limitare l'accesso agli indirizzari e utilizzare l'autorizzazione pubblica sugli oggetti contenuti all'interno dell'indirizzario. Limitando il numero delle autorizzazioni private definite per gli oggetti si migliorano le prestazioni del processo di controllo delle autorizzazioni.

Sicurezza elenco autorizzazioni

È possibile raggruppare gli oggetti con requisiti di sicurezza simili utilizzando un elenco di autorizzazioni.

Un elenco di autorizzazioni, concettualmente, contiene un elenco di utenti e le autorizzazione di cui dispongono gli utenti per gli oggetti protetti dall'elenco. Ogni utente può disporre di un'autorizzazione diversa sulla serie di oggetti protetta dall'elenco. Quando si fornisce un'autorizzazione utente all'elenco di autorizzazioni , il sistema operativo concede in realtà un'**autorizzazione privata per quell'utente** all'elenco di autorizzazioni.

È possibile inoltre utilizzare un elenco di autorizzazioni per definire l'autorizzazione pubblica per gli oggetti contenuti nell'elenco. Se l'autorizzazione pubblica per un oggetto è impostata su *AUTL, l'oggetto ottiene l'autorizzazione pubblica dal relativo elenco di autorizzazioni.

L'oggetto dell'elenco di autorizzazioni viene utilizzato come strumento di gestione dal sistema. In realtà contiene un elenco di tutti gli oggetti che vengono protetti dall'elenco di autorizzazioni. Queste informazioni vengono utilizzate per creare i pannelli che consentono di visualizzare o modificare gli oggetti dell'elenco di autorizzazioni.

Non è possibile utilizzare un elenco di autorizzazioni per proteggere un profilo utente o un altro elenco di autorizzazioni. Per un oggetto, è possibile specificare un solo elenco di autorizzazioni.

Solo il proprietario dell'oggetto, un utente con l'autorizzazione speciale su tutti gli oggetti (*ALLOBJ) o un utente con l'autorizzazione tutti (*ALL) sull'oggetto, può aggiungere o rimuovere l'elenco di autorizzazioni per un oggetto.

Gli oggetti contenuti nella libreria di sistema (QSYS) possono essere protetti con un elenco di autorizzazioni. Tuttavia, il nome di un elenco di autorizzazioni che protegge un oggetto viene memorizzato con l'oggetto stesso. In alcuni casi, quando si installa un nuovo release del sistema operativo, tutti gli oggetti contenuti nella libreria QSYS vengono sostituiti. L'associazione tra gli oggetti e l'elenco di autorizzazioni andrebbe persa.

Consultare l'argomento "Vantaggi dell'utilizzo dell'elenco di autorizzazioni" a pagina 178 per gli esempi su come utilizzare gli elenchi di autorizzazioni.

Gestione elenco autorizzazioni

È possibile concedere l'autorizzazione operativa speciale definita Gestione elenco di autorizzazioni (*AUTLMGT) per gli elenchi di autorizzazioni.

Gli utenti che dispongono dell'autorizzazione *AUTLMGT sono autorizzati ad aggiungere e rimuovere l'autorizzazione dell'utente dall'elenco di autorizzazioni e a modificare le autorizzazioni per tali utenti. L'autorizzazione *AUTLMGT, da sola, non fornisce l'autorizzazione alla protezione dei nuovi oggetti con l'elenco o alla rimozione degli oggetti dall'elenco.

Un utente con l'autorizzazione *AUTLMGT può fornire agli altri solo un'autorizzazione equivalente o inferiore. Ad esempio, si presupponga che USERA disponga dell'autorizzazione *CHANGE e *AUTLMGT sull'elenco di autorizzazioni CPLIST1. USERA può aggiungere USERB a CPLIST1 e fornire a USERB l'autorizzazione *CHANGE o una inferiore. USERA non può fornire a USERB l'autorizzazione *ALL per CPLIST1 poiché USERA non dispone dell'autorizzazione *ALL.

Un utente con l'autorizzazione *AUTLMGT può rimuovere l'autorizzazione per un utente se l'utente *AUTLMGT ha un'autorizzazione sull'elenco uguale o maggiore rispetto al nome del profilo utente rimosso. Se USERC ha l'autorizzazione *ALL per CPLIST1, allora USERA non può rimuovere USERC dall'elenco, poiché USERA dispone solo delle autorizzazioni *CHANGE e *AUTLMGT.

Utilizzo di elenchi di autorizzazioni per proteggere oggetti forniti da IBM

È possibile utilizzare elenchi di autorizzazioni per proteggere oggetti forniti da IBM. Ad esempio, è possibile limitare l'utilizzo di un gruppo di comandi a pochi utenti.

Gli oggetti contenuti nelle librerie fornite da IBM, diverse dalle librerie QUSRSYS e QGPL, vengono sostituiti ogni volta che si installa un nuovo release del sistema operativo. Tuttavia, il collegamento tra gli oggetti nelle librerie fornite da IBM e gli elenchi di autorizzazioni si perde. Inoltre, se un elenco di autorizzazioni protegge un oggetto in QSYS ed è richiesto un ripristino dell'intero sistema, il collegamento tra gli oggetti in QSYS e l'elenco di autorizzazioni si perde. Una volta installato un nuovo release o il ripristino del sistema, utilizzare il comando EDTOBJAUT o GRTOBJAUT per ristabilire il collegamento tra l'oggetto fornito da IBM e l'elenco di autorizzazioni.

Autorizzazione per i nuovi oggetti in una libreria

È possibile specificare l'autorizzazione per i nuovi oggetti in una libreria.

Ogni libreria dispone di un parametro definito CRTAUT (autorizzazione alla creazione). Questo parametro stabilisce l'autorizzazione pubblica predefinita per ogni nuovo oggetto creato in quella libreria. Quando si crea un oggetto, il parametro AUT sul comando di creazione stabilisce l'autorizzazione pubblica per l'oggetto. Se il valore AUT sul comando di creazione è *LIBCRTAUT, valore predefinito per la maggior parte dei comandi, l'autorizzazione pubblica per l'oggetto è impostata sul valore CRTAUT per la libreria.

Ad esempio, si presupponga che la libreria CUSTLIB disponga di un valore CRTAUT *USE. Entrambi i comandi di seguito riportati creano un'area dati definita DTA1 con l'autorizzazione pubblica *USE:

- Specificando il parametro AUT:

  ```
  CRTDTAARA DTAARA(CUSTLIB/DTA1) +
     TYPE(*CHAR) AUT(*LIBCRTAUT)
  ```

- Consentendo al parametro AUT di essere impostato sul valore predefinito. *LIBCRTAUT è il valore predefinito:

  ```
  CRTDTAARA DTAARA(CUSTLIB/DTA1) +
     TYPE(*CHAR)
  ```

Il valore CRTAUT predefinito per una libreria è *SYSVAL. Ogni nuovo oggetto creato nella libreria mediante AUT(*LIBCRTAUT) ha l'autorizzazione pubblica impostata sul valore del valore di sistema QCRTAUT. Il valore di sistema QCRTAUT viene fornito come *CHANGE. Ad esempio, si presupponga che la libreria ITEMLIB abbia un valore CRTAUT *SYSVAL. Questo comando crea l'area dati DTA2 con l'autorizzazione pubblica di modifica:

```
CRTDTAARA DTAARA(ITEMLIB/DTA2) +
   TYPE(*CHAR) AUT(*LIBCRTAUT)
```

"Assegnazione dell'autorizzazione e della proprietà ai nuovi oggetti" a pagina 156 mostra altri esempio di come il sistema assegna la proprietà e l'autorizzazione sui nuovi oggetti.

Il valore CRTAUT per una libreria può essere impostato anche sul nome dell'elenco di autorizzazioni. Ogni nuovo oggetto creato nella libreria con AUT(*LIBCRTAUT) viene protetto dall'elenco di autorizzazioni. L'autorizzazione pubblica per l'oggetto è impostata su *AUTL.

Il valore CRTAUT della libreria non viene utilizzato durante lo spostamento (MOVOBJ), la creazione di un duplicato (CRTDUPOBJ) o il ripristino di un oggetto all'interno della libreria. Viene utilizzata l'autorizzazione pubblica dell'oggetto esistente.

Se il parametro REPLACE (*YES) viene utilizzato sul comando di creazione, l'autorizzazione dell'oggetto esistente viene utilizzata al posto del valore CRTAUT della libreria.

Rischi di CRTAUT (Creazione autorizzazione)

È necessario considerare i rischi quando si modifica CRTAUT (Creazione autorizzazione) per una libreria delle applicazioni.

Se le applicazioni utilizzano l'autorizzazione predefinita per i nuovi oggetti creati durante l'elaborazione delle applicazioni, è necessario controllare chi possiede l'autorizzazione per modificare le descrizioni delle librerie. La modifica dell'autorizzazione CRTAUT per una libreria delle applicazioni potrebbe consentire l'accesso non autorizzato ai nuovi oggetti creati nella libreria.

Autorizzazione per i nuovi oggetti in un indirizzario

È possibile specificare l'autorizzazione per i nuovi oggetti in un indirizzario.

Quando si crea un nuovo indirizzario utilizzando i comandi CRTDIR (Creazione indirizzario), MD (Creazione indirizzario)o MKDIR (Creazione indirizzario), si specifica l'autorizzazione ai dati e agli oggetti che il pubblico riceve per il nuovo indirizzario. Se si utilizza l'opzione *INDIR predefinita, l'autorizzazione per l'indirizzario creato viene stabilita dal relativo indirizzario principale. In caso contrario, è possibile specificare l'autorizzazione specifica desiderata.

Quando si crea un nuovo indirizzario utilizzando l'API mkdir()--Creazione indirizzario, il proprietario, il gruppo principale e le autorizzazioni pubbliche all'oggetto per l'indirizzario creato vengono determinati dall'indirizzario in cui si effettua la creazione, mentre il proprietario, il gruppo principale e le autorizzazioni pubbliche ai dati vengono determinati dalla modalità specificata sulla chiamata API.

I due seguenti esempi mostrano risultati differenti quando si crea un nuovo indirizzario con differenti opzioni.

Il primo esempio crea un nuovo indirizzario nel file system ″root″(/) utilizzando il comando CRTDIR e specificando l'autorizzazione *PUBLIC.

Condizioni di partenza: autorizzazioni sull'indirizzario principale:

```
                                  Visualizzazione autorizzazione

Oggetto. . . . . . . . . . . . . :   /sanders/mytest
proprietario. . . . . . . . . . . :   SANDERS
Gruppo primario  . . . . . . . . . :   SANDERSGP3
Elenco autorizzazioni  . . . . . . :   *NONE

             Autorizz.     -----Autorizzazioni oggetto-----
Utente       dati     Esist.   Gest.   Alter.   Rif.
*PUBLIC      *RWX       X        X       X        X
SANDERS      *RW
SANDERSGP3   *RX
QPGMR        *RWX
QTCM         *RWX       X        X       X        X
```

L'utente SANDERS immette il seguente comando:
CRTDIR DIR('/sanders/mytest/deletemepub') DTAAUT(*R) OBJAUT(*NONE)

Risultati: autorizzazioni sull'indirizzario creato:

```
                                  Visualizzazione autorizzazione

Oggetto. . . . . . . . . . . . . :   /sanders/mytest/deletemepub
Proprietario. . . . . . . . . . . :   SANDERS
Gruppo primario  . . . . . . . . . :   SANDERSGP3
Elenco autorizzazioni  . . . . . . :   *NONE

             Autorizz.     -----Autorizzazioni oggetto-----
Utente       dati     Esist.   Gest.   Alter.   Rif.
*PUBLIC      *R
SANDERS      *RWX
SANDERSGP3   *RX
```

Note:

1. Le autorizzazioni sui dati e sull'oggetto *PUBLIC vengono impostate in base ai parametri DTAAUT e OBJAUT.
2. Le autorizzazioni ai dati del proprietario (SANDERS) vengono impostate su *RWX ma le autorizzazioni all'oggetto vengono ereditate dal proprietario dell'indirizzario principale. Ciò significa che il proprietario di tale indirizzario non ha alcuna autorizzazione all'oggetto nel nuovo indirizzario, poiché il proprietario dell'indirizzario principale non ha alcuna autorizzazione all'oggetto dell'indirizzario principale.
3. Il nuovo indirizzario dispone di un profilo del gruppo principale SANDERSGP3 poiché l'indirizzario principale presenta SANDERSGP3 come profilo di gruppo principale.

Il secondo esempio mostra il modo in cui tutte le autorizzazioni vengono ereditate dall'indirizzario principale quando si crea un nuovo indirizzario utilizzando il comando CRTDIR nel file system ″root″(/).

Condizioni di partenza: autorizzazioni sull'indirizzario principale:

```
                                  Visualizzazione autorizzazione

Oggetto. . . . . . . . . . . . . :   /sanders/mytest
Proprietario. . . . . . . . . . . :   SANDERS
Gruppo primario  . . . . . . . . . :   SANDERSGP3
Elenco autorizzazioni  . . . . . . :   *NONE

             Autorizz.     -----Autorizzazioni oggetto-----
Utente       dati     Esist.   Gest.   Alter.   Rif.
*PUBLIC      *RWX       X        X       X        X
SANDERS      *RW
SANDERSGP3   *RX
QPGMR        *RWX
QTCM         *RWX       X        X       X        X
```

L'utente SANDERSUSR immette il seguente comando:
CRTDIR DIR('/sanders/mytest/deletemepub')

Risultati: autorizzazioni sull'indirizzario creato:

```
                                  Visualizzazione autorizzazione

Oggetto. . . . . . . . . . . . . :   /sanders/mytest/deletemepub
Proprietario. . . . . . . . . . . :   SANDERSUSR
Gruppo primario  . . . . . . . . . :   SANDERSGP3
Elenco autorizzazioni  . . . . . . :   *NONE

             Autorizz.     -----Autorizzazioni oggetto-----
Utente       dati     Esist.   Gest.   Alter.   Rif.
*PUBLIC      *RWX       X        X       X        X
SANDERSUSR   *RWX
SANDERSGP3   *RX
QPGMR        *RWX
QTCM         *RWX       X        X       X        X
SANDERS      *RW
```

Note:

1. Le autorizzazioni all'oggetto e ai dati *PUBLIC vengono ereditate dall'indirizzario principale; quindi, l'autorizzazione ai dati è impostata su *RWX con tutte le autorizzazioni all'oggetto.
2. Le autorizzazioni ai dati del proprietario (SANDERSUSR) vengono impostate su *RWX ma le autorizzazioni all'oggetto vengono ereditate dal proprietario dell'indirizzario principale. Ciò significa che il proprietario di tale indirizzario non ha alcuna autorizzazione all'oggetto nel nuovo indirizzario, poiché il proprietario dell'indirizzario principale non ha alcuna autorizzazione all'oggetto dell'indirizzario principale.
3. Il nuovo indirizzario dispone di un profilo del gruppo principale SANDERSGP3 poiché l'indirizzario principale presenta SANDERSGP3 come profilo di gruppo principale.
4. Tutti gli utenti autorizzati privatamente all'indirizzario principale (QPGMR, QTCM) e al proprietario dell'indirizzario principale (SANDERS) viene concessa la stessa autorizzazione privata al nuovo indirizzario.

Proprietà oggetto

Questo argomento descrive la proprietà oggetto e le relative funzioni nel sistema.

Ogni oggetto viene assegnato ad un proprietario al momento della sua creazione. Il proprietario è l'utente che crea l'oggetto oppure il profilo gruppo se il profilo utente del membro ha specificato che il profilo gruppo deve essere il proprietario dell'oggetto. Quando si crea un oggetto, al proprietario vengono concesse tutte le autorizzazioni dati e oggetto sull'oggetto. "Assegnazione dell'autorizzazione e della proprietà ai nuovi oggetti" a pagina 156 mostra gli esempi su come il sistema assegna la proprietà ai nuovi oggetti.

Il proprietario di un oggetto dispone sempre di tutte le autorizzazioni sull'oggetto a meno che alcune o tutte le autorizzazioni non vengano rimosse specificatamente. Come proprietario di un oggetto, è possibile scegliere di rimuovere alcune autorizzazioni specifiche come misura precauzionale, a condizione che non si disponga dell'autorizzazione speciale *ALLOBJ. Ad esempio, se esiste un file contenente informazioni importanti, è possibile rimuovere l'autorizzazione all'esistenza dell'oggetto per impedire all'utente stesso di cancellare accidentalmente il file. Tuttavia, come proprietario dell'oggetto, è possibile concedere l'autorizzazione oggetto a se stessi in qualsiasi momento. Il proprietario di un oggetto dell'IFS appena creato dispone delle stesse autorizzazioni all'oggetto per l'oggetto IFS del proprietario dell'indirizzario principale. Controllare l'argomento Pianificazione e impostazione sicurezza del sistema per verificare se le regole per le autorizzazioni all'oggetto si applicano a tutti i file system o solo ad alcuni.

La proprietà di un oggetto può essere trasferita da un utente ad un altro. La proprietà può essere trasferita ad un singolo profilo utente o a un profilo di gruppo. Un profilo di gruppo può possedere oggetti, se il gruppo contiene dei membri.

I seguenti paragrafi si applicano agli oggetti basati sia sull'indirizzario che sulla libreria.

Quando si modifica il proprietario di un oggetto, è possibile conservare o revocare l'autorizzazione dell'ex proprietario.

Non è possibile cancellare un profilo che possiede gli oggetti. La proprietà degli oggetti deve essere trasferita ad un nuovo proprietario oppure gli oggetti devono essere cancellati prima di poter cancellare il profilo. Il comando Cancellazione profilo utente (DLTUSRPRF) consente di gestire gli oggetti di proprietà quando si cancella il profilo.

La proprietà dell'oggetto viene utilizzata dal sistema come strumento di gestione. Il profilo del proprietario per un oggetto contiene un elenco di tutti gli utenti che dispongono dell'autorizzazione privata sull'oggetto. Queste informazioni vengono utilizzate per creare i pannelli per la modifica o la visualizzazione dell'autorizzazione sull'oggetto.

I profili che possiedono molti oggetti con molte autorizzazioni private possono assumere dimensioni molto ampie. La dimensione di un profilo che possiede molti oggetti coinvolge le prestazioni durante la visualizzazione e la gestione dell'autorizzazione sugli oggetti posseduti e durante il salvataggio o il ripristino dei profili. È possibile inoltre che vengano influenzate anche le operazioni del sistema. Per impedire gli impatti sulle prestazioni o sulle operazioni del sistema, non assegnare gli oggetti ad un solo profilo proprietario per l'intero ambiente System i5. Ogni applicazione e gli oggetti dell'applicazione devono essere di proprietà di un profilo separato. Inoltre, i profili utente forniti da IBM non dovrebbero possedere i dati utente o gli oggetti.

Il proprietario di un oggetto necessita inoltre di memoria sufficiente per l'oggetto. Consultare "Memoria massima" a pagina 101 per ulteriori informazioni.

Proprietà gruppo degli oggetti

Questo argomento fornisce informazioni dettagliate sulla proprietà gruppo degli oggetti.

Una volta creato un oggetto, il sistema controlla il profilo dell'utente che ha creato l'oggetto per stabilire la proprietà dell'oggetto. Se l'utente è un membro di un profilo gruppo, il campo OWNER nel profilo utente specifica se l'utente o il gruppo deve possedere il nuovo oggetto.

Se il gruppo possiede l'oggetto (OWNER è *GRPPRF), all'utente che crea l'oggetto non viene concessa automaticamente alcuna autorizzazione specifica sull'oggetto. L'utente ottiene l'autorizzazione sull'oggetto mediante il gruppo. Se l'utente possiede l'oggetto (OWNER è *USRPRF), l'autorizzazione gruppo sull'oggetto viene stabilita dal campo GRPAUT nel profilo utente. Gli oggetti creati negli indirizzari non utilizzano i valori OWNER e GRPAUT per determinare l'autorizzazione proprietà o gruppo. L'oggetto sarà sempre di proprietà del creatore.

Il campo *tipo di autorizzazione gruppo* (GRPAUTTYP) nel profilo utente determina se il gruppo 1) diventa il gruppo principale per l'oggetto oppure se 2) viene fornita l'autorizzazione privata all'oggetto. "Assegnazione dell'autorizzazione e della proprietà ai nuovi oggetti" a pagina 156 mostra diversi esempi.

Se l'utente che possiede l'oggetto passa ad un gruppo utenti diverso, il profilo gruppo originale conserva ancora l'autorizzazione su qualsiasi oggetto creato.

Anche se il campo *Proprietario* in un profilo utente è *GRPPRF, l'utente deve disporre ancora di memoria sufficiente per poter conservare un nuovo oggetto durante la sua creazione. Una volta creato, la proprietà viene trasferita al profilo gruppo. Il parametro MAXSTG nel profilo utente determina quanta memoria ausiliaria viene concessa ad un utente.

Valutare gli oggetti che un utente può creare, come ad esempio i programmi query, quando si effettua una scelta tra la proprietà gruppo e utente individuale:

- Se l'utente passa ad un dipartimento differente e ad un gruppo utenti diverso, l'utente è ancora proprietario degli oggetti?
- È importante sapere chi crea gli oggetti? I pannelli dell'autorizzazione oggetto mostra il proprietario dell'oggetto, non l'utente che ha creato l'oggetto.

  Nota: il pannello Visualizzazione descrizione oggetto mostra il creatore dell'oggetto.

  Se la funzione di controllo del giornale è attiva, una voce Creazione oggetto (CO) viene scritta sul giornale di controllo QAUDJRN nel momento in cui l'oggetto viene creato. Questa voce identifica la creazione del profilo utente. La voce viene scritta solo se il valore di sistema QAUDLVL include *CREATE e il valore di sistema QAUDCTL comprende *AUDLVL.

  Concetti correlati

  "Profili di gruppo" a pagina 5
  Un *profilo di gruppo* è un tipo speciale di profilo utente. Piuttosto che fornire l'autorizzazione a ciascun utente singolarmente, è possibile utilizzare un profilo di gruppo per definire l'autorizzazione per un gruppo di utenti.

Gruppo principale per un oggetto

È possibile specificare un gruppo principale per un oggetto.

Il nome del profilo gruppo principale e l'autorizzazione del gruppo principale sull'oggetto vengono memorizzati con l'oggetto. Utilizzando l'autorizzazione del gruppo principale si le prestazioni migliorano rispetto all'autorizzazione gruppo privato durante il controllo dell'autorizzazione su un oggetto.

Un profilo deve essere un profilo gruppo (deve avere un gid) da assegnare come gruppo principale per un oggetto. Lo stesso profilo non può essere il proprietario dell'oggetto e il relativo gruppo principale.

Quando un utente crea un nuovo oggetto, i parametri nel profilo utente controllano se il gruppo dell'utente possiede l'autorizzazione sull'oggetto e il tipo. Il parametro *Tipo di autorizzazione di gruppo* (GRPAUTTYP) in un profilo utente può essere utilizzato per rendere il gruppo utente il gruppo principale

per l'oggetto. "Assegnazione dell'autorizzazione e della proprietà ai nuovi oggetti" mostra esempi di come viene assegnata l'autorizzazione quando vengono creati i nuovi oggetti. Per un oggetto basato sull'indirizzario in alcuni file system, l'oggetto eredita il gruppo principale del relativo indirizzario principale. Ad esempio, se l'indirizzario principale presenta il gruppo principale FRED, FRED avrà problemi nel tentativo di creare gli elementi in tale indirizzario principale. Ciò significa che lo stesso profilo utente non può essere sia il proprietario che il profilo di gruppo principale per lo stesso oggetto.

È possibile modificare il gruppo principale per un oggetto basato sulla libreria o sull'indirizzario utilizzando uno dei seguenti comandi:

- Comando CHGOBJPGP (Modifica gruppo principale oggetto)
- Comando CHGPGP (Modifica gruppo principale)
- Opzione 9 sul comando WRKOBJPGP (Gestione oggetti per gruppo principale)

È possibile modificare l'autorizzazione del gruppo principale utilizzando il comando EDTOBJAUT (Editazione autorizzazione oggetto) o i comandi per la concessione e la revoca dell'autorizzazione. È possibile modificare l'autorizzazione del gruppo principale per un oggetto basato su un indirizzario o su una libreria utilizzando il comando CHGAUT (Modifica autorizzazione) o il comando WRKAUT (Gestione autorizzazione).

Concetti correlati

"Profili di gruppo" a pagina 5
Un *profilo di gruppo* è un tipo speciale di profilo utente. Piuttosto che fornire l'autorizzazione a ciascun utente singolarmente, è possibile utilizzare un profilo di gruppo per definire l'autorizzazione per un gruppo di utenti.

Il profilo utente Proprietario predefinito (QDFTOWN)

Il profilo utente Proprietario predefinito (QDFTOWN) è un profilo utente fornito da IBM che viene utilizzato quando un oggetto non possiede proprietario o quando la proprietà dell'oggetto potrebbe condurre a rischi per la sicurezza.

Di seguito vengono riportate delle situazioni che potrebbero fare in modo che la proprietà di un oggetto venga assegnata al profilo QDFTOWN:

- Se un profilo proprietario viene danneggiato e cancellato, gli oggetti relativi non dispongono più di un utente. Il comando Riacquisizione memoria (RCLSTG) assegna la proprietà di questi oggetti al profilo utente del proprietario predefinito (QDFTOWN).
- Se un oggetto viene ripristinato e il profilo del proprietario non esiste.
- Se un programma che deve essere ricreato viene ripristinato, ma la creazione del programma non riesce. Consultare l'argomento "Convalida dei programmi in fase di ripristino" a pagina 18 per ulteriori informazioni su quali condizioni fanno in modo che la proprietà venga assegnata a QDFTOWN.
- Se si supera il limite massimo di memorizzazione per il profilo utente che possiede un titolare autorizzazione con lo stesso nome del file spostato, ridenominato o la cui libreria è stata ridenominato.

Il sistema fornisce il profilo utente QDFTOWN poiché tutti gli oggetti devono avere un proprietario. Quando il sistema viene consegnato, solo un utente con l'autorizzazione speciale *ALLOBJ può visualizzare e accedere a questo profilo utente e trasferire la proprietà degli oggetti associati al profilo utente QDFTOWN. È possibile concedere ad altri utente l'autorizzazione al profilo QDFTOWN. Il profilo utente QDFTOWN è stato concepito per il solo utilizzo da parte del sistema. L'utente non deve creare la sicurezza, in tal modo QDFTOWN possiede normalmente gli oggetti.

Assegnazione dell'autorizzazione e della proprietà ai nuovi oggetti

È possibile assegnare l'autorizzazione e la proprietà ai nuovi oggetti sul sistema.

Il sistema utilizza diversi valori per assegnare l'autorizzazione e la proprietà quando si crea un nuovo oggetto sul sistema:

- Parametri sul comando CRTxxx
- Il valore di sistema QCRTAUT
- Il valore CRTAUT della libreria
- I valori nel profilo utente del creatore

Dalla Figura 6 alla Figura 9 a pagina 160 vengono visualizzati diversi esempi su come vengono visualizzati questi valori:

Valore di sistema QCRTAUT:
*CHANGE

Parametro libreria CRTAUT:
*USE

Valori nel profilo USERA (Creatore):

GRPPRF:
DPT806

OWNER:
*USRPRF

GRPAUT:
*CHANGE

GRPAUTTYP:
*PRIVATE

Comando utilizzato per creare l'oggetto:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
        TYPE(*CHAR) AUT(*LIBCRTAUT)
```

o

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
        TYPE(*CHAR)
```

Valori per il nuovo oggetto:

Autorizzazione pubblica:
*USE

Autorizzazione proprietario:
USERA *ALL

Autorizzazione gruppo principale:
Nessuna

Autorizzazione privata:
DPT806 *CHANGE

Nota:

*LIBCRTAUT è il valore predefinito per il parametro AUT sulla maggior parte dei comandi CRTxxx.

Figura 6. Esempio nuovo oggetto: Autorizzazione pubblica dalla libreria, Gruppo a cui è stata fornita l'autorizzazione privata.

Valore di sistema QCRTAUT:
*CHANGE

Parametro libreria CRTAUT:
*SYSVAL

Valori nel profilo USERA (Creatore):

GRPPRF:
DPT806

OWNER:
*USRPRF

GRPAUT:
*CHANGE

GRPAUTTYP:
*PRIVATE

Comando utilizzato per creare l'oggetto:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
        TYPE(*CHAR) AUT(*LIBCRTAUT)
```

Valori per il nuovo oggetto:

Autorizzazione pubblica:
*CHANGE

Autorizzazione proprietario:
USERA *ALL

Autorizzazione gruppo principale:
Nessuna

Autorizzazione privata:
DPT806 *CHANGE

Figura 7. Esempio nuovo oggetto: Autorizzazione pubblica dal valore di sistema, Gruppo a cui è stata fornita l'autorizzazione privata

Valore di sistema QCRTAUT:
*CHANGE

Parametro libreria CRTAUT:
*USE

Valori nel profilo USERA (Creatore):

GRPPRF:
DPT806

OWNER:
*USRPRF

GRPAUT:
*CHANGE

GRPAUTTYP:
*PGP

Comando utilizzato per creare l'oggetto:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
        TYPE(*CHAR) AUT(*LIBCRTAUT)
```

Valori per il nuovo oggetto:

Autorizzazione pubblica:
*USE

Autorizzazione proprietario:
USERA *ALL

Autorizzazione gruppo principale:
DPT806 *CHANGE

Autorizzazione privata:
Nessuna

Figura 8. Esempio nuovo oggetto: Autorizzazione pubblica dalla libreria, Gruppo a cui è stata fornita l'autorizzazione gruppo principale.

Valore di sistema QCRTAUT:
*CHANGE

Parametro libreria CRTAUT:
*USE

Valori nel profilo USERA (Creatore):

GRPPRF:
DPT806

OWNER:
*GRPPRF

GRPAUT:

GRPAUTTYP:

Comando utilizzato per creare l'oggetto:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
        TYPE(*CHAR) AUT(*CHANGE)
```

Valori per il nuovo oggetto:

Autorizzazione pubblica:
*CHANGE

Autorizzazione proprietario:
DPT806 *ALL

Autorizzazione gruppo principale:
Nessuna

Autorizzazione privata:
Nessuna

Figura 9. Esempio nuovo oggetto: Autorizzazione pubblica specificata, Gruppo che possiede l'oggetto

Oggetti che adottano l'autorizzazione del proprietario

È possibile assegnare l'autorizzazione adottata a un programma utente per consentire all'utente di modificare un file cliente.

Alcune volte un utente necessita di diverse autorizzazioni su un oggetto o un'applicazione, a seconda della situazione. Ad esempio, un utente potrebbe essere autorizzato a modificare le informazioni in un file cliente quando utilizza i programmi delle applicazioni che forniscono tale funzione. Tuttavia, lo stesso utente potrebbe essere autorizzato a visualizzare, ma non a modificare, le informazioni cliente quando utilizza uno strumento di supporto decisionale, come ad esempio SQL.

Una soluzione a questa situazione è 1) fornire all'utente l'autorizzazione *USE alle informazioni cliente per consentire la query dei file e 2) utilizzare l'autorizzazione adottata nei programmi di gestione della clientela per consentire all'utente di modificare i file.

Quando un oggetto utilizza l'autorizzazione del proprietario, questa viene definita *autorizzazione adottata*. Gli oggetti di tipo *PGM, *SRVPGM, *SQLPKG e i programmi Java possono adottare l'autorizzazione.

Quando si crea un programma, l'utente specifica un parametro del profilo utente (USRPRF) sul comando CRTxxxPGM. Questo parametro stabilisce se il programma utilizza o meno l'autorizzazione del proprietario del programma, oltre all'autorizzazione dell'utente che esegue il programma.

Consultare l'argomento Limit the use of adopted authority riguardante considerazioni sulla sicurezza e l'autorizzazione adottata quando si utilizzano i pacchetti SQL.

La seguente descrizione si applica all'autorizzazione adottata:

- L'autorizzazione adottata viene aggiunta a qualsiasi altra autorizzazione rilevata per l'utente.
- L'autorizzazione adottata viene controllata solo se l'autorizzazione che l'utente, il gruppo dell'utente o il pubblico possiede su un oggetto non è adeguata per l'operazione richiesta.
- Vengono utilizzate le autorizzazioni speciali (quali ad esempio *ALLOBJ) presenti nel profilo dell'utente.
- Se il profilo del proprietario è un membro di un profilo gruppo, l'autorizzazione del gruppo *non* viene utilizzata per l'autorizzazione adottata.
- L'autorizzazione pubblica *non* viene utilizzata per l'autorizzazione adottata. Ad esempio, USER1 esegue il programma LSTCUST, che richiede l'autorizzazione *USE sul file CUSTMST:
  - L'autorizzazione pubblica sul file CUSTMST è *USE.
  - L'autorizzazione di USER1 è *EXCLUDE.
  - USER2 possiede il programma LSTCUST, che adotta l'autorizzazione del proprietario.
  - USER2 non possiede il file CUSTMST e non dispone alcune autorizzazione su di esso.
  - Sebbene l'autorizzazione pubblica sia sufficiente per fornire a USER2 l'accesso al file CUSTMST, USER1 non ottiene l'accesso. L'autorizzazione del proprietario, l'autorizzazione del gruppo principale e l'autorizzazione privata vengono utilizzate per l'autorizzazione adottata.
  - Solo l'autorizzazione viene adottata. Non vengono adottati altri attributi del profilo utente. Ad esempio, gli attributi delle possibilità limitate non vengono adottati.
- L'autorizzazione adottata è attiva fino a quando il programma che utilizza l'autorizzazione adottata rimane nello stack di chiamata. Ad esempio, si supponga che PGMA utilizzi l'autorizzazione adottata:
  - Se PGMA avvia PGMB utilizzando il comando CALL, questi sono degli stack di chiamata prima e dopo il comando CALL:

Tabella 119. Autorizzazione adottata e comando CALL

Stack di chiamata prima del comando CALL:	**Stack di chiamata dopo il comando CALL:**
QCMD • • • PGMA	QCMD • • • PGMA PGMB

    Poiché PGMA rimane nello stack di chiamata dopo che PGMB è stato richiamato, PGMB utilizza l'autorizzazione adottata di PGMA. (L'utilizzo del parametro dell'autorizzazione adottata (USEADPAUT) può sovrascrivere tale operazione. Consultare "Programmi che ignorano l'autorizzazione adottata" a pagina 164 per ulteriori informazioni sul parametro USEADPAUT.)
  - Se PGMA avvia PGMB utilizzando il comando TFRCTL (Trasferimento controllo), gli stack di chiamata appariranno nel seguente modo:

Tabella 120. Autorizzazione adottata e comando TFRCTL

Stack di chiamata prima del comando TFRCTL:	Stack di chiamata dopo il comando TFRCTL:
QCMD • • • PGMA	QCMD • • • PGMB

PGMB non utilizza l'autorizzazione adottata di PGMA, poiché PGMA non è più presente nello stack di chiamata.

- Se il programma in esecuzione sotto l'autorizzazione adottata viene interrotto, l'utilizzo dell'autorizzazione adottata viene sospeso. Le seguenti funzioni non utilizzano l'autorizzazione adottata:
  - Richiesta di sistema
  - Tasto di Attenzione (Se il comando Trasferimento a lavoro di gruppo (TFRGRPJOB) è in esecuzione, l'autorizzazione adottata non viene inoltrata al lavoro di gruppo.)
  - Programma di gestione messaggi con interruzione
  - Funzioni di debug

  Nota: l'autorizzazione adottata viene interrotta immediatamente dal tasto di attenzione o da una richiesta di lavoro di gruppo. L'utente deve disporre dell'autorizzazione ad eseguire il programma di gestione del tasto di attenzione o al programma iniziale del lavoro di gruppo oppure il tentativo non riesce.

  Ad esempio, USERA esegue il programma PGM1, che adotta l'autorizzazione di USERB. PGM1 utilizza il comando SETATNPGM e specifica PGM2. USERB dispone dell'autorizzazione *USE su PGM2. USERA dispone dell'autorizzazione *EXCLUDE su PGM2. La funzione SETATNPGM viene eseguita con esito positivo perché viene eseguita utilizzando l'autorizzazione adottata. USERA riceve un errore di autorizzazione quando si tenta di utilizzare il tasto di attenzione poiché l'autorizzazione USERB non è più attiva.
- Se un programma che utilizza l'autorizzazione adottata inoltra un lavoro, quel lavoro inoltrato non dispone dell'autorizzazione adottata del programma che ha inoltrato il lavoro.
- Quando un programma trigger o un programma del punto di uscita viene richiamato, l'autorizzazione adottata dai programmi precedenti nello stack di chiamata non verrà utilizzata come origine dell'autorizzazione per il programma trigger o il programma del punto di uscita.
- L'autorizzazione adottata non viene utilizzata dagli IFS, inclusi i file system "root" (/), QOpenSys, QDLS e gli UDFS (user-defined file system).
- La funzione di adozione del programma non viene utilizzata quando si utilizza il comando Modifica lavoro (CHGJOB) per modificare la coda di emissione per un lavoro. Il profilo utente che apporta la modifica deve disporre dell'autorizzazione sulla nuova coda di emissione.
- Gli oggetti creati, compresi i file di spool che possono contenere dati confidenziali, sono di proprietà dell'utente del programma o del profilo gruppo dell'utente, non del proprietario del programma.
- L'autorizzazione adottata può essere specificata sul comando che crea il programma (CRTxxxPGM) o sul comando Modifica programma (CHGPGM) o sul comando Modifica programma di servizio (CHGSRVPGM) .
- Se si crea un programma utilizzando REPLACE(*YES) sul comando CRTxxxPGM, la nuova copia del programma ha gli stessi valori USRPRF, USEADPAUT e AUT del programma sostituito. I parametri USRPRF e AUT specificati sul parametro CRTxxxPGM vengono ignorati.
- Solo il proprietario del programma può specificare REPLACE(*YES) sul comando CRTxxxPGM quando si specifica USRPRF(*OWNER) sul programma originale.
- Solo un utente che possiede il programma o che dispone delle autorizzazioni speciali *ALLOBJ e *SECADM può modificare il valore del parametro USRPRF.

- È necessario essere collegati come utente che possiede le autorizzazioni speciali *ALLOBJ e *SECADM per trasferire la proprietà di un oggetto che adotta l'autorizzazione.
- Se un altro utente che non è il proprietario del programma o un utente che dispone delle autorizzazioni speciali *ALLOBJ e *SECADM ripristina un programma che adotta l'autorizzazione, tutte le autorizzazioni private e pubbliche al programma vengono revocata per impedire i possibili rischi della sicurezza.

I comandi DSPPGM (Visualizzazione programma) e DSPSRVPGM (Visualizzazione programma di servizio)mostrano se un programma adotta o meno l'autorizzazione (richiesta *Profilo utente*) e se utilizza l'autorizzazione adottata proveniente dai programmi precedenti contenuti nello stack di chiamata (richiesta *Utilizzo autorizzazione adottata*). Il comando Visualizzazione adozione programma (DSPPGMADP) mostra tutti gli oggetti che adottano l'autorizzazione di un profilo utente specifico. Il comando Stampa oggetti di adozione (PRTADPOBJ) fornisce un prospetto con maggiori informazioni sugli oggetti che adottano l'autorizzazione. Questo comando fornisce inoltre un'opzione per stampare un prospetto per gli oggetti modificati dall'ultima volta in cui è stato eseguito il comando.

"Diagramma di flusso 8: come controllare l'autorizzazione adottata" a pagina 195 fornisce maggiori informazioni sull'autorizzazione adottata. L'argomento "Utilizzo dell'autorizzazione adottata nella struttura del menu" a pagina 246 mostra un esempio su come utilizzare l'autorizzazione adottata in un'applicazione.

Autorizzazione adottata e programmi collegati:

Un programma ILE* (*PGM) è un oggetto contenente uno o più moduli. Viene creato da un programma di compilazione ILE*. Un programma ILE può essere collegato ad uno o più programmi di servizio (*SRVPGM).

Per attivare un programma ILE con esito positivo, l'utente deve disporre dell'autorizzazione *EXECUTE al programma ILE e a tutti i programmi di servizio a cui è collegato. Se un programma ILE utilizza l'autorizzazione adottata proveniente da un programma superiore nello stack di chiamata del programma, questa autorizzazione adottata viene utilizzata per controllare l'autorizzazione a tutti i programmi di servizio a cui il programma ILE è collegato. Se il programma ILE adotta l'autorizzazione, l'autorizzazione adottata non verrà controllata quando il sistema controlla l'autorizzazione utente sui programmi di servizio nel momento in cui si attiva il programma.

Suggerimenti e rischi dell'autorizzazione adottata

L'utente deve utilizzare le autorizzazioni adottate con cura per evitare di mettere a rischio la sicurezza.

Consentire l'esecuzione di un programma mediante l'utilizzo dell'autorizzazione adottata rappresenta un rilascio del controllo intenzionale. Si permette all'utente di disporre dell'autorizzazione sugli oggetti, e possibilmente dell'autorizzazione speciale, di cui l'utente solitamente non disporrebbe. L'autorizzazione adottata fornisce un strumento importante che consente di soddisfare requisiti di autorizzazione diversi, ma dovrebbe essere utilizzata con attenzione:

- Adottare l'autorizzazione minima richiesta per soddisfare i requisiti dell'applicazione. Adottare l'autorizzazione di un proprietario dell'applicazione è preferibile rispetto ad adottare l'autorizzazione di QSECOFR o di un utente che dispone dell'autorizzazione speciale *ALLOBJ.
- Controllare attentamente la funzione fornita dai programma che adottano l'autorizzazione. Accertarsi che questi programmi non diano la possibilità all'utente di accedere agli oggetti al di fuori del controllo del programma, fornendo ad esempio la possibilità di immissione di un comando.
- Accertarsi che i programmi che adottano l'autorizzazione e che richiamano altri programmi eseguano chiamate qualificate della libreria. Non utilizzare l'elenco di librerie (*LIBL) sulla chiamata.
- Controllare gli utenti che sono autorizzati al richiamo dei programmi che adottano l'autorizzazione. Utilizzare le interfacce dei menu e la sicurezza della libreria per impedire che questi programmi vengano richiamati senza controllo sufficiente.

Programmi che ignorano l'autorizzazione adottata

È possibile specificare il parametro dell'autorizzazione adottata (USEADPAUT) per controllare se un programma utilizza l'autorizzazione adottata.

È possibile non desiderare che alcuni programmi utilizzino l'autorizzazione adottata dei programmi precedenti nello stack di chiamata. Ad esempio, se si utilizza un programma di menu iniziale che adotta l'autorizzazione del proprietario, è possibile desiderare che alcuni dei programmi richiamati dal programma del menu non utilizzino tale autorizzazione.

Il parametro per l'utilizzo dell'autorizzazione adottata (USEADPAUT) di un programma stabilisce se il sistema utilizza o meno l'autorizzazione adottata dei programmi precedenti nello stack durante il controllo dell'autorizzazione per gli oggetti.

Quando si crea un programma, l'impostazione predefinita prevede l'utilizzo dell'autorizzazione adottata proveniente dai programmi precedenti nello stack. Se non si vuole che il programma utilizzi l'autorizzazione adottata, è possibile modificare il programma con il comando Modifica programma (CHGPGM) o il comando Modifica programma di servizio (CHGSRVPGM) per impostare il parametro USEADPAUT su *NO. Se si crea un programma utilizzando REPLACE(*YES) sul comando CRTxxxPGM, la nuova copia del programma dispone degli stessi valori USRPRF, USEADPAUT e AUT del programma sostituito.

L'argomento "Come ignorare l'autorizzazione adottata" a pagina 249 mostra un esempio di come utilizzare questo parametro nella struttura del menu. Consultare "Utilizzo autorizzazione adottata (QUSEADPAUT)" a pagina 38 per informazioni sul valore di sistema QUSEADPAUT.

Attenzione: in alcune situazioni, è possibile utilizzare l'istruzione MODINVAU MI per impedire l'inoltro dell'autorizzazione adottata alle funzioni richiamate. L'istruzione MODINVAU può essere utilizzata per impedire l'inoltro di una qualsiasi autorizzazione adottata dai programmi C e C++ alle funzioni richiamate in un altro programma o programma di servizio. Ciò può rivelarsi estremamente utile quando non si conosce l'impostazione USEADPAUT della funzione richiamata.

Concetti correlati

"Come ignorare l'autorizzazione adottata" a pagina 249
La tecnica di utilizzare l'autorizzazione adottata nella struttura del menu richiede che l'utente ritorni al menu iniziale prima di eseguire delle query. Se si desidera sfruttare l'opportunità di avviare una query dai menu dell'applicazione e da un menu iniziale, è possibile impostare il programma QRYSTART per ignorare l'autorizzazione adottata.

Archivi autorizzazioni

L'archivio autorizzazioni è uno strumento che consente di conservare le autorizzazioni per un file di database descritto dal programma che non esiste attualmente sul sistema.

L'utilizzo principale di un archivio autorizzazioni è nelle applicazioni dell'ambiente System/36, che spesso cancellano i file descritti dal programma per poi crearli nuovamente.

È possibile creare un archivio autorizzazioni per un file già esistente o per un file che non esiste, utilizzando il comando CRTAUTHLR (Creazione archivio autorizzazioni). Le seguenti descrizioni si applicano agli archivi autorizzazioni:

- Gli archivi autorizzazioni possono soltanto proteggere i file nell'ASP (Auxiliary storage pool) di sistema o utente di base. Non possono proteggere i file in un ASP indipendente.
- L'archivio autorizzazioni viene associato ad un file o ad una libreria specifica. Possiede lo stesso nome del file.
- Gli archivi autorizzazioni possono essere utilizzati solo per i file di database e i file logici descritti dal programma.

- Una volta creato l'archivio autorizzazioni, vengono aggiunte le relative autorizzazioni private come se fosse un file. Utilizzare i comandi per concedere, revocare e visualizzare le autorizzazioni degli oggetti e per specificare il tipo di oggetto *FILE. Sui pannelli per l'autorizzazione degli oggetti, l'archivio autorizzazioni non può essere distinto dal file stesso. I pannelli non indicano se il file esiste o meno e nemmeno se il file dispone di un archivio autorizzazioni.
- Se un file viene associato ad un archivio autorizzazioni, le autorizzazioni definite per l'archivio autorizzazioni vengono utilizzate durante il controllo dell'autorizzazione. Ogni autorizzazione privata definita per il file viene ignorata.
- Utilizzare il comando DSPAUTHLR (Visualizzazione archivio autorizzazioni) per visualizzare o stampare tutti gli archivi autorizzazioni presenti sul sistema. Inoltre, l'utente può utilizzare tale comando per creare un file di emissione (OUTFILE) per l'elaborazione.
- Se si crea un archivio autorizzazioni per un file esistente:
  - L'utente che ha creato un archivio autorizzazioni deve disporre dell'autorizzazione *ALL sul file.
  - Il proprietario del file diventa il proprietario dell'archivio autorizzazioni senza tener conto dell'utente che ha creato l'archivio autorizzazioni.
  - L'autorizzazione pubblica per l'archivio autorizzazioni deriva dal file. Il parametro dell'autorizzazione pubblica (AUT) sul comando CRTAUTHLR viene ignorato.
  - L'autorizzazione del file esistente viene copiata sull'archivio autorizzazioni.
- Se si crea un file e un archivio autorizzazioni per il file che già esiste:
  - L'utente che ha creato il file deve disporre dell'autorizzazione *ALL sull'archivio autorizzazioni.
  - Il proprietario dell'archivio autorizzazioni diventa il proprietario del file senza tener conto dell'utente che ha creato il file.
  - L'autorizzazione pubblica per il file deriva dall'archivio autorizzazioni. Il parametro dell'autorizzazione pubblica (AUT) sul comando CRTPF o CRTLF viene ignorato.
  - L'archivio autorizzazioni viene collegato al file. L'autorizzazione specificata per l'archivio autorizzazioni viene utilizzata per proteggere il file.
- Se si cancella l'archivio autorizzazioni, le informazioni sull'autorizzazione vengono trasferite sul file stesso.
- Se un file viene rinominato e il nuovo nome del file corrisponde a un archivio autorizzazioni corrispondente, l'autorizzazione e la proprietà del file vengono modificate in modo da corrispondere all'archivio autorizzazioni. L'utente che ridenomina il file necessita dell'autorizzazione *ALL sull'archivio autorizzazioni.
- Se un file viene spostato in una libreria diversa e l'archivio autorizzazioni esiste per quel nome file e per la libreria di destinazione, l'autorizzazione e la proprietà del file vengono modificate in modo da corrispondere all'archivio autorizzazioni. L'utente che sposta il file deve disporre dell'autorizzazione *ALL sull'archivio autorizzazioni.
- La proprietà dell'archio autorizzazioni e il file corrispondono sempre. Se si modifica la proprietà del file, anche la proprietà dell'archivio autorizzazioni viene modificata.
- Quando si ripristina un file, se l'archivio autorizzazioni esiste per quel nome file e per la libreria per la quale è stato ripristinato, viene collegato all'archivio autorizzazioni.
- Gli archivi autorizzazioni non possono essere creati per i file contenuti in queste librerie: QSYS, QRCL, QRECOVERY, QSPL, QTEMP e QSPL0002 – QSPL0032.

Archivi autorizzazioni e migrazione System/36

System/36 Migration Aid crea un archivio autorizzazioni per ogni file che viene migrato. Crea inoltre un archivio autorizzazioni per le voci contenute nel file di sicurezza delle risorse System/36 se non esiste un file corrispondente su System/36.

Gli archiovi autorizzazioni sono necessari solo per i file che vengono cancellati e ricreati dalle applicazioni. Utilizzare il comando DLTAUTHLR (Cancellazione archivio autorizzazioni) per cancellare gli archivi autorizzazioni non necessari.

Rischi archivio autorizzazioni

È necessario prendere in considerazione la sicurezza quando si utilizza un archivio autorizzazioni.

Un archivio autorizzazioni consente di definire l'autorizzazione per un file prima che tale file esista. In determinate circostanze, ciò può consentire ad un utente non autorizzato di ottenere l'accesso alle informazioni. Se un utente sapesse che un'applicazione potrebbe creare, spostare o ridenominare un file, l'utente potrebbe creare un archivio autorizzazioni per il nuovo file. L'utente può accedere al file.

Per limitare questo rischio, il comando CRTAUTHLR viene fornito con l'autorizzazione pubblica *EXCLUDE. Solo gli utenti che posseggono l'autorizzazione *ALLOBJ possono utilizzare il comando, a meno che non si conceda l'autorizzazione ad altri.

Gestione autorizzazione

Questo argomento descrive i metodi più comunemente utilizzati per l'impostazione, la gestione e la visualizzazione delle informazioni sulle autorizzazioni relative al sistema.

L'Appendice A, "Comandi di sicurezza", a pagina 331 fornisce un elenco completo dei comandi disponibili per la gestione dell'autorizzazione. Le descrizioni che seguono non trattano tutti i parametri per i comandi o tutti i campi sui pannelli. Per i dettagli completi, consultare le informazioni in linea.

Pannelli autorizzazioni

Questa sezione tratta alcune caratteristiche dei pannelli che visualizzano le autorizzazioni oggetto.

Quattro pannelli visualizzano le autorizzazioni degli oggetti:

- Pannello Visualizzazione autorizzazione oggetto
- Pannello Editazione autorizzazione oggetto
- Pannello Visualizzazione autorizzazione
- Pannello Gestione autorizzazione

La Figura 10 mostra la versione base del pannello Visualizzazione autorizzazione oggetto:

```
                        Visualizzazione autorizzazione oggetto

Oggetto. . . . . :   CUSTNO    Proprietario  . . . . . :   PGMR1
  Libreria. . . . :   CUSTLIB   Gruppo principale  . . . :   DPTAR
Tipo oggetto . . . :   *DTAARA   Unità ASP   . . . . :   *SYSBAS

L'oggetto protetto dall'elenco di autorizzazioni  . . :   *NONE

                       Autorizzazione
Utente        Gruppo   oggetto
*PUBLIC                  *EXCLUDE
PGMR1                    *ALL
DPTAR                    *CHANGE
DPTSM                    *USE
F3=Fine F11=Visualiz. autoriz. ogget. dettag. F12=Annull.  F17=Inizio
```

Figura 10. Pannello Visualizzazione autorizzazione oggetto

I nomi delle autorizzazioni definiti dal sistema vengono visualizzati in questo pannello. F11 attiva e disattiva questa e altre due versioni del pannello. Uno mostra le autorizzazioni oggetto dettagliate:

```
                          Visualizzazione autorizzazione oggetto

Oggetto. . . . . :   CUSTNO    Proprietario  . . . . . :   PGMR1
  Libreria. . . . . :   CUSTLIB   Gruppo principale  . . . :   DPTAR
Tipo di oggetto. . :   *DTAARA         Unità ASP . . . . :   *SYSBAS

Oggetto protetto dall'elenco di autorizzazioni . . . . :   *NONE

                        Autor.    ----------Oggetto----------
Utente     Gruppo       oggetto   Opr  Gest.Esist. Alter. Rif.
*PUBLIC                 *EXCLUDE    X
PGMR1                   *ALL        X    X     X      X     X
DPTAR                   *CHANGE     X
DPTSM                   *USE        X
:
F3=Fine F11=Visualiz. autoriz. dati F12=Annull. F17=Inizio F18=Fine
```

L'altro pannello mostra le autorizzazioni dati:

```
                          Visualizzazione autorizzazione oggetto

Oggetto. . . . . :   CUSTNO    Proprietario  . . . . . :   PGMR1
  Libreria. . . . . :   CUSTLIB   Gruppo principale  . . . :   DPTAR
Tipo di oggetto. . :   *DTAARA     Unità ASP .  . . . . :   *SYSBAS

Oggetto protetto dall'elenco di autorizzazioni. . . . . :   *NONE

                        Autorizz.  ---------------Dati---------------
Utente     Gruppo       oggetto   Lett. Agg. Aggior. Canc.   Esecuz.
*PUBLIC                  *EXCLUDE
PGMR1                   *ALL        X    X     X      X     X
DPTAR                   *CHANGE     X     X     X       X       X
DPTSM                   *USE        X                           X
```

Se si dispone dell'autorizzazione *OBJMGT su un oggetto, l'utente visualizzerà tutte le autorizzazioni private per quell'oggetto. Se non si dispone dell'autorizzazione *OBJMGT, l'utente visualizza solo le proprie origini dell'autorizzazione per l'oggetto.

Ad esempio, se USERA visualizza l'autorizzazione per l'area di dati CUSTNO, viene visualizzata solo l'autorizzazione pubblica.

Se USERB, che è un membro del profilo gruppo DPTAR, visualizza l'autorizzazione per l'area dati CUSTNO, verrà visualizzato come segue:

```
                          Visualizzazione autorizzazione oggetto

Oggetto. . . . . :   CUSTNO    Proprietario  . . . . . :   PGMR1
  Libreria. . . . . :   CUSTLIB   Gruppo principale  . . . :   DPTAR
Tipo di oggetto. . :   *DTAARA     Unità ASP .  . . . . :   *SYSBAS

Oggetto protetto dall'elenco di autorizzazioni. . . . . :   *NONE

                        Autorizzazione
Utente        Gruppo   oggetto
*GROUP      DPTAR       *CHANGE
```

Se USERB esegue un programma che adotta l'autorizzazione di PGMR1 e visualizza l'autorizzazione per l'area dati CUSTNO, verrà visualizzato come segue:

```
                          Visualizzazione autorizzazione oggetto

Oggetto.. . . . . :   CUSTNO    Proprietario  . . . . . :   PGMR1
  Libreria  . . . :   CUSTLIB   Gruppo principale  . . . :   DPTAR
Tipo di oggetto. . :   *DTAARA     Unità ASP .  . . . . :   *SYSBAS

Oggetto protetto dall'elenco di autorizzazioni  . . . . :   *NONE

                        Autorizzazione
Utente        Gruppo    oggetto
*ADOPTED                USER DEF
*PUBLIC                  *EXCLUDE
PGMR1                   *ALL
*GROUP      DPTAR       *CHANGE
DPTSM                    *USE
```

L'autorizzazione *ADOPTED indica solo l'autorizzazione aggiuntiva proveniente dal proprietario del programma. USERB riceve da PGMR1 tutte le autorizzazioni che non sono inserite in *CHANGE. Il pannello visualizza tutte le autorizzazioni private poiché USERB ha adottato *OBJMGT. Il pannello dettagliato apparirà come segue:

```
                          Visualizzazione autorizzazione oggetto

Oggetto. . . . . :   CUSTNO    Proprietario  . . . . . :   PGMR1
  Libreria. . . . :   CUSTLIB   Gruppo principale  . . . :   DPTAR
Tipo di oggetto. . :   *DTAARA     Unità ASP .  . . . . :   *SYSBAS

Oggetto protetto dall'elenco di autorizzazioni  . . . . :   *NONE

                        Autorizzaz. -----------Oggetto-----------
Utente    Gruppo        oggetto    Opr Gest. Esist. Alter. Rif.
*ADOPTED                USER DEF         X     X      X     X
*PUBLIC                   *EXCLUDE
PGMR1                    *ALL        X    X     X      X     X
*GROUP     DPTAR        *CHANGE     X
DPTSM                    *USE        X
F3=Fine F11=Visualiz. autoriz. dati F12=Annull. F17=Inizio F18=Fine
```

Se il campo dell'opzione utente (USROPT) nel profilo utente di USERB comprende *EXPERT, ecco come apparirà il pannello:

```
                          Visualizzazione autorizzazione oggetto

Oggetto. . . . . :   CUSTNO    Proprietario  . . . . . :   PGMR1
  Libreria. . . . :   CUSTLIB   Gruppo principale  . . . :   DPTAR
Tipo di oggetto. . :   *DTAARA    Unità ASP . . . . .:   *SYSBAS

Oggetto protetto dall'elenco di autorizzazioni . . . . :   *NONE

                OBJECT     -----Oggetto------   ------Dati--------
Utente  Gruppo  Autorizzaz. O   M   E   A   R   R   A   U   D   E
*ADOPTED        USER DEF        X   X   X   X
*PUBLIC                  *EXCLUDE
PGMR1           *ALL        X   X   X   X   X   X   X   X   X   X
*GROUP  DPTAR   *CHANGE     X                   X   X   X   X   X
DPTSM           *USE        X                   X               X
```

Prospetti autorizzazioni

Sono disponibili diversi prospetti che facilitano il controllo dell'implementazione della sicurezza.

Ad esempio, è possibile controllare gli oggetti con l'autorizzazione *PUBLIC diversa da *EXCLUDE e gli oggetti con autorizzazioni private utilizzando i seguenti comandi:

- Stampa oggetti autorizzati pubblicamente (PRTPUBAUT)
- Stampa autorizzazioni private (PRTPVTAUT)

Informazioni correlate

System security tools

Gestione librerie

È possibile specificare l'autorizzazione per le librerie e i nuovi oggetti creati nelle librerie.

Due parametri sul comando Creazione libreria (CRTLIB) coinvolgono l'autorizzazione:

Autorizzazione (AUT): il parametro AUT può essere utilizzato per specificare una delle seguenti autorizzazioni:

- L'autorizzazione pubblica per la libreria
- L'elenco di autorizzazioni che protegge la libreria.

Il parametro AUT si applica alla libreria stessa, non agli oggetti contenuti nella libreria. Se si specifica il nome di un elenco di autorizzazioni, l'autorizzazione pubblica per la libreria è impostata su *AUTL.

Se non si specifica AUT al momento della creazione di una libreria, *LIBCRTAUT è il valore predefinito. Il sistema utilizza il valore CRTAUT proveniente dalla libreria QSYS, che viene fornita come *SYSVAL.

Creazione autorizzazione (CRTAUT): il parametro CRTAUT determina l'autorizzazione predefinita per i nuovi oggetti creati nella libreria. CRTAUT può essere impostato su una delle autorizzazioni definite dal sistema (*ALL, *CHANGE, *USE o *EXCLUDE), su *SYSVAL (il valore di sistema QCRTAUT) o sul nome di un elenco di autorizzazioni.

Nota: è possibile modificare il valore CRTAUT per una libreria che utilizza il comando Modifica libreria (CHGLIB).

Se l'utente PGMR1 immette questo comando:

```
CRTLIB TESTLIB AUT(LIBLST) CRTAUT(OBJLST)
```

l'autorizzazione per la libreria apparirà come segue:

```
                        Visualizzazione autorizzazione oggetto

Oggetto . . . . . :   TESTLIB    Proprietario  . . . . . :   PGMR1
  Libreria. . . . :   QSYS        Gruppo principale  . . . :   *NONE
Tipo di oggetto. . :   *LIB          Unità ASP . . . . . :   *SYSBAS

Oggetto protetto da elenco di autorizzazioni. . . . . :   LIBLST

                         Autorizzazione
Utente        Gruppo   oggetto
*PUBLIC                 *AUTL
PGMR1                   *ALL
```

- Poiché è stato specificato un elenco di autorizzazioni per il parametro AUT, l'autorizzazione pubblica viene impostata su *AUTL.

- L'utente che esegue il comando CRTLIB possiede la libreria, a meno che il profilo dell'utente non specifichi OWNER(*GRPPRF). Al proprietario viene fornita automaticamente l'autorizzazione *ALL.
- Il valore CRTAUT non viene visualizzato sui pannelli delle autorizzazioni degli oggetti. Utilizzare il comando Visualizzazione descrizione libreria (DSPLIBD) per visualizzare il valore CRTAUT per una libreria.

```
                      Visualizzazione descrizione libreria

Libreria. . . . . :   TESTLIB

Tipo  . . . . . :   PROD
Numero ASP . . . . . : 1
Unità ASP . . . . . :   *SYSBAS
Creazione autorizzazione. . . . . :   OBJLST
Creazione controllo oggetto. . . . . :   *SYSVAL
Descrizione testo . . . . . :   Rec. cliente
```

Creazione di oggetti

È possibile specificare l'autorizzazione di un nuovo oggetto.

Quando si crea un nuovo oggetto, è possibile specificare l'autorizzazione (AUT) o utilizzare il valore predefinito, *LIBCRTAUT. Se PGMR1 immette questo comando:

```
CRTDTAARA (TESTLIB/DTA1) +
   TYPE(*CHAR)
```

l'autorizzazione per l'area dati apparirà come segue:

```
                         Visualizzazione autorizzazione oggetto

Oggetto. . . . . :   DTA1        Proprietario. . . . . :   PGMR1
  Libreria. . . . . :   TESTLIB     Gruppo principale. . . :   *NONE
Tipo di oggetto. . :   *DTAARA     Unità ASP . . . . . :   *SYSBAS

Oggetto protetto dall'elenco di autorizzazioni. . . . . :   OBJLST

                        Autorizzazione
Utente        Gruppo   oggetto
*PUBLIC                 *AUTL
PGMR1                   *ALL
```

L'elenco di autorizzazioni (OBJLST) proviene dal parametro CRTAUT specificato al momento della creazione di TESTLIB.

Se PGMR1 immette questo comando:

```
CRTDTAARA (TESTLIB/DTA2) AUT(*CHANGE) +
   TYPE(*CHAR)
```

l'autorizzazione per l'area dati apparirà come segue:

```
                          Visualizzazione autorizzazione oggetto

Oggetto. . . . . :   DTA2       Proprietario. . . . . :   PGMR1
  Libreria. . . . :   TESTLIB    Gruppo principale. . . :   *NONE
Tipo di oggetto. . :   *DTAARA     Unità ASP . . . . . :   *SYSBAS

Oggetto protetto dall'elenco di autorizzazioni . . . . :   *NONE

                        Autorizzazione
Utente        Gruppo   oggetto
*PUBLIC                 *CHANGE
PGMR1                   *ALL
```

Gestione autorizzazione oggetto individuale

È possibile modificare l'autorizzazione per un oggetto.

Per modificare l'autorizzazione per un oggetto, è necessario disporre di una delle seguenti autorizzazioni:

- Autorizzazione *ALLOBJ o appartenenza a un profilo gruppo che dispone dell'autorizzazione speciale *ALLOBJ.

  Nota: l'autorizzazione del gruppo non è utilizzata se si dispone di un'autorizzazione privata sull'oggetto.
- Proprietà dell'oggetto. Se un profilo gruppo possiede l'oggetto, ogni membro del gruppo può agire come proprietario dell'oggetto, a meno che al membro non sia stata fornita un'autorizzazione specifica che non soddisfa i requisiti necessari per la modifica dell'autorizzazione dell'oggetto.
- L'autorizzazione *OBJMGT sull'oggetto e le autorizzazioni concesse o revocate (tranne *EXCLUDE). Ogni utente può gestire l'autorizzazione dell'oggetto e può concedere o revocare l'autorizzazione *EXCLUDE.

Il modo più semplice per modificare l'autorizzazione per un singolo oggetto consiste nell'utilizzare il pannello Modifica autorizzazione oggetto. Questo pannello può essere richiamato direttamente utilizzando il comando Modifica autorizzazione oggetto (EDTOBJAUT) o selezionato come opzione dal pannello Gestione oggetti per proprietario o Gestione oggetti (WRKOBJ).

```
                          Editazione autorizzazione oggetto

Oggetto . . . . . :   DTA1       Proprietario. . . . . :   PGMR1
  Libreria  . . . . :   TESTLIB        Gruppo principale . . . :   *NONE
Tipo di oggetto . :   *DTAARA    Unità ASP . . . . . :   *SYSBAS

Immettere le modifiche alle autorizzazioni correnti e premere Invio.

  Oggetto protetto da elenco di autorizzazioni. . . . :   OBJLST

                        Autorizzazione
Utente        Gruppo   oggetto
*PUBLIC                 *AUTL
PGMR1                   *ALL
```

È possibile utilizzare inoltre questi comandi per modificare l'autorizzazione oggetto:

- Modifica autorizzazione (CHGAUT)
- Gestione autorizzazione (WRKAUT)
- Concessione autorizzazione oggetto (GRTOBJAUT)

- Revoca autorizzazione oggetto (RVKOBJAUT)

Per specificare le sottoserie di autorizzazioni generiche, come ad esempio Lettura/Scrittura (*RW) o Scrittura/Esecuzione (*WX), è necessario utilizzare i comandi CHGAUT o WRKAUT.

Specifica autorizzazione definita dall'utente

Questo argomento fornisce informazioni sulla specifica delle autorizzazioni definite dall'utente.

La colonna Autorizzazione oggetto sul pannello Modifica autorizzazione oggetto consente di specificare una qualsiasi delle serie di autorizzazioni definite dal sistema (*ALL, *CHANGE, *USE, *EXCLUDE). Se si desidera specifica l'autorizzazione che non è una serie definita dal sistema, utilizzare F11 (Visualizzazione dettagli).

Nota: se il campo *Opzioni utente* (USROPT) nel profilo utente è impostato su *EXPERT, l'utente vedrà sempre questa versione dettagliata del pannello senza dover premere F11.

Ad esempio, PGMR1 rimuove l'autorizzazione *OBJEXIST sul file CONTRACTS, per impedire la cancellazione accidentale del file. Poiché PGMR1 dispone di una combinazione di autorizzazioni che non fa parte delle serie definite dal sistema, il sistema inserisce *USER DEF* (definito dall'utente) nella colonna Autorizzazione oggetto:

```
                          Editazione autorizzazione oggetto

Oggetto . . . . . :   CONTRACTS      Proprietario. . . . . :   PGMR1
  Libreria. . . . . :   TESTLIB        Gruppo principale . . . :   *NONE
Tipo di oggetto. . :   *FILE       Unità ASP . . . . . :   *SYSBAS

Immettere le modifiche alle autorizzazioni correnti e premere Invio.

  Oggetto protetto dall'elenco di autorizzazioni. . . . . :   LIST2

                       Autor.    ----------Oggetto----------
Utente     Gruppo      oggetto   Opr  Gest.Esist. Alter. Rif.
*PUBLIC                *AUTL
PGMR1                  USER DEF    X    X            X     X
```

È possibile premere F11 (Visualizzazione autorizzazioni dati) per visualizzare o modificare le autorizzazioni dati:

```
                          Editazione autorizzazione oggetto

 Oggetto . . . . . :   CONTRACTS      Proprietario. . . . . :   PGMR1
  Libreria  . . . . . :   TESTLIB        Gruppo principale . . . :   *NONE
 Tipo di oggetto . . :   *FIL        Unità ASP . . . . . :   *SYSBAS

Immettere le modifiche alle autorizzazioni correnti e premere Invio.

 Oggetto protetto dall'elenco di autorizzazioni. . . . :   LIST2

                       Autorizz.  ---------------Dati---------------
Utente     Gruppo      oggetto   Lett. Agg. Aggior. Canc.   Esecuz.
*PUBLIC                *AUTL
PGMR1                  USER DEF    X     X     X       X        X
```

Concessione autorizzazione ai nuovi utenti

È possibile concedere l'autorizzazione ai nuovi utenti.

Per fornire l'autorizzazione ad altri utenti, premere il tasto F6 (Aggiunta nuovi utenti) dal pannello Modifica autorizzazione oggetto. L'utente visualizza il pannello Aggiunta nuovi utenti che consente di definire l'autorizzazione per più utenti:

```
                            Aggiunta nuovi utenti

Oggetto. . . . . . . :   DTA1
  Libreria . . . . . :     TESTLIB

Immettere nuovi utenti e premere Invio.

            Autorizzazione
Utente      Autorizzazione
USER1       *USE
USER2       *CHANGE
PGMR2       *ALL
```

Rimozione di un'autorizzazione utente

È possibile anche rimuovere un'autorizzazione dell'utente per un oggetto.

La rimozione dell'autorizzazione dell'utente per un oggetto differisce dalla concessione dell'autorizzazione *EXCLUDE all'utente. L'autorizzazione *EXCLUDE indica che l'utente non può, specificatamente, utilizzare l'oggetto. Solo l'autorizzazione speciale *ALLOBJ e l'autorizzazione adottata sovrascrivono l'autorizzazione *EXCLUDE.

Nota: è possibile sovrascrivere l'autorizzazione *EXCLUDE per un profilo gruppo se l'utente dispone di un altro profilo gruppo con autorizzazione privata all'oggetto.

Rimuovere un'autorizzazione utente indica che l'utente non dispone di autorizzazioni specifiche sull'oggetto. L'utente può ottenere l'accesso mediante un profilo gruppo, un elenco di autorizzazioni, l'autorizzazione pubblica, l'autorizzazione speciale *ALLOBJ o l'autorizzazione adottata.

È possibile rimuovere l'autorizzazione di un utente utilizzando il pannello Modifica autorizzazione oggetto. Immettere degli spazi nel campo Autorizzazione oggetto per l'utente e premere il tasto Invio. L'utente viene rimosso dal pannello. È possibile inoltre utilizzare il comando Revoca autorizzazione oggetto (RVKOBJAUT). Revocare l'autorizzazione specifica dell'utente oppure revocare l'autorizzazione *ALL per l'utente.

Nota: il comando RVKOBJAUT revoca solo l'autorizzazione specificata dall'utente. Ad esempio, USERB dispone dell'autorizzazione *ALL su FILEB nella libreria LIBB. L'utente revoca l'autorizzazione *CHANGE:

```
RVKOBJAUT OBJ(LIBB/FILEB) OBJTYPE(*FILE) +
USER(*USERB) AUT(*CHANGE)
```

Dopo l'esecuzione del comando, l'autorizzazione di USERB su FILEB appare come di seguito riportato:

```
                      Visualizzazione autorizzazione oggetto

Oggetto . . . . . :   FILEB     Proprietario  . . . . . :   PGMR1
  Libreria. . . . . :   LIBB      Gruppo principale . . . :   *NONE
Tipo di oggetto. . :   *FILE     Unità ASP .  . . . . :   *SYSBAS

  Oggetto protetto dall'elenco di autorizzazioni. . . :   *NONE

                     Autoriz.   --------Oggetto------------
Utente     Gruppo       oggetto   Opr  Gest.Esist. Alter. Rif.
USERB            USER DEF         X    X       X       X
```

```
                      Visualizzazione autorizzazione oggetto

Oggetto . . . . . :   FILEB     Proprietario  . . . . . :   PGMR1
  Libreria. . . . . :   LIBB      Gruppo principale . . . :   *NONE
Tipo di oggetto. . :   *FILE     Unità ASP  . . . . . :   *SYSBAS

Oggetto protetto da elenco di autorizzazioni . . . . . .   *NONE

                     Autorizz.  ---------------Dati---------------
Utente     Gruppo       oggetto   Lett. Agg. Aggior. Canc.   Esecuz.
USERB                   USER DEF
```

Gestione autorizzazione per più oggetti

Fornisce informazioni su come apportare modifiche all'autorizzazione su più di un oggetto alla volta.

Il pannello Modifica autorizzazione oggetto consente di gestire in modo interattivo l'autorizzazione per un oggetto alla volta. Il comando Concessione autorizzazione oggetto (GRTOBJAUT) consente di apportare modifiche all'autorizzazione su più di un oggetto alla volta. È possibile utilizzare il comando dell'autorizzazione GRTOBJAUT in modalità interattiva o in batch. È possibile inoltre richiamarlo da un programma.

Di seguito, vengono riportati degli esempi su come utilizzare il comando GRTOBJAUT, visualizzando il pannello di richiesta. Quando si esegue il comando, si riceve un messaggio per ciascun oggetto che indica se la modifica è stata apportata. Le modifiche all'autorizzazione richiedono un blocco esclusivo sull'oggetto e non possono essere apportata quando l'oggetto è in uso. Stampare la registrazione dei lavori per un record di modifiche tentate ed eseguite.

- Per fornire a tutti gli oggetti contenuti nella libreria TESTLIB un'autorizzazione pubblica *USE:

```
                   Concessione autorizzazione oggetto (GRTOBJAUT)

Immettere le scelte e premere Invio.
Oggetto. . . . . .  *ALL
Libreria  . . . . . .  TESTLIB
Tipo oggetto. . . . . .  *ALL
Unità ASP  . . . . . .  *
Utenti. . . . . .  *PUBLIC
+ per altri valori
Autorizzazione. . . . . .  *USE
```

Questo esempio del comando GRTOBJAUT fornisce l'autorizzazione specificata ma non rimuove le autorizzazioni maggiori di quella specificata. Se alcuni oggetti nella libreria TESTLIB dispongono dell'autorizzazione pubblica *CHANGE, il comando visualizzato non riduce l'autorizzazione pubblica

su *USE. Per accertarsi che tutti gli oggetti in TESTLIB dispongano dell'autorizzazione pubblica *USE, utilizzare il comando GRTOBJAUT con il parametro REPLACE.

```
GRTOBJAUT OBJ(TESTLIB/*ALL) OBJTYPE(*ALL) +
          USER(*PUBLIC) REPLACE(*YES)
```

Il parametro REPLACE indica se le autorizzazioni specificate sostituiscono l'autorizzazione esistente per l'utente. Il valore predefinito di REPLACE(*NO) fornisce l'autorizzazione specificata, ma non rimuove l'autorizzazione maggiore di quella specificata, a meno che non sia stata concessa l'autorizzazione *EXCLUDE.

Questi comandi impostano l'autorizzazione pubblica solo per gli oggetti attualmente esistenti nella libreria. Per impostare l'autorizzazione pubblica per i nuovi oggetti creati in seguito, utilizzare il parametro CRTAUT sulla descrizione della libreria.

- Fornire l'autorizzazione *ALL ai file di lavoro nella libreria TESTLIB agli utenti AMES e SMITHR. In questo esempio, i file di lavoro iniziano tutti con i caratteri WRK:

```
                    Concessione autorizzazione oggetto (GRTOBJAUT)

Immettere le scelte e premere Invio.

Oggetto. . . . . . . . . . . .   WRK*
  Libreria . . . . . . . . . .   TESTLIB
Tipo oggetto  . . . . . . . . .   *FILE
Unità ASP  . . . . . . . . . . *
Utenti . . . . . . . . . . . .   AMES
             + per altri valori  SMITHR
Autorizzazione. . . . . . . . .   *ALL
```

Questo comando utilizza un nome generico per specificare i file. L'utente specifica un nome generico immettendo una stringa di caratteri seguita da un asterisco (*). Le informazioni in linea indicano i parametri di un comando che consentono un nome generico.

- Per proteggere i file che iniziano con i caratteri AR* utilizzando un elenco di autorizzazioni chiamato ARLST1 e fare in modo che i file richiamino l'autorizzazione pubblica dall'elenco, utilizzare i due seguenti comandi:

  1. Proteggere i file con l'elenco di autorizzazioni utilizzando il comando GRTOBJAUT:

```
                    Concessione autorizzazione oggetto

Immettere le scelte e premere Invio.

Oggetto. . . . . . . . . . . .   AR*
  Libreria . . . . . . . . . .   TESTLIB
Tipo oggetto  . . . . . . . . .   *FILE
Unità ASP  . . . . . . . . . . *

:
Elenco di autorizzazioni  . . . . . .   ARLST1
```

  2. Impostare l'autorizzazione pubblica per i file su *AUTL, utilizzando il comando GRTOBJAUT:

```
                    Concessione autorizzazione oggetto

Immettere le scelte e premere Invio.

Oggetto. . . . . .   AR*
  Libreria . . . . . .   TESTLIB
Tipo oggetto  . . . . . .   *FILE
Unità ASP  . . . . . .  *
Utenti . . . . . .   *PUBLIC
              + per altri valori
Autorizzazione. . . . . .   *AUTL
```

Gestione proprietà oggetto

È possibile modificare la proprietà di un oggetto in diversi modi.

Per modificare la proprietà di un oggetto, utilizzare uno dei seguenti comandi:

- Comando Modifica proprietario oggetto (CHGOBJOWN)
- Comando Gestione oggetti per proprietario (WRKOBJOWN)
- Comando Modifica proprietario (CHGOWN)

Il pannello Gestione oggetti per proprietario mostra tutti gli oggetti di proprietà di un profilo. È possibile assegnare singoli oggetti a un nuovo proprietario. Inoltre, l'utente può modificare la proprietà di più di un oggetto alla volta, utilizzando il parametro NEWOWN (nuovo proprietario) nella parte inferiore del pannello:

```
                        Gestione oggetti per proprietario

Profilo utente . . . . . :   OLDOWNER

Immettere le opzioni e premere Invio.
  2=Modifica autorizzazione  4=Eliminaz.   5=Visualizzaz. autore
  8=Visualizzazione descrizione   9=Modifica proprietario
                                                          Unità
Opz  Oggetto       Libreria      Tipo      Attributo      ASP
     COPGMMSG      COPGMLIB      *MSGQ                    *SYSBAS
9    CUSTMAS       CUSTLIB       *FILE                    *SYSBAS
9    CUSTMSGQ      CUSTLIB       *MSGQ                    *SYSBAS
     ITEMMSGQ      ITEMLIB       *MSGQ                    *SYSBAS

Parametri o comandi
===> NEWOWN(OWNIC)
F3=Fine   F4=Richies. F5=Rivisual. F9=Duplicazione
F18=Fine
```

Quando si modifica la proprietà utilizzando un metodo, è possibile scegliere di rimuovere l'autorizzazione sull'oggetto del proprietario precedente. Il valore predefinito per il parametro CUROWNAUT (autorizzazione proprietario corrente) è *REVOKE.

Per trasferire la proprietà di un oggetto, è necessario disporre:

- Dell'autorizzazione all'esistenza dell'oggetto per l'oggetto
- Dell'autorizzazione *ALL o della proprietà, se l'oggetto è un elenco di autorizzazioni
- L'autorizzazione all'aggiunta per il profilo utente del nuovo proprietario
- L'autorizzazione alla cancellazione per il profilo utente dell'attuale proprietario

L'utente non può cancellare un profilo utente che possiede gli oggetti. L'argomento "Cancellazione profili utente" a pagina 130 mostra i metodi per gestire gli oggetti di proprietà quando si cancella un profilo.

Il pannello Gestione oggetti per proprietario comprende gli oggetti IFS (Integrated File System). Per tali oggetti, la colonna *Oggetto* nel pannello mostra i primi 18 caratteri del nome del percorso. Se il nome del percorso ha una lunghezza superiore a 18 caratteri, appare il simbolo maggiore di (>) alla fine del nome del percorso. Per visualizzare il nome del percorso assoluto, posizionare il cursore ovunque sul nome del percorso e premere il tasto F22.

Gestione autorizzazione gruppo principale

È possibile modificare il gruppo principale o l'autorizzazione del gruppo principale su un oggetto.

Per modificare il gruppo principale o l'autorizzazione del gruppo principale su un oggetto, utilizzare uno dei seguenti comandi:

- CHGOBJPGP (Modifica gruppo principale oggetto)
- WRKOBJPGP (Gestione oggetti per gruppo principale)
- CHGPGP (Modifica gruppo principale)

Quando si modifica il gruppo primario dell'oggetto, si specifica l'autorizzazione posseduta dal nuovo gruppo principale. È possibile inoltre revocare l'autorizzazione del vecchio gruppo principale. Se non si revoca l'autorizzazione del vecchio gruppo principale, diviene un'autorizzazione privata.

Il nuovo gruppo principale non può essere il proprietario dell'oggetto.

Per modificare il gruppo principale di un oggetto, è necessario disporre di tutte le seguenti autorizzazioni:

- L'autorizzazione *OBJEXIST per l'oggetto.
- Se l'oggetto è un file, libreria o descrizione del sottosistema, sono necessarie le autorizzazioni *OBJOPR e *OBJEXIST.
- Se l'oggetto è un elenco di autorizzazioni, è necessaria l'autorizzazione speciale *ALLOBJ o bisogna essere il proprietario dell'elenco di autorizzazioni.
- Se si revoca l'autorizzazione per il vecchio gruppo principale, è necessaria l'autorizzazione *OBJMGT.
- Se si specifica un valore diverso da *PRIVATE, è necessaria l'autorizzazione *OBJMGT e tutte le autorizzazioni fornite.

Utilizzo di un oggetto di riferimento

Sia il pannello Editazione autorizzazione oggetto che il comando GRTOBJAUT consentono di fornire l'autorizzazione ad un oggetto (o gruppo di oggetti) in base all'autorizzazione di un oggetto di riferimento.

Questo strumento si rivela utile in alcune situazioni, ma l'utente dovrebbe comunque valutare l'utilizzo di un elenco di autorizzazioni che soddisfino i requisiti. Consultare "Vantaggi dell'utilizzo dell'elenco di autorizzazioni" a pagina 178 per informazioni sui vantaggi dell'utilizzo degli elenchi di autorizzazioni.

Copia autorizzazione da un utente

È possibile copiare tutte le autorizzazioni private da un profilo utente su un altro mediante il comando Concessione autorizzazione utente (GRTUSRAUT).

Questo metodo può risultare utile in determinate situazioni. Ad esempio, il sistema non consente di rinominare un profilo utente. Per creare un profilo identico con un nome diverso sono necessarie diverse operazioni, compresa la copia delle autorizzazioni dei profili originali. "Ridenominazione di un profilo utente" a pagina 135 visualizza un esempio di come sia possibile fare ciò.

Il comando GRTUSRAUT copia solo le autorizzazioni private. Non vengono copiate le autorizzazioni speciali; né viene trasferita la proprietà dell'oggetto.

Il comando GRTUSRAUT non dovrebbe essere utilizzato in alternativa alla creazione dei profili gruppo. GRTUSRAUT crea un set duplicato di autorizzazioni private, che aumenta il tempo impiegato per il salvataggio del sistema e rende la gestione delle autorizzazioni più difficile. GRTUSRAUT copia le autorizzazioni così come esistono in un particolare momento. Se l'autorizzazione viene richiesta in futuro dai nuovi oggetti, ogni singolo profilo deve avere garantita l'autorizzazione. Il profilo gruppo fornisce questa funzione automaticamente.

Per utilizzare il comando GRTUSRAUT, è necessario disporre di tutte le autorizzazioni copiate. Se non si dispone di un'autorizzazione, tale autorizzazione non viene concessa al profilo di destinazione. Il sistema invia un messaggio per ciascuna autorizzazione concessa o meno al profilo utente di destinazione. Stampare la registrazione lavori per un record completo. Per evitare di avere un set parziale di autorizzazioni copiate, il comando GRTUSRAUT dovrebbe essere eseguito da un utente con l'autorizzazione speciale *ALLOBJ.

Attività correlate

"Copia delle autorizzazioni private" a pagina 129
È possibile copiare le autorizzazioni private da un profilo utente ad un altro utilizzando il comando Concessione autorizzazione utente (GRTUSRAUT).

Gestione elenchi di autorizzazioni

Questa sezione descrive i passi per la creazione di un elenco di autorizzazioni.

Per impostare un elenco di autorizzazioni è necessario rispettare tre passi:

1. Creazione dell'elenco di autorizzazioni.
2. Aggiunta degli utenti all'elenco di autorizzazioni.
3. Protezione degli oggetti con l'elenco di autorizzazioni.

I passi 2 e 3 possono essere eseguiti in qualsiasi ordine.

Vantaggi dell'utilizzo dell'elenco di autorizzazioni

| È possibile utilizzare elenchi di autorizzazioni per proteggere gli oggetti sul proprio sistema.

Un elenco autorizzazioni dispone dei seguenti vantaggi:

- Gli elenchi autorizzazioni semplificano la gestione delle autorizzazioni. L'autorizzazione utente viene definita per l'elenco autorizzazioni e non per il singolo oggetto presente sull'elenco. Se un nuovo oggetto viene protetto dall'elenco autorizzazioni, gli utenti sull'elenco ottengono l'autorizzazione per l'oggetto.
- È possibile effettuare un'operazione per fornire un'autorizzazione utente a tutti gli oggetti presenti sull'elenco.
- Gli elenchi di autorizzazioni riducono il numero di autorizzazioni private sul sistema. Ogni utente dispone di un'autorizzazione privata per un oggetto, l'elenco autorizzazioni. In questo modo, l'utente avrà l'autorizzazione a tutti gli oggetti presenti sull'elenco. Riducendo il numero di autorizzazioni private nel sistema si hanno i seguenti vantaggi:
  - Si riduce la dimensione dei profili utente.
  - Si migliorano le prestazioni quando si salva il sistema (SAVSYS) o si salvano i dati sulla sicurezza (SAVSECDTA).
- Gli elenchi di autorizzazioni forniscono un metodo sicuro per proteggere i file. Se si utilizzano autorizzazioni private, ogni utente disporrà di un'autorizzazione privata per ogni membro file. Se si utilizza un elenco di autorizzazioni, ogni utente avrà una sola autorizzazione. Inoltre, non è possibile né concedere né revocare un'autorizzazione per i file aperti. Se si protegge un file con un elenco di autorizzazioni, è possibile modificare le autorizzazioni, anche quando il file è aperto.
- Gli elenchi autorizzazioni forniscono un modo per tenere in mente le autorizzazioni quando viene salvato un oggetto. Quando viene salvato un oggetto protetto da un elenco di autorizzazioni, il nome

dell'elenco autorizzazioni viene salvato con l'oggetto. Se l'oggetto viene cancellato e ripristinato sullo stesso sistema, viene collegato di nuovo, automaticamente, all'elenco di autorizzazioni. Se l'oggetto viene ripristinato su un sistema differente, l'elenco di autorizzazioni non viene collegato, a meno che non venga specificato ALWOBJDIF(*ALL) o ALWOBJDIF(*AUTL) sul comando di ripristino.

- Da un punto di vista di gestione della sicurezza, l'elenco di autorizzazioni è il metodo migliore per gestire gli oggetti con gli stessi requisiti di sicurezza. Anche quando sono presenti pochi oggetti protetti dall'elenco, risulta più vantaggioso utilizzare un elenco di autorizzazioni invece di utilizzare autorizzazioni private per l'oggetto. Poiché le autorizzazioni si trovano in una determinata parte (nell'elenco di autorizzazioni), risulta più semplice modificare l'utente che dispone dell'autorizzazione per l'oggetto. Inoltre, risulta più semplice proteggere qualsiasi nuovo oggetto con le stesse autorizzazioni degli oggetti esistenti.

Creazione di un elenco di autorizzazioni

Utilizzare il comando CRTAUTL (Creazione di un elenco di autorizzazioni) per creare un elenco di autorizzazioni.

Non è necessaria alcuna autorizzazione sulla libreria QSYS per creare un elenco di autorizzazioni in quella libreria. Utilizzare il comando CRTAUTL (Creazione elenco di autorizzazioni):

```
                     Creazione elenco di autorizzazione (CRTAUTL)

Immettere le scelte e premere Invio.

Elenco di autorizzazioni. . . . . .   custlst1       Nome
Testo 'descrizione'. . . . . .   File cancellati a fine mese

                           Parametri aggiuntivi

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

Il parametro AUT imposta l'autorizzazione pubblica per ciascuno degli oggetti protetti dall'elenco. L'autorizzazione pubblica dall'elenco di autorizzazioni viene utilizzata solo quando l'autorizzazione pubblica protetta dall'elenco è *AUTL.

Concessione dell'autorizzazione agli utenti per un elenco di autorizzazioni

Utilizzare il pannello the Editazione elenco di autorizzazioni (EDTAUTL) per concedere l'autorizzazione agli utenti per l'elenco di autorizzazioni creato.

Per gestire l'autorizzazione di cui gli utenti dispongono per l'elenco di autorizzazioni, è necessario avere l'autorizzazione *AUTLMGT (gestione elenco autorizzazioni) ed anche le autorizzazioni specifiche che si stanno concedendo. Consultare l'argomento "Gestione elenco autorizzazioni" a pagina 149 per una descrizione completa.

È possibile utilizzare il pannello Editazione elenco di autorizzazioni (EDTAUTL) per modificare l'autorizzazione utente sull'elenco di autorizzazioni o per aggiungere nuovi utenti all'elenco:

```
                          Editazione elenco di autorizzazioni

Oggetto . . . . . :   CUSTLST1        proprietario. . . . . :   PGMR1
  Libreria  . . . . :     QSYS          Gruppo principale  . . . :   *NONE

Immettere le modifiche alle autorizzazioni correnti e premere Invio.

            Autorizz. Gestione
Utente       oggetto   elenco
*PUBLIC     *USE
PGMR1       *ALL        X
```

Per fornire ai nuovi utenti l'autorizzazione sull'elenco di autorizzazioni, premere il tasto F6 (Aggiunta nuovi utenti):

```
                              Aggiunta nuovi utenti

Oggetto. . . . . :   CUSTLST1    Propriet.. . PGMR1
  Libreria . . . . :     QSYS

Immettere nuovi utenti e premere Invio.

            Autorizz. Gestione
Utente       oggetto   elenco
AMES        *CHANGE
SMITHR      *CHANGE
```

Ogni autorizzazione utente sull'elenco viene in realtà memorizzata come autorizzazione privata in quel profilo utente. È possibile inoltre utilizzare i comandi per gestire gli utenti dell'elenco di autorizzazioni, in modalità interattiva o in batch:

- Utilizzare il comando Aggiunta voce elenco di autorizzazioni (ADDAUTLE) per definire l'autorizzazione per utenti aggiuntivi.
- Utilizzare il comando Modifica voce elenco di autorizzazioni (CHGAUTLE) per modificare l'autorizzazione per gli utenti già autorizzati all'elenco.
- Utilizzare il comando Eliminazione voce elenco di autorizzazioni (RMVAUTLE) per rimuovere l'autorizzazione di un elenco sull'elenco.
- Utilizzare il comando Gestione autorizzazione (WRKAUT) per visualizzare l'elenco di utenti autorizzati di un oggetto.
- Utilizzare il comando Modifica autorizzazione (CHGAUT) per modificare l'autorizzazione di un utente per l'oggetto.

Protezione degli oggetti con un elenco di autorizzazioni.

Per proteggere un oggetto con un elenco di autorizzazioni, è necessario possedere l'oggetto, disporre dell'autorizzazione *ALL su di esso oppure disporre dell'autorizzazione speciale *ALLOBJ.

Utilizzare il pannello Editazione autorizzazione oggetto, il comando GRTOBJAUT, il comando WRKAUT o il comando CHGAUT per proteggere un oggetto con un elenco di autorizzazioni.

```
                          Editazione autorizzazione oggetto

Oggetto . . . . . :   ARWRK1      Proprietario. . . . . :   PGMR1
  Libreria. . . . :   TESTLIB       Gruppo principale . . . . :   *NONE
Tipo di oggetto. . :   *FILE     Unità ASP  . . . . . :   *SYSBAS

Immettere le modifiche alle autorizzazioni correnti e premere Invio.

  Oggetto protetto dall'elenco di autorizzazioni. . . . . .   ARLST1

            Autorizzazione
Utente      Autorizzazione
*PUBLIC     *AUTL
PGMR1       *ALL
```

Impostare l'autorizzazione pubblica per l'oggetto su *AUTL, se si desidera che l'autorizzazione pubblica provenga dall'elenco di autorizzazioni.

Sul pannello Editazione elenco di autorizzazioni, è possibile utilizzare F15 (Visualizzazione oggetti elenco di autorizzazioni) per elencare tutti gli oggetti protetti dall'elenco:

```
                     Visualizzazione oggetti elenco autorizzazioni

Elenco di autorizzazioni . . . . . :   CUSTLST1
  Libreria. . . . . . . . . . . . :   CUSTLIB
Proprietario. . . . . . . . . . . . :   OWNAR
Gruppo principale. . . . . . . . . :   DPTAR

                                          Gruppo
Oggetto     Libreria    Tipo      Propriet.   principale  Testo
CUSTMAS     CUSTLIB     *FILE     OWNAR
CUSTADDR    CUSTLIB     *FILE     OWNAR
```

Questo è un semplice elenco informativo. Non è possibile aggiungere o rimuovere oggetti dall'elenco. È possibile inoltre utilizzare il comando Visualizzazione oggetti elenco autorizzazioni (DSPAUTLOBJ) per visualizzare o stampare un elenco di tutti gli oggetti protetti dall'elenco.

Impostazione di un elenco di autorizzazioni

L'impostazione di un elenco di autorizzazioni rende più semplice modificare chi è autorizzato agli oggetti e proteggere qualsiasi nuovo oggetto con le stesse autorizzazioni degli oggetti esistenti.

Nell'azienda di giocattoli JKL, viene utilizzato un elenco di autorizzazioni per proteggere tutti i file di lavoro utilizzati nell'elaborazione dell'inventario di fine mese. Tali file di lavoro vengono eliminati, per effettuare questa operazione, è necessario disporre dell'autorizzazione *OBJMGT. Quando i requisiti dell'applicazione cambiano, è possibile aggiungere più file all'applicazione. Inoltre, quando cambiano le responsabilità lavoro, utenti differenti possono eseguire l'elaborazione di fine mese. L'elenco di autorizzazioni, rende più semplice la gestione di queste modifiche.

Attenersi a questa procedura per impostare l'elenco di autorizzazioni.

1. Creare l'elenco di autorizzazioni:
   ```
   CRTAUTL ICLIST1
   ```
2. Proteggere tutti i file di lavoro con l'elenco di autorizzazioni:
   ```
   GRTOBJAUT OBJ(ITEMLIB/ICWRK*) +
             OBJTYP(*FILE) AUTL(ICLIST1)
   ```
3. Aggiungere gli utenti all'elenco che ha eseguito l'elaborazione di fine mese:
   ```
   ADDAUTLE AUTL(ICLIST1) USER(USERA) AUT(*ALL)
   ```

Se si utilizzano gli elenchi di autorizzazioni, non si dovrebbe disporre dell'autorizzazione privata per l'oggetto. Sono necessarie due ricerche delle autorizzazioni private dell'utente durante il controllo autorizzazione se l'oggetto dispone di autorizzazioni private ed è protetto da un elenco di autorizzazioni. La prima ricerca viene effettuata per le autorizzazioni private sull'oggetto; la seconda ricerca viene effettuata per le autorizzazioni private sull'elenco di autorizzazioni. Le due ricerche richiedono l'utilizzo delle risorse di sistema; pertanto, è possibile che vengano influenzate le prestazioni. Se si utilizza solo l'elenco di autorizzazioni, viene eseguita una sola ricerca. Inoltre, poiché viene utilizzata la memorizzazione in cache dell'autorizzazione con l'elenco di autorizzazioni, le prestazioni per il controllo autorizzazione non cambieranno anche se si effettua un controllo solo delle autorizzazioni private sull'oggetto.

Cancellazione di un elenco di autorizzazioni

È inoltre possibile desiderare di cancellare l'elenco di autorizzazioni creato.

Non è possibile cancellare un elenco di autorizzazioni se questo viene utilizzato per proteggere ogni oggetto. Utilizzare il comando DSPAUTLOBJ per elencare tutti gli oggetti protetti dall'elenco. Utilizzare il pannello Editazione autorizzazione oggetto, il comando CHGAUT (modifica autorizzazione) o il comando RVKOBJAUT (Revoca autorizzazione oggetto) per modificare l'autorizzazione di ciascun oggetto. Quando l'elenco di autorizzazioni non protegge più gli oggetti, utilizzare il comando DLTAUTL (Cancellazione elenco di autorizzazioni) per cancellarlo.

Controllo dell'autorizzazione da parte del sistema

Quando un utente tenta di eseguire un'operazione su un oggetto, il sistema verifica che l'utente dispone di un'autorizzazione adeguata per l'operazione.

Il sistema controlla innanzitutto l'autorizzazione al percorso della libreria o dell'indirizzario contenente l'oggetto. Se l'autorizzazione al percorso della libreria o dell'indirizzario è adeguato, il sistema controlla l'autorizzazione all'oggetto stesso. In caso di file di database, il controllo dell'autorizzazione viene eseguito all'apertura del file, non quando si esegue ogni singola operazione sul file.

Durante il processo di controllo dell'autorizzazione, quando si rileva l'autorizzazione (anche se non è adeguata all'operazione richiesta), il controllo dell'autorizzazione viene arrestato e l'accesso viene concesso o negato. La funzione dell'autorizzazione adottata rappresenta l'eccezione a questa regola. L'autorizzazione adottata può sovrascrivere ogni specifica (e inadeguata) autorizzazione rilevata. Consultare l'argomento "Oggetti che adottano l'autorizzazione del proprietario" a pagina 160 per ulteriori informazioni sull'autorizzazione adottata.

Il sistema verifica un'autorizzazione utente su un oggetto nel seguente ordine:

1. Autorizzazione oggetto - percorso rapido
2. Autorizzazione speciale *ALLOBJ dell'utente
3. Autorizzazione specifica utente sull'oggetto
4. Autorizzazione utente sull'elenco di autorizzazioni di protezione dell'oggetto
5. Autorizzazione speciale *ALLOBJ gruppi
6. Autorizzazione gruppi sull'oggetto
7. Autorizzazione gruppi sull'elenco di autorizzazioni di protezione dell'oggetto
8. Autorizzazione pubblica specificata per l'oggetto o per l'elenco di autorizzazioni che protegge l'oggetto
9. Autorizzazione proprietario programma, se si utilizza l'autorizzazione adottata

Nota: le autorizzazioni provenienti da uno o più dei gruppi utente possono essere accumulate per garantire un'autorizzazione sufficiente per l'oggetto a cui è necessario accedere.

Diagrammi di flusso controllo autorizzazione

Questa sezione introduce i diagrammi di flusso, le descrizioni e gli esempi del controllo dell'autorizzazione.

Utilizzarli per rispondere a domande specifiche sul funzionamento o la diagnosi di problemi, da parte di un particolare schema di autorizzazioni con le proprie definizioni delle autorizzazioni. I grafici inoltre evidenziano i tipi di autorizzazione che hanno il maggiore effetto sulle prestazioni.

Il processo di controllo dell'autorizzazione è diviso in un diagramma di flusso principale e diversi diagrammi di flusso minori che mostrano passi specifici del processo. A seconda della combinazione delle autorizzazioni per un oggetto, i passi in alcuni diagrammi di flusso potrebbero venire ripetuti diverse volte.

I numeri nella parte superiore delle immagini dei diagrammi di flusso vengono utilizzati negli esempi successivi ai diagrammi.

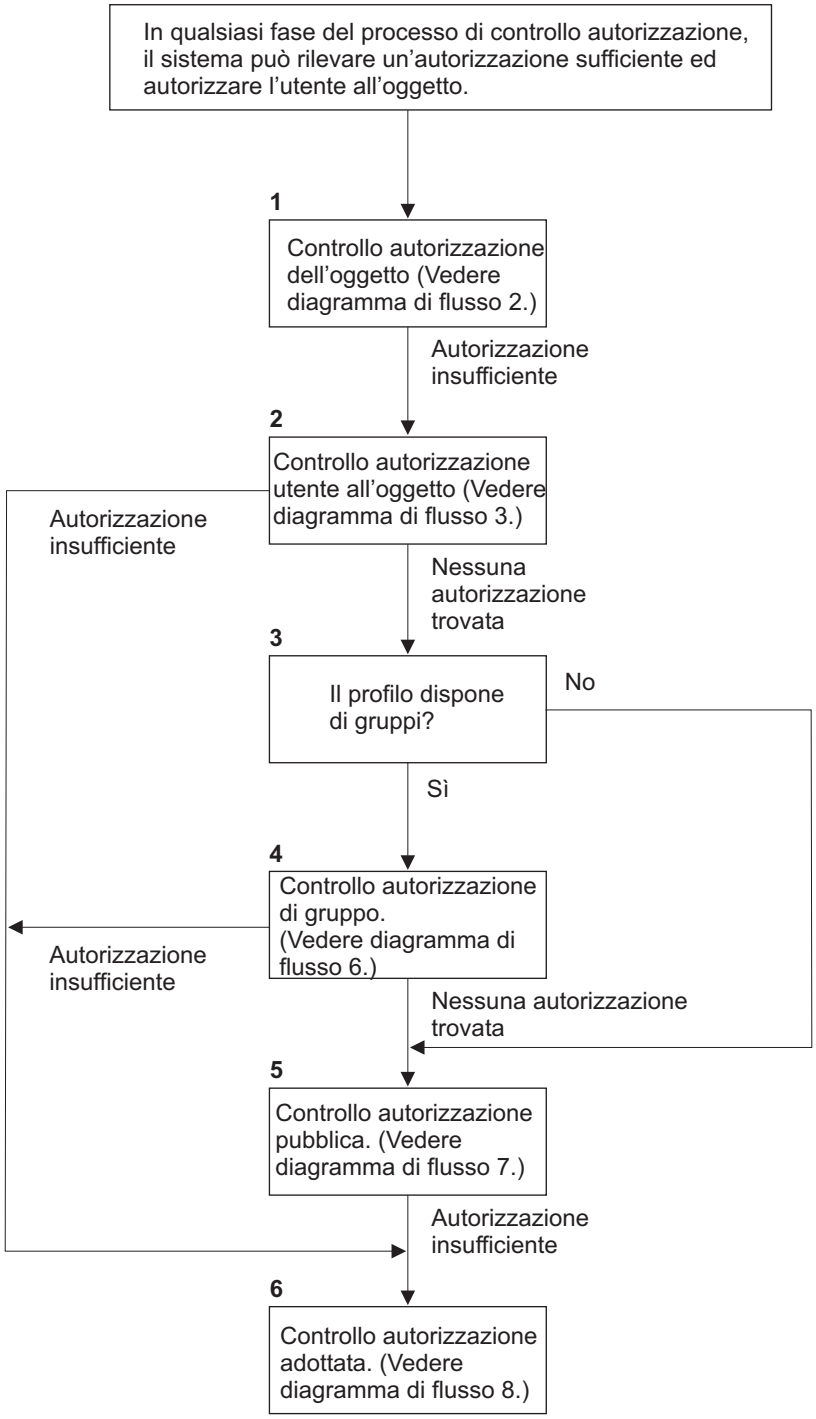
Vengono evidenziati i passi che rappresentano la ricerca delle autorizzazioni private di un profilo:

- Passo 6 nella Figura 13 a pagina 187
- Passo 6 nella Figura 16 a pagina 193
- Passo 2 nella Figura 19 a pagina 198

Ripetendo questi passi è probabile che si verifichino dei problemi nelle prestazioni durante il processo di controllo dell'autorizzazione.

Diagramma di flusso 1: Processo di controllo dell'autorizzazione principale

I passi nel diagramma di flusso 1 mostrano il processo principale seguito dal sistema durante il controllo dell'autorizzazione per un oggetto.



Se l'utente non è autorizzato, può verificarsi uno o più casi tra quelli riportati di seguito:
1) Viene inviato un messaggio all'utente o al programma; 2) Il programma ha esito negativo;
3) Nel giornale di verifica viene scritta una voce AF.

RBAFW508-0

Figura 11. Diagramma di flusso 1: Processo di controllo dell'autorizzazione principale

Descrizione del diagramma di flusso 1: Processo di controllo dell'autorizzazione principale.

Nota: in ogni passo del processo di controllo dell'autorizzazione, il sistema potrebbe rilevare autorizzazioni sufficienti e autorizzare l'utente sull'oggetto.

1. Il sistema controlla l'autorizzazione dell'oggetto. (Consultare il diagramma di flusso 2: Percorso rapido per il controllo dell'autorizzazione dell'oggetto.) Se il sistema rileva che quell'autorizzazione non è sufficiente, passa direttamente al Passo 2.
2. Il sistema controlla l'autorizzazione dell'utente sull'oggetto. (Consultare il diagramma di flusso 3: Come viene controllata l'autorizzazione utente su un oggetto.) Se il sistema determina che l'utente non dispone dell'autorizzazione sull'oggetto, passa direttamente al Passo 3. Se il sistema rileva che quell'autorizzazione utente non è sufficiente, passa direttamente al Passo 6.
3. Il sistema controlla se il profilo utente appartiene a ciascun gruppo. In caso affermativo, il sistema procede al Passo 4. In caso contrario, il sistema procede al Passo 5.
4. Il sistema determina l'autorizzazione del gruppo. (Consultare il Diagramma di flusso 6). Se il sistema determina che non esiste alcuna autorizzazione di gruppo all'oggetto, passa al Passo 5. Se il sistema determina che l'autorizzazione di gruppo all'oggetto non è sufficiente, passa al Passo 6.
5. Il sistema controlla l'autorizzazione pubblica dell'oggetto. (Consultare il Diagramma di flusso 7.) Se il sistema determina che l'autorizzazione pubblica non è sufficiente, procede al Passo 6.
6. Il sistema controlla l'autorizzazione adottata dell'oggetto. (Consultare il Diagramma di flusso 8.)

Diagramma di flusso 2: Percorso rapido per il controllo dell'autorizzazione dell'oggetto

I passi nel Diagramma di flusso 2 vengono eseguiti utilizzando le informazioni memorizzate con l'oggetto. Questo è il metodo più veloce per l'autorizzazione di un utente su un oggetto.

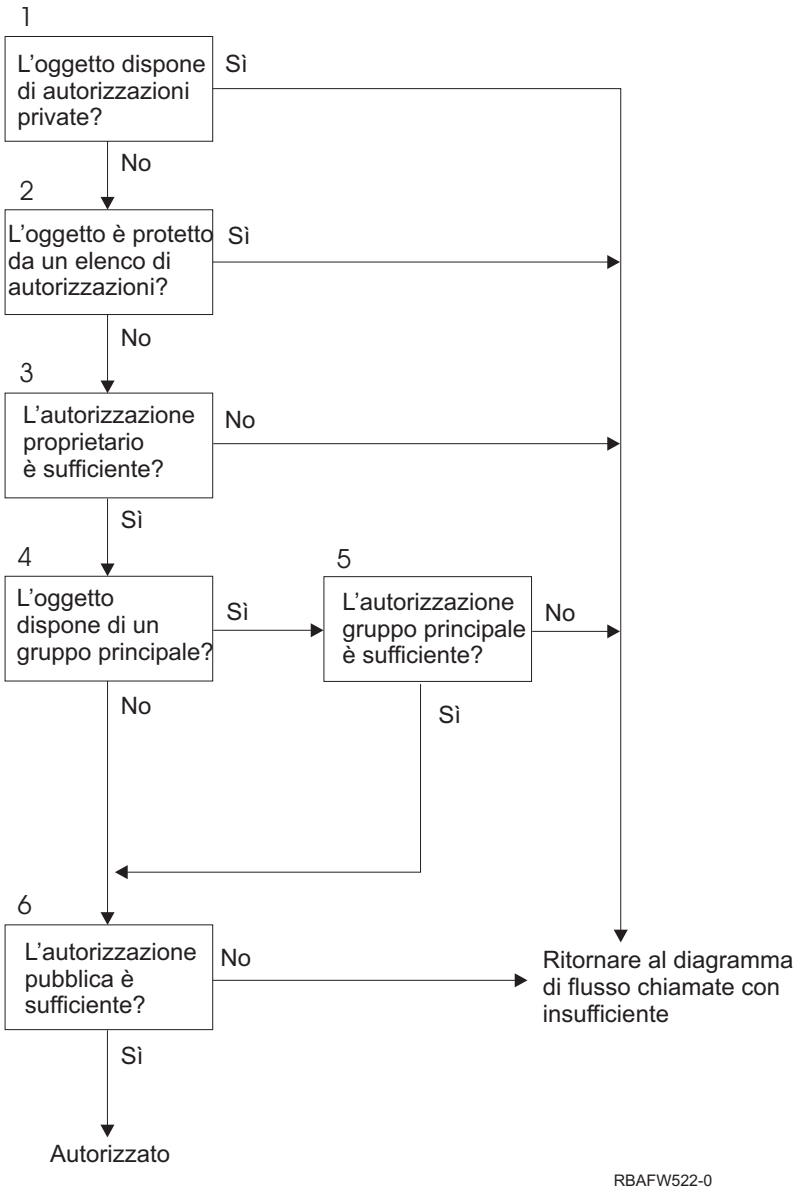


Figura 12. Diagramma di flusso 2: Percorso rapido per l'autorizzazione dell'oggetto

Descrizione Diagramma di flusso 2: Percorso rapido per l'autorizzazione dell'oggetto

1. Il sistema determina se l'oggetto dispone di autorizzazioni private. In caso affermativo, il sistema ritorna al diagramma di flusso chiamante con autorizzazioni insufficienti. In caso contrario, il sistema procede al Passo 2.
2. Il sistema determina se l'oggetto è protetto da un elenco di autorizzazioni. In caso affermativo, il sistema ritorna al diagramma di flusso chiamante con autorizzazioni insufficienti. In caso contrario, il sistema procede al Passo 3.
3. Il sistema determina se il proprietario dell'oggetto dispone di autorizzazioni sufficienti. In caso negativo, il sistema ritorna al diagramma di flusso chiamante con autorizzazioni insufficienti. In caso affermativo, il sistema passa alla Fase 4.
4. Il sistema determina se l'oggetto dispone di un gruppo principale. In caso affermativo, il sistema procede al Passo 5. In caso contrario, il sistema procede al Passo 6.
5. Il sistema determina se il gruppo principale dell'oggetto dispone di autorizzazioni sufficienti. In caso affermativo, il sistema procede al Passo 6. In caso negativo, il sistema ritorna al diagramma di flusso chiamante con autorizzazioni insufficienti.

6. Il sistema determina se l'autorizzazione pubblica è sufficiente o meno. In caso affermativo, l'oggetto viene autorizzato. In caso negativo, il sistema ritorna al diagramma di flusso chiamante con autorizzazioni insufficienti.

Diagramma di flusso 3: Come viene controllata l'autorizzazione utente su un oggetto

I passi contenuti nel diagramma di flusso 3 vengono eseguiti per il profilo utente individuale.

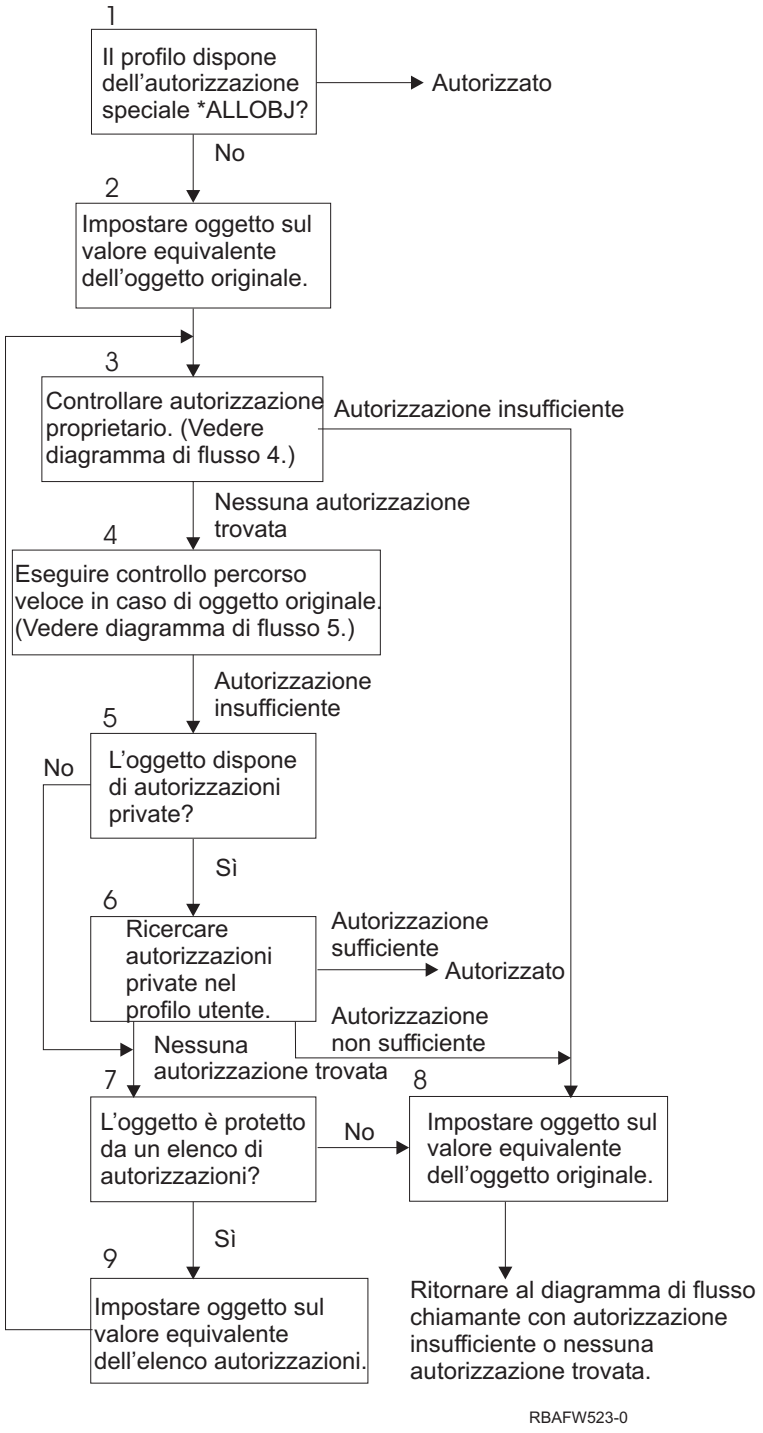


Figura 13. Diagramma di flusso 3: Controllo autorizzazione utente

Descrizione del diagramma di flusso 3: Controllo autorizzazione utente

1. Il sistema determina se il profilo utente dispone dell'autorizzazione *ALLOBJ. Se il profilo dispone dell'autorizzazione *ALLOBJ, il profilo viene autorizzato. Qualora non disponesse dell'autorizzazione *ALLOBJ, il controllo dell'autorizzazione procede al Passo 2.
2. Il sistema imposta l'autorizzazione dell'oggetto sul valore equivalente dell'oggetto originale. Il controllo dell'autorizzazione procede al Passo 3.
3. Il sistema controlla l'autorizzazione del proprietario. Se l'autorizzazione non è sufficiente, continua con il Passo 8. Nel caso in cui non venga trovata alcuna autorizzazione, continua con il Passo 4.
4. Il sistema completa il controllo dell'autorizzazione del percorso rapido dell'oggetto originale. (Consultare il Diagramma di flusso 5). Se l'autorizzazione non è sufficiente, il controllo dell'autorizzazione procede al Passo 5.
5. Il sistema determina se l'oggetto dispone delle autorizzazioni private. In caso affermativo, il controllo dell'autorizzazione procede al Passo 6. Qualora non fossero disponibili autorizzazioni private, il controllo dell'autorizzazione procede al Passo 7.
6. Il sistema controlla le autorizzazioni private con il profilo utente. Se l'autorizzazione è sufficiente, l'utente viene autorizzato. Se l'autorizzazione non è sufficiente, il controllo dell'autorizzazione procede al Passo 8. Qualora non si rilevassero delle autorizzazione, il controllo delle autorizzazioni procede al Passo 7.
7. Il sistema determina se l'oggetto è protetto o meno da un elenco di autorizzazioni. Qualora non fosse protetto, il controllo dell'autorizzazione procede al Passo 8. Nel caso in cui fosse protetto da un elenco di autorizzazioni, il controllo delle autorizzazioni procede al Passo 9.
8. Il sistema imposta l'oggetto affinché sia uguale all'oggetto originale e ritorna al diagramma di flusso con un'autorizzazione insufficiente o senza alcuna autorizzazione rilevata.
9. Il sistema imposta l'oggetto affinché sia uguale all'elenco di autorizzazioni e ritorna al Passo 3.

Diagramma di flusso 4: Come controllare l'autorizzazione del proprietario

Il diagramma di flusso 4 mostra il processo per il controllo dell'autorizzazione del proprietario. Il nome del profilo utente e l'autorizzazione del proprietario su un oggetto vengono memorizzati con l'oggetto.

Esistono diverse possibilità di utilizzo dell'autorizzazione proprietario per poter accedere ad un oggetto:

- Il profilo utente possiede l'oggetto.
- Il profilo utente possiede l'elenco di autorizzazioni.
- Il profilo gruppo utente possiede l'oggetto.
- Il profilo gruppo utente possiede l'elenco di autorizzazioni.
- Si utilizza l'autorizzazione adottata e il proprietario del programma possiede l'oggetto.
- Si utilizza l'autorizzazione adottata e il proprietario del programma possiede l'elenco di autorizzazioni.

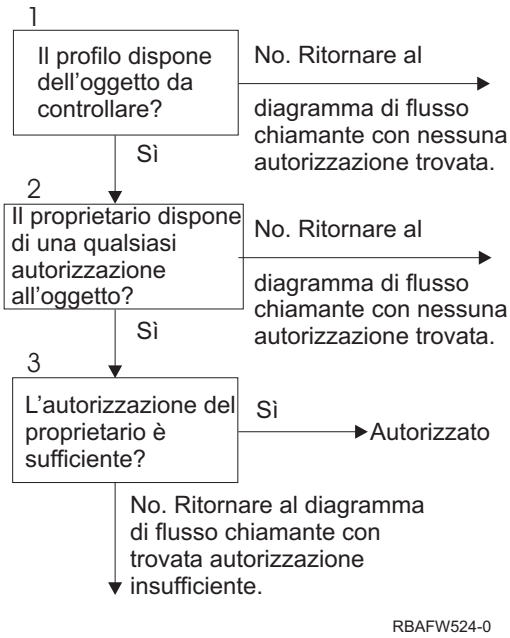


Figura 14. Diagramma di flusso 4: Controllo autorizzazione proprietario

Descrizione del diagramma di flusso 4: Controllo autorizzazione proprietario

1. Il sistema determina se il profilo utente possiede l'oggetto controllato. Se il profilo utente non possiede l'oggetto, allora procede al Passo 2. Se il profilo utente non possiede l'oggetto, il sistema ritorna al diagramma di flusso chiamante senza alcuna autorizzazione trovata.
2. Se il profilo utente non possiede l'oggetto, il sistema determina se il se il proprietario dispone dell'autorizzazione all'oggetto. Se i proprietario dispone dell'autorizzazione sull'oggetto, allora il controllo dell'autorizzazione procede al Passo 3. Se il sistema stabilisce che il proprietario non dispone dell'autorizzazione sull'oggetto, il sistema ritorna al diagramma di flusso chiamante senza alcuna autorizzazione rilevata.
3. Se il proprietario non dispone dell'autorizzazione sull'oggetto, il sistema stabilisce se questa autorizzazione è sufficiente per accedere all'oggetto. Se l'autorizzazione è sufficiente, il proprietario viene autorizzato all'oggetto. Qualora non fosse sufficiente, il sistema ritorna al diagramma di flusso con l'autorizzazione insufficiente rilevata.

Diagramma di flusso 5: Percorso rapido per il controllo dell'autorizzazione utente

Il diagramma di flusso 5 mostra il percorso rapido per la verifica dell'autorizzazione utente senza effettuare le ricerche nelle autorizzazioni private.

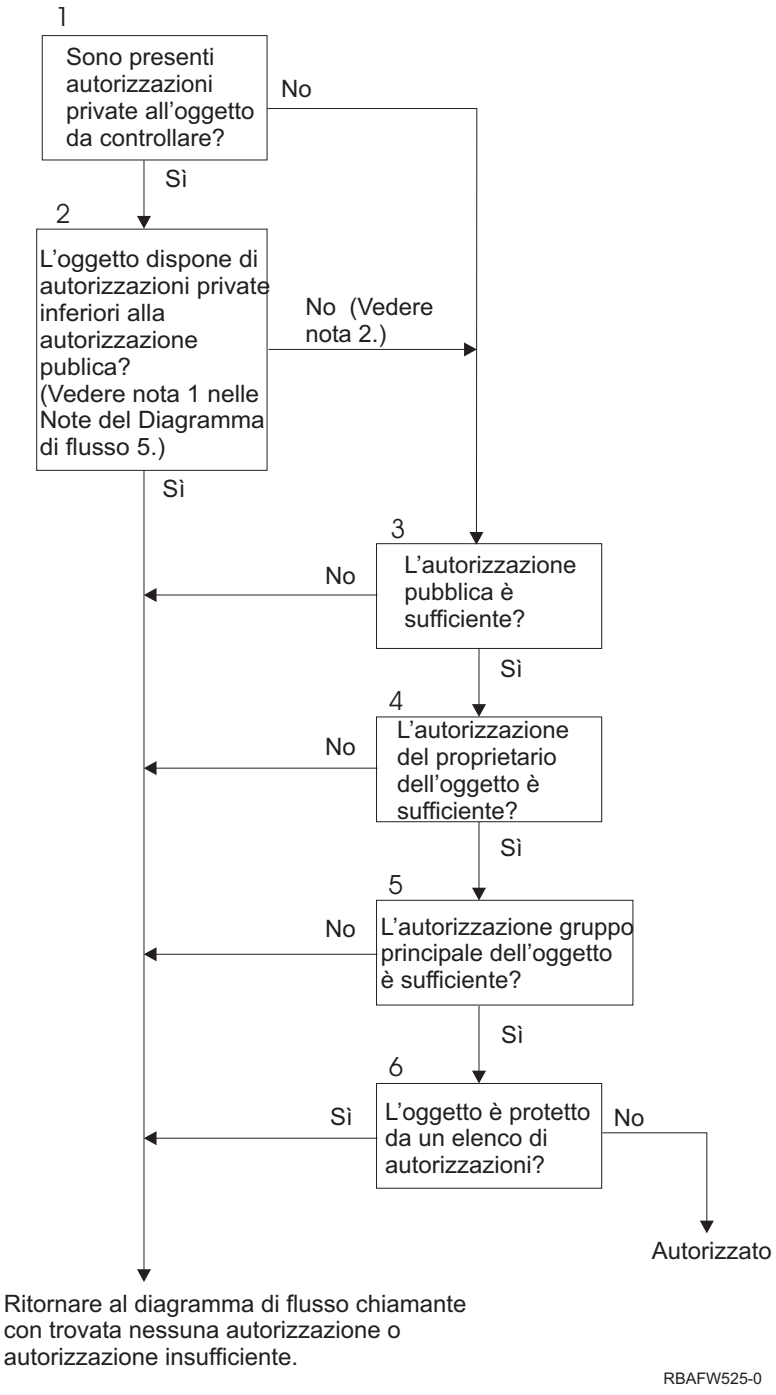


Figura 15. Diagramma di flusso 5: Percorso rapido per l'autorizzazione utente

Note diagramma di flusso 5:

1. L'autorizzazione viene considerata inferiore alla pubblica se ogni autorizzazione presente per *PUBLIC non è presente per un altro utente. Nell'esempio riportato nella Tabella 121 a pagina 191, il pubblico dispone delle autorizzazioni *OBJOPR, *READ e *EXECUTE sull'oggetto. WILSONJ dispone dell'autorizzazione *EXCLUDE e non dispone di alcuna delle autorizzazioni di cui dispone invece il pubblico. Per questo motivo, questo oggetto dispone di un'autorizzazione inferiore all'autorizzazione pubblica. (Anche OWNAR dispone di un'autorizzazione inferiore rispetto al pubblico ma l'autorizzazione del proprietario non viene considerata come autorizzazione privata.)

Tabella 121. Autorizzazione Pubblica e Privata

Autorizzazione	Gli utenti			
	OWNAR	**DPTMG**	**WILSONJ**	***PUBLIC**
Autorizzazioni oggetto:				
*OBJOPR		X		X
*OBJMGT	X			
*OBJEXIST				
*OBJALTER				
*OBJREF				
Autorizzazioni dati				
*READ		X		X
*ADD		X		
*UPD		X		
*DLT		X		
*EXECUTE		X		X
*EXCLUDE			X	

2. Questo percorso fornisce un metodo per l'utilizzo dell'autorizzazione pubblica, se possibile, anche se l'autorizzazione privata esiste per un oggetto. Il sistema si accerta che, in seguito, il processo di controllo dell'autorizzazione non neghi l'accesso all'oggetto per alcun motivo. Se il risultato di questa verifica è *Sufficiente*, è possibile evitare la ricerca nelle autorizzazioni private.

Descrizione Diagramma di flusso 5: Percorso rapido per l'autorizzazione utente

Questo diagramma di flusso mostra il percorso rapido per la verifica dell'autorizzazione utente senza effettuare le ricerche nelle autorizzazioni private.

1. Il sistema stabilisce l'eventuale presenza di autorizzazioni private sull'oggetto che si sta controllando. In caso di autorizzazioni private sull'oggetto, il controllo dell'autorizzazione procede al Passo 2. Qualora non fossero disponibili autorizzazioni private, il controllo dell'autorizzazione procede al Passo 3.
2. Se sono presenti delle autorizzazioni private, il sistema stabilisce se l'oggetto presenta delle autorizzazioni private inferiori all'autorizzazione pubblica. (Consultare nota 1.) Se l'oggetto dispone di autorizzazioni private inferiori all'autorizzazione pubblica, il sistema ritorna al diagramma di flusso chiamante senza autorizzazione o con un'autorizzazione insufficiente rilevata. Se l'oggetto non dispone delle autorizzazioni private inferiori all'autorizzazione pubblica, (Consultare nota 2), il controllo dell'autorizzazione procede al Passo 3.
3. Se l'oggetto non dispone di autorizzazioni private o se l'oggetto non dispone delle autorizzazioni private inferiori all'autorizzazione pubblica, il sistema stabilisce se l'autorizzazione pubblica è sufficiente. Se l'autorizzazione pubblica è sufficiente, il controllo dell'autorizzazione procede al Passo 4. Se l'autorizzazione pubblica non è sufficiente, il sistema ritorna al diagramma di flusso chiamante senza autorizzazione o con un'autorizzazione insufficiente rilevata.
4. Se l'autorizzazione pubblica è sufficiente, il sistema determina se l'autorizzazione del proprietario dell'oggetto è sufficiente o meno. Se l'autorizzazione del proprietario dell'oggetto è sufficiente, la verifica delle autorizzazioni procede al Passo 5. Se l'autorizzazione del proprietario dell'oggetto non è sufficiente, il sistema ritorna al diagramma di flusso chiamante senza autorizzazioni o con un'autorizzazione insufficiente rilevata.
5. Se l'autorizzazione del proprietario dell'oggetto è sufficiente, il sistema stabilisce se l'autorizzazione del gruppo principale dell'oggetto è sufficiente o meno. Se l'autorizzazione del gruppo principale dell'oggetto è sufficiente, il controllo dell'autorizzazione procede al Passo 6. Se l'autorizzazione del

gruppo principale dell'oggetto non è sufficiente, il sistema ritorna al diagramma di flusso chiamante senza autorizzazione o con un'autorizzazione insufficiente rilevata.

6. Se l'autorizzazione del gruppo principale dell'oggetto è sufficiente, il sistema stabilisce se l'oggetto è protetto o meno da un elenco di autorizzazioni. Se l'oggetto è protetto da un elenco di autorizzazioni, il sistema ritorna al diagramma di flusso chiamante senza autorizzazione o con un'autorizzazione insufficiente rilevata. Se l'oggetto non è protetto da un elenco di autorizzazioni, l'utente è autorizzato all'oggetto.

Diagramma di flusso 6: come controllare l'autorizzazione gruppo

Un utente può essere un membro di 16 gruppi, al massimo. Un gruppo può disporre dell'autorizzazione privata su un oggetto oppure può essere il gruppo principale per un oggetto.

le autorizzazioni provenienti da uno o più dei gruppi utente possono essere accumulate per garantire un'autorizzazione sufficiente per l'oggetto a cui è necessario accedere. Ad esempio, WAGNERB necessita dell'autorizzazione *CHANGE sul file CRLIM. L'autorizzazione *CHANGE comprende *OBJOPR, *READ, *ADD, *UPD, *DLT e *EXECUTE. La Tabella 122 mostra le autorizzazioni per il file CRLIM:

Tabella 122. Autorizzazioni gruppi accumulate

	Gli utenti			
Autorizzazione	**OWNAR**	**DPT506**	**DPT702**	***PUBLIC**
Autorizzazioni oggetto:				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
Autorizzazioni dati				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X	X	
*DLT	X		X	
*EXECUTE	X	X	X	
*EXCLUDE				X

WAGNERB necessita sia di DPT506 che di DPT702 per ottenere un'autorizzazione sufficiente sul file CRLIM. DPT506 non dispone dell'autorizzazione *DLT, mentre DPT702 non dispone dell'autorizzazione *ADD.

Il Diagramma di flusso 6 (Figura 16 a pagina 193) mostra le fasi di controllo dell'autorizzazione di gruppo.

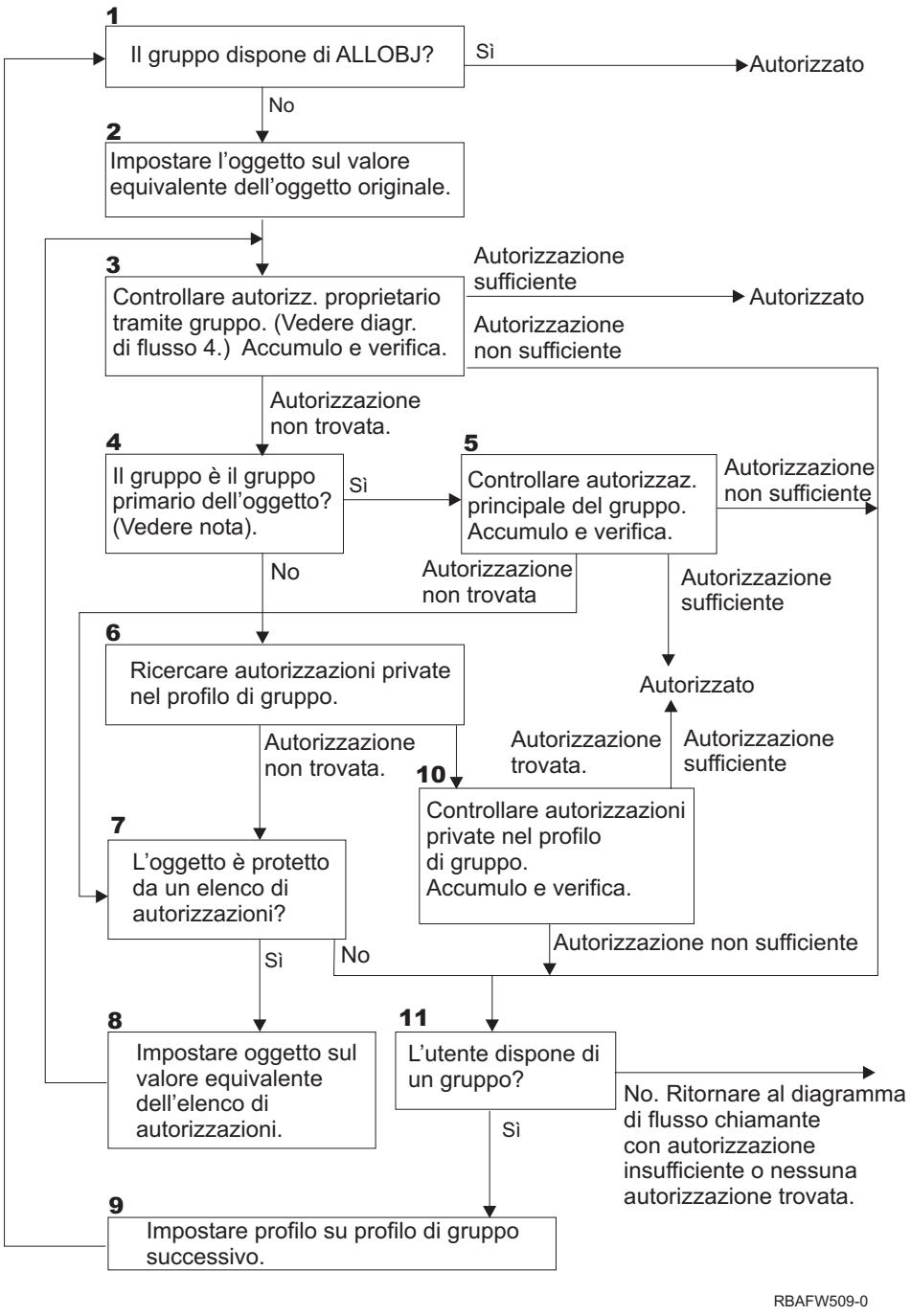


Figura 16. Il Diagramma di flusso 6: Controllo autorizzazione gruppo

Nota: se l'utente viene collegato come il profilo che rappresenta il gruppo principale per un oggetto, l'utente non può ricevere l'autorizzazione sull'oggetto mediante il gruppo principale.

Descrizione del Diagramma di flusso 6: Controllo autorizzazione gruppo

1. Il sistema determina se il gruppo dispone dell'autorizzazione *ALLOBJ. In caso affermativo, il gruppo viene autorizzato. In caso contrario, il controllo dell'autorizzazione procede al Passo 2.
2. Il gruppo non dispone dell'autorizzazione *ALLOBJ, quindi il sistema imposta l'oggetto che viene controllato in modo che sia uguale all'oggetto originale.
3. Una volta che il sistema imposta l'oggetto sul valore originale, viene controllata l'autorizzazione del proprietario. (Consultare Diagramma di flusso 4) Se l'autorizzazione è sufficiente, il gruppo viene

autorizzato. Se l'autorizzazione non è sufficiente, il controllo dell'autorizzazione procede al Passo 11. Se non si rileva l'autorizzazione, il controllo dell'autorizzazione procede al Passo 4.

4. Se non si rileva l'autorizzazione del proprietario, il sistema controlla se il gruppo è il gruppo principale dell'oggetto.

   Nota: se l'utente viene collegato come il profilo che rappresenta il gruppo principale per un oggetto, l'utente non può ricevere l'autorizzazione sull'oggetto mediante il gruppo principale.

   Se il gruppo è il gruppo principale dell'oggetto, il controllo dell'autorizzazione procede al Passo 5. Se il gruppo non è il gruppo principale dell'oggetto, il controllo dell'autorizzazione procede al Passo 6.
5. Il gruppo è il gruppo principale dell'oggetto, quindi, il sistema controlla e verifica l'autorizzazione del gruppo principale. Se l'autorizzazione del gruppo principale è sufficiente, il gruppo viene autorizzato. Se l'autorizzazione del gruppo principale non viene rilevata, il controllo dell'autorizzazione procede al Passo 7. Se l'autorizzazione del gruppo principale non è sufficiente, il controllo dell'autorizzazione procede al Passo 11
6. Il gruppo non è il gruppo principale dell'oggetto, quindi il sistema controlla le autorizzazioni private nel profilo di gruppo. Se si rileva l'autorizzazione, il controllo dell'autorizzazione procede al Passo 10. Se non si rileva l'autorizzazione, il controllo dell'autorizzazione procede al Passo 7.
7. Non si rileva alcuna autorizzazione per le autorizzazioni private per il profilo gruppo, quindi il sistema controlla se l'oggetto è protetto o meno da un elenco di autorizzazioni. Se l'oggetto è protetto da un elenco di autorizzazioni, il controllo dell'autorizzazione procede al Passo 8. Se l'oggetto invece non è protetto da un elenco di autorizzazioni, il controllo dell'autorizzazione procede al Passo 11.
8. L'oggetto è protetto da un elenco di autorizzazioni, quindi il sistema imposta l'oggetto in modo tale che venga controllato come l'elenco di autorizzazioni e il controllo dell'autorizzazione ritorna al Passo 3.
9. L'utente appartiene ad un altro profilo gruppo, quindi il sistema imposta questo profilo sul profilo gruppo successivo e ritorna al Passo 1 per avviare nuovamente il processo di controllo dell'autorizzazione.
10. L'autorizzazione viene rilevata per le autorizzazioni private all'interno del profilo gruppo, quindi, le autorizzazioni private vengono controllate e verificate nel profilo gruppo. Se le autorizzazioni sono sufficienti, il profilo gruppo viene autorizzato. Se non è sufficiente, il controllo dell'autorizzazione procede al Passo 11.
11. Autorizzazione non rilevata o insufficiente quindi il sistema controlla se gli utenti sono associati ad un altro profilo gruppo. Se l'utente appartiene ad un altro profilo gruppo, il sistema ritorna al Passo 9. Se l'utente non appartiene ad un altro profilo gruppo, il sistema ritorna al diagramma di flusso chiamante con un'autorizzazione insufficiente o senza alcuna autorizzazione.

Diagramma di flusso 7: Come viene controllata l'autorizzazione pubblica

Quando si controlla l'autorizzazione pubblica, il sistema deve stabilire se utilizzare o meno l'autorizzazione pubblica per l'oggetto o per l'elenco di autorizzazioni.

Il diagramma di flusso 7 mostra il processo:

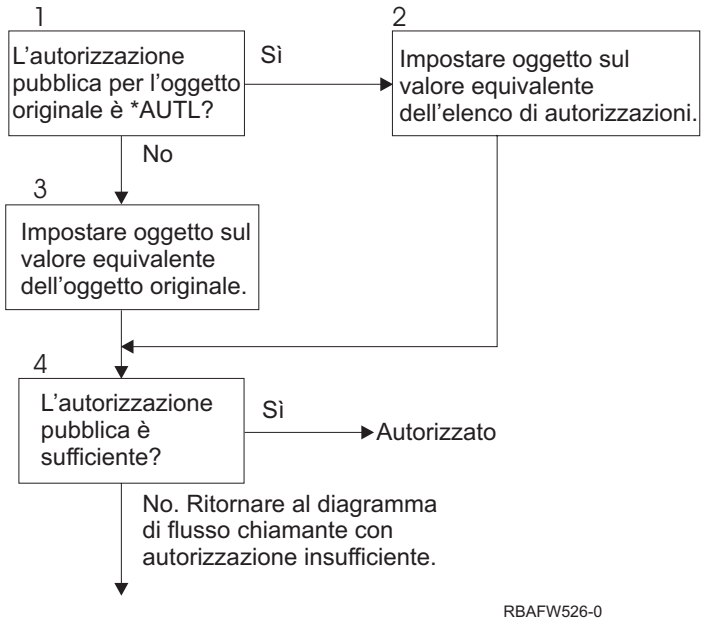


Figura 17. Diagramma di flusso 7: Controllo dell'autorizzazione pubblica

Descrizione del diagramma di flusso 7: Controllo dell'autorizzazione pubblica.

Il diagramma di flusso 7 mostra come il sistema deve stabilire se utilizzare o meno l'autorizzazione pubblica per l'oggetto o l'elenco di autorizzazioni.

1. Il sistema stabilisce se l'autorizzazione pubblica per l'oggetto originale è *AUTL. Se l'autorizzazione pubblica per l'oggetto originale è *AUTL, il sistema procede al Passo 2. Se l'autorizzazione pubblica per l'oggetto originale non è *AUTL, il sistema procede al Passo 3.
2. Se l'autorizzazione pubblica per l'oggetto originale è *AUTL, il sistema imposta l'oggetto controllato in modo uguale all'elenco di autorizzazioni e procede al Passo 4.
3. Se l'autorizzazione pubblica per l'oggetto originale non è *AUTL, il sistema imposta l'oggetto controllato sull'oggetto originale e procede al Passo 4.
4. Se l'oggetto controllato è stato impostato in modo uguale all'elenco di autorizzazioni o all'oggetto originale, il sistema stabilisce se l'autorizzazione pubblica è sufficiente. Se l'autorizzazione pubblica è sufficiente, l'utente viene autorizzato sull'oggetto. Se l'autorizzazione pubblica non è sufficiente, il sistema ritorna al diagramma di flusso chiamante con autorizzazione insufficiente.

Diagramma di flusso 8: come controllare l'autorizzazione adottata

Se si rileva un'autorizzazione insufficiente durante il controllo dell'autorizzazione utente, il sistema controlla l'autorizzazione adottata.

Il sistema potrebbe utilizzare l'autorizzazione adottata dal programma originale richiamato dall'utente o dai programmi precedenti nello stack di chiamata. Per fornire le prestazioni migliori e ridurre la frequenza con la quale si effettuano le ricerche nelle autorizzazioni private, il processo di controllo dell'autorizzazione adottata verifica se il proprietario del programma dispone dell'autorizzazione speciale *ALLOBJ o se possiede l'oggetto controllato. Questa operazione viene ripetuta per ogni programma nello stack che utilizza l'autorizzazione privata.

Se non si rileva l'autorizzazione sufficiente, il sistema controlla se il proprietario del programma dispone dell'autorizzazione privata per l'oggetto controllato. Questa operazione viene ripetuta per ogni programma nello stack che utilizza l'autorizzazione privata.

La Figura 18 a pagina 196 e la Figura 19 a pagina 198 mostrano il processo per il controllo dell'autorizzazione adottata.

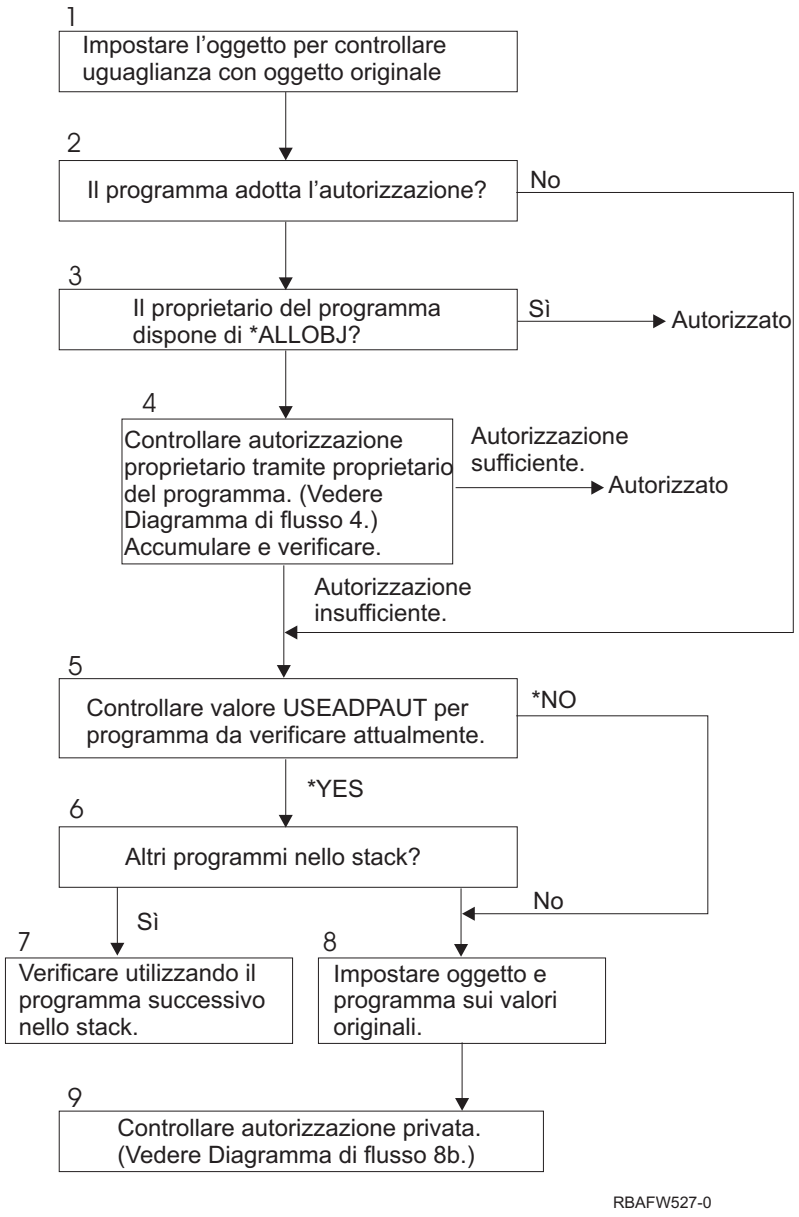


*Figura 18. Diagramma di flusso 8A: controllo utente *ALLOBJ autorizzazione adottata e proprietario*

Descrizione del diagramma di flusso 8A: controllo utente *ALLOBJ autorizzazione adottata e proprietario

Il diagramma di flusso 8A descrive il modo in cui il sistema controlla l'autorizzazione adottata quando si rileva un'autorizzazione insufficiente durante il controllo dell'autorizzazione utente.

1. Il sistema imposta l'oggetto controllato sull'oggetto originale e procede al Passo 2.
2. Il sistema stabilisce se il programma adotta l'autorizzazione. Se il programma adotta l'autorizzazione, il controllo dell'autorizzazione procede al Passo 3. Se il programma non adotta l'autorizzazione e l'autorizzazione non è sufficiente, il controllo dell'autorizzazione procede al Passo 5.
3. Se il programma non adotta l'autorizzazione, il sistema determina se il proprietario del programma dispone dell'autorizzazione *ALLOBJ. Se il proprietario dell'autorizzazione dispone dell'autorizzazione *ALLOBJ, l'utente viene autorizzato. Se il proprietario del programma non dispone dell'autorizzazione *ALLOBJ, il controllo dell'autorizzazione procede al Passo 4.

4. Se il proprietario del programma non dispone dell'autorizzazione *ALLOBJ, il sistema controlla e verifica l'autorizzazione del proprietario. Se l'autorizzazione è sufficiente, l'utente viene autorizzato. Se l'autorizzazione non è sufficiente, il controllo dell'autorizzazione procede al Passo 5.
5. Il sistema controlla il valore USEADPAUT per il programma attualmente in fase di verifica. Se il valore è uguale a *NO, il controllo dell'autorizzazione procede al Passo 6. Se il valore è uguale a *YES, il controllo dell'autorizzazione procede al Passo 6.
6. Se il valore USEADPAUT è uguale a *YES, il sistema determina se sono presenti altri programmi in attesa nello stack. In questo caso, il controllo dell'autorizzazione procede al Passo 7. Qualora non fossero presenti altri programmi in attesa nello stack, il controllo dell'autorizzazione procede al Passo 8.
7. Verificare utilizzando il programma successivo nello stack e ritornare al Passo 2.
8. Se non fossero presenti altri programmi nello stack o il valore USEADPAUT è uguale a *NO, il sistema imposta l'oggetto e il programma sui valori originali e procede al Passo 9.
9. Il sistema controlla l'autorizzazione privata. Questa fase è spiegata in Diagramma di flusso 8B: Controllo dell'autorizzazione adottata utilizzando le autorizzazioni private.

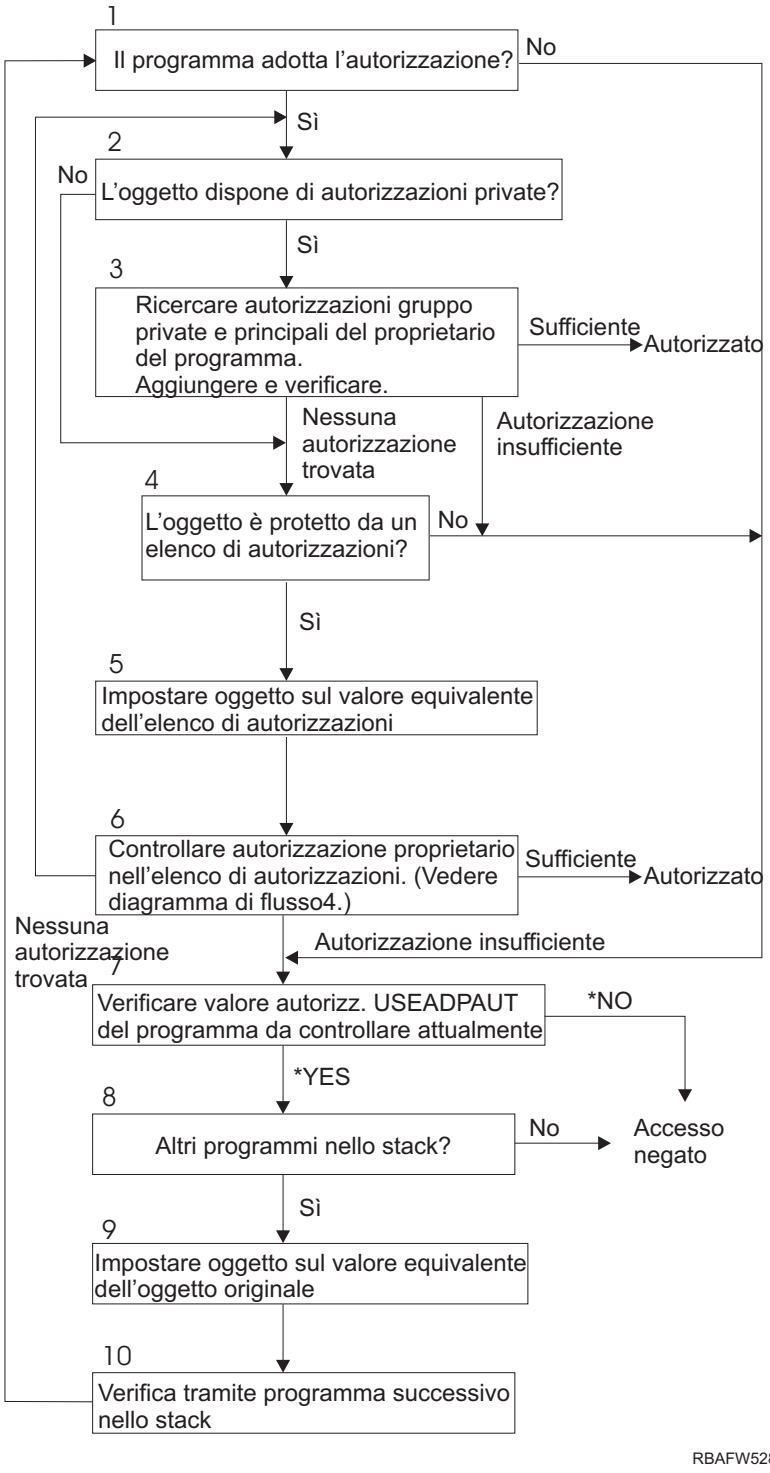


Figura 19. Diagramma di flusso 8B: controllo dell'autorizzazione adottata utilizzando le autorizzazioni private

Descrizione del diagramma di flusso 8B: controllo dell'autorizzazione adottata utilizzando le autorizzazioni private

1. Il sistema stabilisce se il programma può adottare o meno l'autorizzazione. In caso affermativo, procedere al Passo 2. In caso negativo, procedere al Passo 7.
2. Il sistema stabilisce se l'oggetto dispone o meno di autorizzazioni private. In caso affermativo, procedere al Passo 3. In caso negativo, procedere al Passo 4.

3. Il sistema controlla le autorizzazioni del gruppo principale e private per il proprietario del programma. Se l'autorizzazione è sufficiente, il programma viene autorizzato. Se si rileva un autorizzazione insufficiente, procedere al Passo 7. In caso contrario, procedere al Passo 4.
4. Il sistema determina se l'oggetto è protetto da un elenco di autorizzazioni. In caso affermativo, procedere al Passo 5. In caso negativo, procedere al Passo 7.
5. Il sistema imposta l'oggetto in modo che sia uguale all'elenco di autorizzazioni e procede quindi al Passo 6.
6. Il sistema controlla l'autorizzazione del proprietario sull'elenco di autorizzazioni. (Consultare il Diagramma di flusso 4). Se non si rileva alcuna autorizzazione, ritornare al Passo 2. Se invece si rilevano autorizzazioni sufficienti, il programma viene autorizzato.
7. Il sistema verifica il valore dell'autorizzazione USEADPAUT per il programma attualmente controllato. Se impostato su *YES, procedere al Passo 8. Se impostato su *NO, l'accesso viene negato.
8. Il sistema controlla l'eventuale presenza di altri programmi nello stack. In caso affermativo, precedere al Passo 9. In caso contrario, l'accesso viene negato.
9. Il sistema imposta l'oggetto in modo che sia uguale all'oggetto originale e procede al Passo 10.
10. Verificare utilizzando il programma successivo nello stack e ritornare al Passo 1.

Concetti correlati

"Come ignorare l'autorizzazione adottata" a pagina 249
La tecnica di utilizzare l'autorizzazione adottata nella struttura del menu richiede che l'utente ritorni al menu iniziale prima di eseguire delle query. Se si desidera sfruttare l'opportunità di avviare una query dai menu dell'applicazione e da un menu iniziale, è possibile impostare il programma QRYSTART per ignorare l'autorizzazione adottata.

Esempi di controllo autorizzazione

Questa sezione include diversi esempi di controllo autorizzazione.

Questi esempi dimostrano le fasi seguite dal sistema per stabilire se un utente è abilitato ad accedere ad un oggetto. Questi esempi sono stati concepiti per mostrare come funziona il controllo delle autorizzazioni e dove potrebbero verificarsi determinati problemi delle prestazioni.

La Figura 20 mostra le autorizzazioni per il file PRICES. Di seguito alla figura vengono riportati diversi esempi di accesso richiesto a questo file il processo di controllo delle autorizzazioni. Negli esempi, la ricerca delle autorizzazioni private (Diagramma di flusso 4, Passo 6) viene evidenziata in quanto parte del processo di controllo delle autorizzazioni che potrebbe causare dei problemi di prestazioni qualora venisse ripetuto diverse volte.

```
                        Visualizzazione autorizzazione oggetto

Oggetto . . . . . :   PRICES           Proprietario . . . . . :   OWNCP
  Libreria. . . . :   CONTRACTS       Gruppo principale  . . . :   *NONE
Tipo di oggetto. . :   *FILE     Unità ASP  . . . . . :   *SYSBAS

Oggetto protetto da elenco di autorizzazioni . . . . . . . . . . . . :   *NONE

                       Autorizzazione
Utente        Gruppo   oggetto
OWNCP                  *ALL
DPTSM                  *CHANGE
DPTMG                  *CHANGE
WILSONJ                *USE
*PUBLIC                *USE
```

Figura 20. Autorizzazione per il file PRICES

Caso 1: Utilizzo autorizzazione gruppo privata

Questo caso illustra come utilizzare l'autorizzazione gruppo privata.

L'utente ROSSM desidera accedere al file PRICES utilizzando il programma CPPGM01. CPPGM01 richiede l'autorizzazione *CHANGE al file. ROSSM è un membro del profilo gruppo DPTSM. Né ROSSM né DPTSM dispone dell'autorizzazione speciale *ALLOBJ. Il sistema esegue questi passi per stabilire se consentire o meno a ROSSM l'accesso al file PRICES:

1. Diagramma di flusso 1, passo 1.
   a. Diagramma di flusso 2, passo 1.
2. Diagramma di flusso 1, passo 2.
   a. Diagramma di flusso 3, passi 1 e 2. Oggetto da controllare = CONTRACTS/PRICES *FILE.
   b. Diagramma di flusso 3, passo 3.
      1) Diagramma di flusso 4, passo 1. Ritornare al Diagramma di flusso 3 senza alcuna autorizzazione rilevata. ROSSM non possiede il file PRICES.
   c. Diagramma di flusso 3, passo 4.
      1) Diagramma di flusso 5, passi 1, 2 e 3. L'autorizzazione pubblica non è sufficiente.
   d. Diagramma di flusso 3, passo 5.
   e. Diagramma di flusso 3, passo 6. ROSSM non dispone dell'autorizzazione privata al file PRICES.
   f. Diagramma di flusso 3, passi 7 e 8. Il file PRICES non è protetto da un elenco di autorizzazioni. Ritornare al Diagramma di flusso 1 senza alcuna autorizzazione rilevata.
3. Diagramma di flusso 1, passi 3 e 4. DPTSM è il profilo gruppo per ROSSM.
   a. Diagramma di flusso 6, passi 1, 2 e 3.
      1) Diagramma di flusso 4, passo 1. DPTSM non possiede il file PRICES.
   b. Diagramma di flusso 6, passo 4. DPTSM non è il gruppo principale per il file PRICES.
   c. Diagramma di flusso 6, passo 6. Autorizzato. (DPTSM dispone dell'autorizzazione *CHANGE).

Risultato:

ROSSM è autorizzato in quanto il profilo gruppo DPTSM dispone dell'autorizzazione *CHANGE.

Analisi:

Utilizzare l'autorizzazione gruppo in questo esempio rappresenta una buona soluzione per la gestione delle autorizzazioni. Riduce il numero delle autorizzazioni private sul sistema ed di facile comprensione e controllo. Tuttavia, l'utilizzo dell'autorizzazione gruppo privata in genere dà inizio a due ricerche di autorizzazioni private (per l'utente e per il gruppo), nel caso in cui l'autorizzazione pubblica non fosse adeguata. Una ricerca dell'autorizzazione privata può essere evitata, rendendo DPTSM il gruppo principale del file PRICES.

Caso 2: Utilizzo autorizzazione gruppo principale

Questo caso illustra come utilizzare l'autorizzazione gruppo principale.

ANDERSJ necessita dell'autorizzazione *CHANGE sul file CREDIT. ANDERSJ è un membro del gruppo DPTAR. Né ANDERSJ né DPTAR dispone dell'autorizzazione speciale *ALLOBJ. La Figura 21 a pagina 201 mostra le autorizzazioni per il file CREDIT.

```
                        Visualizzazione autorizzazione oggetto

Oggetto. . . . . :   CREDIT          Proprietario. . . . . :   OWNAR
  Libreria . . . . :   ACCTSRCV      Gruppo principale  . . . :   DPTAR
Tipo di oggetto. . :   *FILE     Unità ASP  . . . . . :   *SYSBAS

Oggetto protetto da elenco di autorizzazioni  . . . . . :   *NONE

                       Autorizzazione
Utente        Gruppo   oggetto
OWNAR                   *ALL
DPTAR                   *CHANGE
*PUBLIC                 *USE
```

Figura 21. Autorizzazione per il file CREDIT

Il sistema esegue questi passi per determinare se consentire ad ANDERSJ di disporre dell'accesso *CHANGE al file CREDIT:

1. Diagramma di flusso 1, passo 1.
   a. Diagramma di flusso 2, passo 1. L'autorizzazione DPTAR è un'autorizzazione gruppo principale, non un'autorizzazione privata.
   b. Diagramma di flusso 2, passi 2, 3, 4, 5 e 6. L'autorizzazione pubblica non è sufficiente.
2. Diagramma di flusso 1, passo 2.
   a. Diagramma di flusso 3, passi 1 e 2. Oggetto da controllare = ACCTSRCV/CREDIT *FILE.
   b. Diagramma di flusso 3, passo 3.
      1) Diagramma di flusso 4, passo 1. ANDERSJ non possiede il file CREDIT. Ritornare al Diagramma di flusso 3 senza alcuna autorizzazione rilevata.
   c. Diagramma di flusso 3, passo 4.
      1) Diagramma di flusso 5, passo 1. Il file CREDIT non dispone di autorizzazioni private.
      2) Diagramma di flusso 5, passo 3. L'autorizzazione pubblica non è sufficiente. Ritornare al Diagramma di flusso 3 senza alcuna autorizzazione rilevata.
   d. Diagramma di flusso 3, passi 5, 7 e 8. Il file CREDIT non è protetto da un elenco di autorizzazioni. Ritornare al Diagramma di flusso 1 senza alcuna autorizzazione rilevata.
3. Diagramma di flusso 1, passi 3 e 4. ANDERSJ è un membro del profilo gruppo DPTAR.
   a. Diagramma di flusso 6, passi 1 e 2. Oggetto da controllare = ACCTSRCV/CREDIT *FILE.
   b. Diagramma di flusso 6, passo 3.
      1) Diagramma di flusso 4, passo 1. DPTAR non possiede il file CREDIT. Ritornare al Diagramma di flusso 6 senza alcuna autorizzazione rilevata.
   c. Diagramma di flusso 6, passi 4 e 5. Autorizzato. DPTAR è il gruppo principale del file CREDIT e dispone dell'autorizzazione *CHANGE.

Risultato:

ANDERSJ viene autorizzato in quanto DPTAR è il gruppo principale del file CREDIT e dispone dell'autorizzazione *CHANGE.

Analisi:

Se si utilizza l'autorizzazione del gruppo principale, le prestazioni del controllo delle autorizzazioni risultano migliorate rispetto a quando si specifica l'autorizzazione privata per il gruppo. Questo esempio non richiede ricerche di autorizzazioni private.

Concetti correlati

"Considerazioni per gruppi principali per gli oggetti" a pagina 256
Qualsiasi oggetto sul sistema può disporre di un gruppo principale. L'autorizzazione del gruppo principale fornisce prestazioni migliori se il gruppo principale è il primo gruppo per molti utenti di un oggetto.

Caso 3: Utilizzo autorizzazione pubblica

Questo caso descrive la procedura per l'utilizzo dell'autorizzazione pubblica.

L'utente JONESP desidera accedere al file CREDIT utilizzando il programma CPPGM06. CPPGM06 richiede l'autorizzazione *USE al file. JONESP è un membro del profilo gruppo DPTSM e non dispone dell'autorizzazione speciale *ALLOBJ. Il sistema esegue questi passi per stabilire se consentire a JONESP l'accesso al file CREDIT:

Diagramma di flusso 1, passo 1.

1. Diagramma di flusso 2, passo 1. Il file CREDIT non dispone di autorizzazioni private. L'autorizzazione DPTAR è un'autorizzazione gruppo principale, non un'autorizzazione privata.
2. Diagramma di flusso 2, passi 2 e 3. L'autorizzazione del proprietario (OWNAR) è sufficiente.
3. Diagramma di flusso 2, passi 4 e 5. L'autorizzazione del gruppo principale (DPTAR) è sufficiente.
4. Diagramma di flusso 2, passo 6. Autorizzato. L'autorizzazione pubblica è sufficiente.

Analisi:

Questo esempio mostra il miglioramento delle prestazioni ottenuto quando si salta la definizione delle autorizzazioni private per un oggetto.

Caso 4: Utilizzo autorizzazione pubblica senza ricerca dell'autorizzazione privata

Questo caso descrive come utilizzare l'autorizzazione pubblica senza ricercare l'autorizzazione privata.

L'utente JONESP desidera accedere al file PRICES utilizzando il programma CPPGM06. CPPGM06 richiede l'autorizzazione *USE al file. JONESP è un membro del profilo gruppo DPTSM e non dispone dell'autorizzazione speciale *ALLOBJ. Il sistema esegue questi passi per stabilire se consentire a JONESP l'accesso al file PRICES:

1. Diagramma di flusso 1, passo 1.
   a. Diagramma di flusso 2, passo 1. Il file PRICES dispone di autorizzazioni private.
2. Diagramma di flusso 1, passo 2.
   a. Diagramma di flusso 3, passi 1 e 2. Oggetto da controllare = CONTRACTS/PRICES *FILE.
   b. Diagramma di flusso 3, passo 3.
      1) Diagramma di flusso 4, passo 1. JONESP non possiede il file PRICES. Ritornare al Diagramma di flusso 3 senza alcuna autorizzazione rilevata.
   c. Diagramma di flusso 3, passo 4.
      1) Diagramma di flusso 5, passi 1, 2 e 3. L'autorizzazione pubblica non è sufficiente.
      2) Diagramma di flusso 5, passo 4. L'autorizzazione del proprietario è sufficiente. (OWNCP dispone di *ALL.)
      3) Diagramma di flusso 5, passo 5. Il file PRICES non dispone di un gruppo principale.
      4) Diagramma di flusso 5, passo 6. Autorizzato. (Il file PRICES non è protetto da un elenco di autorizzazioni.)

Analisi:

Questo esempio mostra il miglioramento delle prestazioni ottenuto quando si salta la definizione delle autorizzazioni private per un oggetto, inferiori all'autorizzazione pubblica. Sebbene l'autorizzazione

privata esista per il file PRICES, l'autorizzazione pubblica è sufficiente per questa richiesta e può essere utilizzata senza la ricerca delle autorizzazioni private.

Caso 5: Utilizzo autorizzazione adottata

Questo caso dimostra il miglioramento delle prestazioni derivanti dall'utilizzo dell'autorizzazione adottata.

L'utente SMITHG desidera accedere al file PRICES utilizzando il programma CPPGM08. SMITHG non è un membro di un gruppo e non dispone dell'autorizzazione speciale *ALLOBJ. Il programma CPPGM08 richiede l'autorizzazione *CHANGE sul file. CPPGM08 è di proprietà del profilo OWNCP e adotta l'autorizzazione proprietario (USRPRF è *OWNER).

1. Diagramma di flusso 1, passo 1.
   a. Diagramma di flusso 2, passo 1.
2. Diagramma di flusso 1, passo 2.
   a. Diagramma di flusso 3, passi 1 e 2. Oggetto da controllare = CONTRACTS/PRICES *FILE.
   b. Diagramma di flusso 3, passo 3.
      1) Diagramma di flusso 4, passo 1. SMITHG non possiede il file PRICES. Ritornare al Diagramma di flusso 3 senza alcuna autorizzazione rilevata.
   c. Diagramma di flusso 3, passo 4.
      1) Diagramma di flusso 5, passi 1, 2 e 3. L'autorizzazione pubblica non è sufficiente.
   d. Diagramma di flusso 3, passo 5.
   e. **Diagramma di flusso 3, passo 6**. SMITHG non dispone dell'autorizzazione privata.
   f. Diagramma di flusso 3, passi 7 e 8. Il file PRICES non è protetto da un elenco di autorizzazioni. Ritornare al Diagramma di flusso 1 senza alcuna autorizzazione rilevata.
3. Diagramma di flusso 1, passo 3. SMITHG non dispone dei un gruppo.
4. Diagramma di flusso 1, passo 5.
   a. Diagramma di flusso 7, passo 1. L'autorizzazione pubblica non è *AUTL.
   b. Diagramma di flusso 7, passo 3. Oggetto da controllare = CONTRACTS/PRICES *FILE.
   c. Diagramma di flusso 7, passo 4. L'autorizzazione pubblica non è sufficiente.
5. Diagramma di flusso 1, passo 6.
   a. Diagramma di flusso 8A, passo 1. Oggetto da controllare = CONTRACTS/PRICES *FILE.
   b. Diagramma di flusso 8A, passi 2 e 3. OWNCP non dispone dell'autorizzazione *ALLOBJ.
   c. Diagramma di flusso 8A, passo 4.
      1) Diagramma di flusso 4, passi 1, 2 e 3. Autorizzato. OWNCP possiede i file PRICES e dispone dell'autorizzazione sufficiente.

Analisi:

Questo esempio dimostra il miglioramento delle prestazioni derivanti dall'utilizzo dell'autorizzazione adottata quando il proprietario del programma possiede anche gli oggetti dell'applicazione.

Il numero di passi necessari per l'esecuzione del controllo delle autorizzazioni non ha quasi alcun effetto sulle prestazioni, poiché la maggior parte dei passi non richiede il richiamo di nuove informazioni. In questo esempio, sebbene vengano eseguite molti fasi, le ricerche nelle autorizzazioni private vengono effettuate una sola volta (per l'utente SMITHG).

Confrontare questo esempio con il "Caso 1: Utilizzo autorizzazione gruppo privata" a pagina 199.

- Se si sta modificando il Caso 1 in modo che il profilo del gruppo DPTSM possegga il file PRICES e disponga dell'autorizzazione *ALL su di esso, le caratteristiche delle prestazioni dei due esempi sono uguali. Tuttavia, un profilo gruppo che possiede gli oggetti dell'applicazioni potrebbe rappresentare un problema per la sicurezza. I membri del gruppo hanno sempre l'autorizzazione del gruppo

(proprietario), a meno che non si fornisca, specificatamente, ai membri del gruppo un'autorizzazione inferiore. Quando si utilizza l'autorizzazione adottata, è possibile controllare le situazioni in cui viene utilizzata l'autorizzazione del proprietario.

- È possibile inoltre modificare il Caso 1 in modo tale che DPTSM sia il gruppo principale per il file PRICES e disponga dell'autorizzazione *CHANGE su di esso. Se DPTSM è il primo gruppo per SMITHG (specificato nel parametro GRPPRF del profilo utente di SMITHG), le caratteristiche delle prestazioni sarebbero uguali a quelle del Caso 5.

Caso 6: Autorizzazione utente e gruppo

Questo caso dimostra che un utente può vedersi negato l'accesso ad un oggetto anche se il gruppo dell'utente dispone di autorizzazione sufficiente.

L'utente WILSONJ desidera accedere al file PRICES utilizzando il programma CPPGM01, che richiede l'autorizzazione *CHANGE. WILSONJ è un membro del profilo gruppo DPTSM e non dispone dell'autorizzazione speciale *ALLOBJ. Il programma CPPGM01 non utilizza l'autorizzazione adottata e ignora ogni autorizzazione adottata precedente (USEADPAUT è *NO).

1. Diagramma di flusso 1, passo 1.
   a. Diagramma di flusso 2, passo 1. PRICES dispone di autorizzazioni private.
2. Diagramma di flusso 1, passo 2.
   a. Diagramma di flusso 3, passi 1 e 2. Oggetto da controllare = CONTRACTS/PRICES *FILE.
   b. Diagramma di flusso 3, passo 3.
      1) Diagramma di flusso 4, passo 1. WILSONJ non possiede il file PRICES. Ritornare al Diagramma di flusso 3 senza alcuna autorizzazione rilevata.
   c. Diagramma di flusso 3, passo 4.
      1) Diagramma di flusso 5, passi 1, 2 e 3. L'autorizzazione pubblica non è sufficiente.
   d. Diagramma di flusso 3, passo 5.
   e. **Diagramma di flusso 3, passo 6**. WILSONJ dispone dell'autorizzazione *USE, che non è sufficiente.
   f. Diagramma di flusso 3, passo 8. Oggetto da verificare = CONTRACTS/PRICES *FILE. Ritornare al Diagramma di flusso 1 con autorizzazione insufficiente.
3. Diagramma di flusso 1, passo 6.
   a. Diagramma di flusso 8A, passo 1. Oggetto da controllare = CONTRACTS/PRICES *FILE.
   b. Diagramma di flusso 8A, passo 2. Il programma CPPGM01 non adotta l'autorizzazione.
   c. Diagramma di flusso 8A, passo 5. Il parametro *USEADPAUT per il programma CPPGM01 è *NO.
   d. Diagramma di flusso 8A, passi 8 e 9.
      1) Diagramma di flusso 8B, passo 1. Il programma CPPGM01 non adotta l'autorizzazione.
      2) Diagramma di flusso 8B, passo 7. Il parametro *USEADPAUT per il programma CPPGM01 è *NO. Accesso negato.

Analisi:

Fornendo all'utente la stessa autorizzazione del pubblico ma inferiore rispetto a quella del gruppo dell'utente, le prestazioni del controllo delle autorizzazioni per gli altri utenti non vengono coinvolte. Tuttavia, se WILSONJ avesse l'autorizzazione *EXCLUDE (inferiore a quella del pubblico), l'utente perderebbe i benefici delle prestazioni illustrati nel Caso 4.

Sebbene questo esempio presenti numerosi passi, le ricerche nelle autorizzazioni private vengono effettuate una sola volta. Ciò garantisce prestazioni accettabili.

Caso 7: Autorizzazione pubblica senza autorizzazione privata

Questo caso dimostra il miglioramento delle prestazioni derivanti dall'utilizzo dell'autorizzazione pubblica senza autorizzazione privata.

Le informazioni sull'autorizzazione per il file ITEM appaiono come di seguito spiegato:

```
                          Visualizzazione autorizzazione oggetto

Oggetto . . . . . . . :   ITEM           Proprietario . . . . . . . :   OWNIC
  Libreria. . . . . :   ITEMLIB        Gruppo principale . . . :   *NONE
Tipo di oggetto. . . :   *FILE          Unità ASP . . . . . :   *SYSBAS

Oggetto protetto da elenco di autorizzazioni . . . . . . . . . . . . :   *NONE

                        Autorizzazione
Utente        Gruppo   oggetto
OWNIC                   *ALL
*PUBLIC     *USE
```

Figura 22. Visualizzazione autorizzazione oggetto

ROSSM necessita dell'autorizzazione *USE sul file ITEM. ROSSM è un membro del profilo gruppo DPTSM. Di seguito vengono riportati i passi del controllo delle autorizzazioni:

Diagramma di flusso 1, passo 1.

1. Diagramma di flusso 2, passi 1, 2 e 3. L'autorizzazione di OWNIC è insufficiente.
2. Diagramma di flusso 2, passo 4. Il file ITEM non dispone di un gruppo principale.
3. Diagramma di flusso 2, passo 6. Autorizzato. L'autorizzazione pubblica è sufficiente.

Analisi:

L'autorizzazione pubblica fornisce le prestazioni migliori quando viene utilizzata senza autorizzazioni private. In questo esempio, non vengono mai effettuate ricerche nelle autorizzazioni private.

Caso 8: Autorizzazione adottata senza autorizzazione privata

Questo caso mostra il vantaggio di utilizzare l'autorizzazione adottata senza autorizzazione privata.

Per questo esempio, tutti i programmi nell'applicazione sono di proprietà del profilo OWNIC. Ogni programma nell'applicazione che richiede più di un'autorizzazione *USE adotta l'autorizzazione del proprietario. Di seguito vengono riportate le fasi per l'utente WILSONJ necessarie per ottenere l'autorizzazione *CHANGE sul file ITEM utilizzando il programma ICPGM10, che adotta l'autorizzazione:

1. Diagramma di flusso 1, passo 1.
   a. Diagramma di flusso 2, passi 1, 2, 3, 4 e 6. L'autorizzazione pubblica non è sufficiente.
2. Diagramma di flusso 1, passo 2.
   a. Diagramma di flusso 3, passi 1 e 2. Oggetto da controllare = ITEMLIB/ITEM *FILE.
   b. Diagramma di flusso 3, passo 3.
      1) Diagramma di flusso 4, passo 1. WILSONJ non possiede il file ITEM. Ritornare al Diagramma di flusso 3 senza alcuna autorizzazione rilevata.
   c. Diagramma di flusso 3, passo 4.
      1) Diagramma di flusso 5, passi 1 e 3. L'autorizzazione pubblica non è sufficiente. Ritornare al Diagramma di flusso 3 senza alcuna autorizzazione rilevata.
   d. Diagramma di flusso 3, passi 5, 7 e 8. Il file ITEM non è protetto da un elenco di autorizzazioni. Ritornare al Diagramma di flusso 1 senza alcuna autorizzazione rilevata.

3. Diagramma di flusso 1, passi 3 e 5. (WILSONJ non possiede un profilo gruppo.)
   a. Diagramma di flusso 7, passi 1, 3 e 4. Il pubblico dispone dell'autorizzazione *USE, che non è sufficiente.
4. Diagramma di flusso 1, passo 6.
   a. Diagramma di flusso 8A, passo 1. Oggetto da controllare = ITEMLIB/ITEM *FILE.
   b. Diagramma di flusso 8A, passi 2, 3 e 4. Il profilo OWNIC non dispone dell'autorizzazione *ALLOBJ.
      1) Diagramma di flusso 4, passi 1, 2 e 3. Autorizzato. OWNIC dispone di autorizzazione sufficiente al file ITEM.

Analisi:

Questo esempio mostra i vantaggi derivanti dall'utilizzo dell'autorizzazione adottata senza l'autorizzazione privata, soprattutto se il proprietario dei programmi possiede anche gli oggetti dell'applicazione. Questo esempio non richiede la ricerca nelle autorizzazioni private.

Caso 9: Utilizzo di un elenco di autorizzazioni

Questo caso dimostra il vantaggio di utilizzare elenchi di autorizzazioni.

Il file ARWKR01 nella libreria CUSTLIB è protetto dall'elenco di autorizzazioni ARLST1. La Figura 23 e la Figura 24 mostrano le autorizzazioni:

```
                          Visualizzazione autorizzazione oggetto

Oggetto. . . . . :   ARWRK01       Proprietario. . . . . :   OWNAR
  Libreria. . . . :   CUSTLIB      Gruppo principale  . . :   *NONE
Tipo oggetto  . . . . :   *FILE        Unità ASP . . . . . :   *SYSBAS

Oggetto protetto da elenco di autorizzazioni. . . . . . . . . . . . :   ARLST1

                        Autorizzazione
Utente        Gruppo    oggetto
OWNCP                   *ALL
*PUBLIC                 *USE
```

Figura 23. Autorizzazione per il file ARWRK01

```
                          Visualizzazione elenco di autorizzazioni

Oggetto. . . . . :   ARLST1      Proprietario. . . . . :   OWNAR
  Libreria . . . . . :   QSYS        Gruppo principale  . . . :   *NONE

                        Autorizz. Gestione
Utente      Gruppo      oggetto    elenco
OWNCP                   *ALL
AMESJ                   *CHANGE
*PUBLIC                 *USE
```

Figura 24. Autorizzazione per l'elenco di autorizzazioni ARLST1

L'utente AMESJ, che non è un membro di un profilo gruppo, necessita dell'autorizzazione *CHANGE sul file ARWRK01. Di seguito vengono riportati i passi del controllo delle autorizzazioni:

1. Diagramma di flusso 1, passo 1.
   a. Diagramma di flusso 2, passi 1 e 2. Il file ARWRK01 viene protetto da un elenco di autorizzazioni.
2. Diagramma di flusso 1, passo 2.
   a. Diagramma di flusso 3, passi 1 e 2. Oggetto da controllare = CUSTLIB/ARWRK01 *FILE.
   b. Diagramma di flusso 3, passo 3.

1) Diagramma di flusso 4, passo 1. AMESJ non possiede il file ARWRK01. Ritornare al Diagramma di flusso 2 senza alcuna autorizzazione rilevata.

c. Diagramma di flusso 3, passo 4.
   1) Diagramma di flusso 5, passi 1 e 3. L'autorizzazione pubblica non è sufficiente. Ritornare al Diagramma di flusso 3 senza alcuna autorizzazione rilevata.

d. Diagramma di flusso 3, passi 5, 7 e 9. Oggetto da controllare = ARLST1 *AUTL.

e. Diagramma di flusso 3, passo 3.
   1) Diagramma di flusso 4, passo 1. AMESJ non possiede l'elenco di autorizzazioni ARLST1. Ritornare al Diagramma di flusso 3 senza alcuna autorizzazione rilevata.

f. Diagramma di flusso 3, passi 4 e 5.

g. Diagramma di flusso 3, passo 6. Autorizzato. AMESJ dispone dell'autorizzazione *CHANGE sull'elenco di autorizzazioni ARLST1.

Analisi:

Questo esempio dimostra che gli elenchi di autorizzazioni possono creare autorizzazioni di facile gestione e fornire buone prestazioni. Ciò è particolarmente vero se gli oggetti protetti dall'elenco di autorizzazioni non dispongono di autorizzazioni private.

Se AMESJ fosse un membro di un profilo gruppo, aggiungerà passi ulteriori a questo esempio, ma non aggiungerà una ricerca ulteriore delle autorizzazioni private, almeno fino a quando nessuna autorizzazione privata viene definita il file ARWRK01. I problemi legati alle prestazioni si verificano per lo più quando le autorizzazioni private, gli elenchi di autorizzazioni e i profili di gruppo sono combinati, come ad esempio nel "Caso 11: Combinazione dei metodi di autorizzazione" a pagina 208.

Caso 10: Utilizzo di gruppi multipli

Questo è un esempio di utilizzo di gruppi multipli.

WOODBC necessita dell'autorizzazione *CHANGE sul file CRLIM. WOODBC è un membro di tre gruppi: DPTAR, DPTSM e DPTMG. DPTAR è il primo profilo gruppo (GRPPRF). DPTSM e DPTMG sono profili gruppo aggiuntivi (SUPGRPPRF). La Figura 25 mostra le autorizzazioni per il file CRLIM:

```
                        Visualizzazione autorizzazione oggetto

Oggetto. . . . . :   CRLIM          Proprietario. . . . . :   OWNAR
  Libreria . . . . . :   CUSTLIB        Gruppo principale. . :   DPTAR
Tipo di oggetto. . :   *FILE     Unità ASP  . . . . . :   *SYSBAS

 Oggetto protetto da elenco di autorizzazioni  . . . . . :   *NONE

                        Autorizzazione
Utente        Gruppo   oggetto
OWNAR                   *ALL
DPTAR                   *CHANGE
DPTSM                    *USE
*PUBLIC                  *EXCLUDE
```

Figura 25. Autorizzazione per il file CRLIM

Di seguito vengono riportati i passi del controllo delle autorizzazioni:

1. Diagramma di flusso 1, passo 1.
   a. Diagramma di flusso 2, passo 1. Ritornare al diagramma di flusso con autorizzazione insufficiente.
2. Diagramma di flusso 1, passo 2.
   a. Diagramma di flusso 3, passi 1 e 2. Oggetto da controllare = CUSTLIB/CRLIM *FILE.
   b. Diagramma di flusso 3, passo 3.

1) Diagramma di flusso 4, passo 1. WOODBC non possiede il file CRLIM. Ritornare al Diagramma di flusso 3 senza alcuna autorizzazione rilevata.

c. Diagramma di flusso 3, passo 4.

1) Diagramma di flusso 5, passi 1, 2 e 3. L'autorizzazione pubblica non è sufficiente.

d. Diagramma di flusso 3, passo 5.

e. Diagramma di flusso 3, passo 6. WOODBC non dispone dell'autorizzazione sul file CRLIM.

f. Diagramma di flusso 3, passi 7 e 8. Il file CRLIM non è protetto da un elenco di autorizzazioni. Ritornare al Diagramma di flusso 1 senza alcuna autorizzazione rilevata.

3. Diagramma di flusso 1, passi 3 e 4. Il primo gruppo per WOODBC è DPTAR.

a. Diagramma di flusso 6, passi 1 e 2. Oggetto da controllare = CUSTLIB/CRLIM *FILE.

b. Diagramma di flusso 6, passo 3.

1) Diagramma di flusso 4, passo 1. DPTAR non possiede il file CRLIM. Ritornare al Diagramma di flusso 6 senza alcuna autorizzazione rilevata.

c. Diagramma di flusso 6, passi 4 e 5. Autorizzato. DPTAR è il gruppo principale e dispone di autorizzazione sufficiente.

Caso 11: Combinazione dei metodi di autorizzazione

Questo caso dimostra una struttura negativa dell'autorizzazione.

WAGNERB necessita dell'autorizzazione *ALL sul file CRLIMWRK. WAGNERB è un membro di questi gruppi: DPTSM, DPT702 e DPTAR. Il primo gruppo di WAGNERB (GRPPRF) è DPTSM. La Figura 26 mostra l'autorizzazione per il file CRLIMWRK.

```
                         Visualizzazione autorizzazione oggetto

Oggetto. . . . . :   CRLIMWRK        Proprietario. . . . . :   OWNAR
  Libreria . . . . . :   CUSTLIB         Gruppo principale  . . . :   *NONE
Tipo di oggetto. . :   *FILE     Unità ASP  . . . . . :   *SYSBAS

Oggetto protetto da elenco di autorizzazione  . . . . . :   CRLST1

                       Autorizzazione
Utente        Gruppo   oggetto
OWNAR                   *ALL
DPTSM                    *USE
WILSONJ                 *EXCLUDE
*PUBLIC     *USE
```

Figura 26. Autorizzazione per il file CRLIMWRK

Il file CRLIMWRK è protetto dall'elenco di autorizzazioni CRLST1. La Figura 27 mostra l'autorizzazione per l'elenco di autorizzazioni CRLST1.

```
                        Visualizzazione elenco di autorizzazioni

Oggetto. . . . . :   CRLST1        Proprietario. . . . . :   OWNAR
  Libreria . . . . . :     QSYS        Gruppo principale  . . . :   DPTAR

                       Autorizz. Gestione
Utente      Gruppo     oggetto    elenco
OWNAR                  *ALL        X
DPTAR                  *ALL
*PUBLIC                 *EXCLUDE
```

Figura 27. Autorizzazione per l'elenco di autorizzazioni CRLST1

Questo esempio mostra molte delle possibilità di controllo delle autorizzazioni. Dimostra inoltre come l'utilizzo di troppe opzioni delle autorizzazioni per un oggetto può peggiorare le prestazioni.

Di seguito vengono riportati i passi necessari per controllare l'autorizzazione di WAGNERB sul file CRLIMWRK:

1. Diagramma di flusso 1, passo 1.
   a. Diagramma di flusso 2, passo 1.
2. Diagramma di flusso 1, passo 2.
   a. Diagramma di flusso 3, passi 1 e 2. Oggetto da controllare = CUSTLIB/CRLIMWRK *FILE.
   b. Diagramma di flusso 3, passo 3.
      1) Diagramma di flusso 4, passo 1. WAGNERB non possiede il file CRLIMWRK. Ritornare al Diagramma di flusso 3 senza alcuna autorizzazione rilevata.
   c. Diagramma di flusso 3, passo 4.
      1) Diagramma di flusso 5, passi 1 e 2. WILSONJ dispone dell'autorizzazione *EXCLUDE, che è inferiore all'autorizzazione pubblica *USE.
   d. Diagramma di flusso 3, passi 5 e 6 (**prima ricerca delle autorizzazioni private**). WAGNERB non dispone dell'autorizzazione privata.
   e. Diagramma di flusso 3, passi 7 e 9. Oggetto da controllare = CRLST1 *AUTL.
   f. Diagramma di flusso 3, passo 3.
      1) Diagramma di flusso 4, passo 1. WILSONJ non possiede CRLST1. Ritornare al Diagramma di flusso 3 senza alcuna autorizzazione rilevata.
   g. Diagramma di flusso 3, passi 4 e 5.
   h. Diagramma di flusso 3, passo 6 (**seconda ricerca delle autorizzazioni private**). WAGNERB non dispone dell'autorizzazione privata su CRLST1.
   i. Diagramma di flusso 3, passi 7 e 8. Oggetto da controllare = CUSTLIB/CRLIMWRK *FILE.
3. Diagramma di flusso 1, passi 3 e 4. Il primo profilo gruppo di WAGNERB è DPTSM.
   a. Diagramma di flusso 6, passi 1 e 2. Oggetto da controllare = CUSTLIB/CRLIMWRK *FILE.
   b. Diagramma di flusso 6, passo 3.
      1) Diagramma di flusso 4, passo 1. DPTSM non possiede il file CRLIMWRK. Ritornare al Diagramma di flusso 6 senza alcuna autorizzazione rilevata.
   c. Diagramma di flusso 6, passo 4. DPTSM non è il gruppo principale per il file CRLIMWRK.
   d. Diagramma di flusso 6, passo 6 (**terza ricerca delle autorizzazioni private**). DPTSM ha l'autorizzazione *USE sul file CRLIMWRK che non è sufficiente.
   e. Diagramma di flusso 6, passo 6 continuare. L'autorizzazione *USE viene aggiunta a ciascuna autorizzazione già rilevata per i gruppi di WAGNERB (nessuna). Un'autorizzazione sufficiente non è stata ancora trovata.
   f. Diagramma di flusso 6, passi 9 e 10. Il gruppo successivo di WAGNERB è DPT702.
   g. Diagramma di flusso 6, passi 1 e 2. Oggetto da controllare = CUSTLIB/CRLIMWRK *FILE.
   h. Diagramma di flusso 6, passo 3.
      1) Diagramma di flusso 4, passo 1. DPT702 non possiede il file CRLIMWRK. Ritornare al Diagramma di flusso 6 senza alcuna autorizzazione rilevata.
   i. Diagramma di flusso 6, passo 4. DPT702 non è il gruppo principale per il file CRLIMWRK.
   j. Diagramma di flusso 6, passo 6 (**quarta ricerca delle autorizzazioni private**). DPT702 non dispone dell'autorizzazione sul file CRLIMWRK.
   k. Diagramma di flusso 6, passi 7 e 8. Oggetto da controllare = CRLST1 *AUTL
   l. Diagramma di flusso 6, passo 3.
      1) Diagramma di flusso 5, passo 1. DPT702 non possiede l'elenco di autorizzazioni CRLST1. Ritornare al Diagramma di flusso 6 senza alcuna autorizzazione rilevata.

m. Diagramma di flusso 6, passi 4 e 6 (**quinta ricerca delle autorizzazioni private**). DPT702 non dispone di autorizzazioni all'elenco di autorizzazioni CRLST1.
n. Diagramma di flusso 6, passi 7, 9 e 10. DPTAR è il profilo gruppo di WAGNERB successivo.
o. Diagramma di flusso 6, passi 1 e 2. Oggetto da controllare = CUSTLIB/CRLIMWRK *FILE.
p. Diagramma di flusso 6, passo 3.
    1) Diagramma di flusso 4, passo 1. DPTAR non possiede il file CRLIMWRK. Ritornare al Diagramma di flusso 6 senza alcuna autorizzazione rilevata.
q. Diagramma di flusso 6, passi 4 e 6 (**sesta ricerca delle autorizzazioni private**). DPTAR non dispone di autorizzazioni sul file CRLIMWRK.
r. Diagramma di flusso 6, passi 7 e 8. Oggetto da controllare = CRLST1 *AUTL
s. Diagramma di flusso 6, passo 3.
    1) Diagramma di flusso 4, passo 1. DPTAR non possiede l'elenco di autorizzazioni CRLST1. Ritornare al Diagramma di flusso 6 senza alcuna autorizzazione rilevata.
t. Diagramma di flusso 6, passi 4 e 5. Autorizzato. DPTAR è il gruppo principale per l'elenco di autorizzazioni CRLST1 e dispone dell'autorizzazione *ALL.

Risultato:

WAGNERB è autorizzato ad eseguire l'operazione richiesta utilizzando l'autorizzazione del gruppo principale di DPTAR sull'elenco di autorizzazioni CRLIST1.

Analisi:

Questo esempio dimostra una struttura negativa dell'autorizzazione, sia per quel che riguarda la gestione che dal punto di vista delle prestazioni. Vengono utilizzate troppe opzioni, rendendo difficile la comprensione, la modifica e il controllo. Le ricerche vengono effettuate nelle autorizzazioni private sei volte, che potrebbero portare a notevoli problemi nelle prestazioni:

Profilo	Oggetto	Tipo	Risultato
WAGNERB	CRLIMWRK	*FILE	Nessuna autorizzazione rilevata
WAGNERB	CRLST1	*AUTL	Nessuna autorizzazione rilevata
DPTSM	CRLIMWRK	*FILE	Autorizzazione *USE (insufficiente)
DPT702	CRLIMWRK	*FILE	Nessuna autorizzazione rilevata
DPT702	CRLST1	*AUTL	Nessuna autorizzazione rilevata
DPTAR	CRLIMWRK	*FILE	Nessuna autorizzazione rilevata

Modificando la sequenza dei profili gruppo di WAGNERB, si modificano le caratteristiche delle prestazioni di questo esempio. Si presupponga che DPTAR sia il primo profilo gruppo di WAGNERB (GRPPRF). Il sistema dovrebbe effettuare la ricerca delle autorizzazioni private 3 volte prima di rilevare l'autorizzazione del gruppo principale di DPTAR sull'elenco di autorizzazioni CRLST1.

- Autorizzazione WAGNERB per il file CRLIMWRK
- Autorizzazione WAGNERB per l'elenco di autorizzazioni di CRLST1
- Autorizzazione DPTAR per il file CRLIMWRK

Una pianificazione attenta dei profili gruppo e degli elenchi di autorizzazioni è fondamentale per avere ottime prestazioni di sistema.

Cache autorizzazioni

Il sistema crea cache delle autorizzazioni per gli utenti per migliorare la flessibilità e le prestazioni.

Dalla Versione 3, Release 7, il sistema crea una cache delle autorizzazioni per l'utente la prima volta che questo accede ad un oggetto. Ogni volta che si accede all'oggetto, il sistema ricerca l'autorizzazione nella cache dell'utente prima di ricercare nel profilo utente. Ciò garantisce un controllo più rapido dell'autorizzazione privata.

La cache delle autorizzazioni contiene fino a 32 autorizzazioni privati sugli oggetti e fino a 32 autorizzazioni private sugli elenchi di autorizzazioni. La cache viene aggiornata quando viene concessa o revocata un'autorizzazione utente. Tutte le cache degli utenti vengono ripulite quando si esegue l'IPL del sistema.

Mentre si consiglia l'utilizzo limitato delle autorizzazioni private, la cache dal canto suo offre una maggiore flessibilità. Ad esempio, è possibile scegliere come proteggere gli oggetti senza preoccuparsi troppo dell'effetto sulle prestazioni del sistema. Ciò è particolarmente vero se gli utenti accedono agli stessi oggetti ripetutamente.

Capitolo 6. Sicurezza gestione lavoro

Questa sezione tratta i problemi di sicurezza associati alla gestione del lavoro sul sistema.

In questa sezione sono descritte le seguenti problematiche.

Informazioni correlate

Gestione lavoro

Inizio lavoro

Il sistema controlla l'autorizzazione ad alcuni oggetti al momento dell'avvio di un lavoro.

Quando si inizia un lavoro sul sistema, gli oggetti vengono associati al lavoro, come ad esempio una coda di emissione, una descrizione del lavoro e le librerie nell'elenco di librerie. L'autorizzazione per alcuni di questi oggetti viene controllata prima che sia consentito l'avvio del lavoro mentre per altri oggetti dopo che il lavoro è stato avviato. Un'autorizzazione inadeguata può causare degli errori o la chiusura del lavoro.

Gli oggetti che sono parte della struttura di un lavoro possono essere specificati nella descrizione lavoro, nel profilo utente e sul comando Inoltro lavoro (SBMJOB) per un lavoro batch.

Avvio di un lavoro interattivo

Questo argomento è una descrizione dell'attività di sicurezza eseguita all'avvio di un lavoro interattivo.

Poiché è possibile specificare gli oggetti utilizzati da un lavoro seguendo diverse procedure, di seguito ne viene riportata una di esempio.

Quando si verifica un errore durante il processo di accesso, viene visualizzato un messaggio nella parte inferiore del pannello di accesso che descrive l'errore. Alcuni errori delle autorizzazioni possono provocare inoltre la scrittura di una registrazione lavori. Se un utente non è in grado di collegarsi a causa di un errore dell'autorizzazione, modificare il profilo utente in modo da specificare un oggetto diverso oppure concedere all'utente l'autorizzazione sull'oggetto.

Dopo che l'utente ha immesso un ID utente e una parola d'ordine, questi passi vengono eseguiti prima che un lavoro venga realmente avviato sul sistema:

1. Il profilo utente e la parola d'ordine vengono verificati. Lo stato del profilo utente deve essere *ENABLED. Il profilo utente specificato sul pannello di accesso deve disporre dell'autorizzazione *OBJOPR e *CHANGE su se stesso.
2. L'autorizzazione utente che consente di utilizzare la stazione di lavoro viene controllata. Consultare "Stazioni di lavoro" a pagina 215 per dettagli.
3. Il sistema verifica l'autorizzazione per i valori nel profilo utente e nella descrizione del lavoro dell'utente che vengono utilizzati per creare la struttura del lavoro, come ad esempio:
   - Descrizione lavoro
   - Coda di emissione
   - Libreria corrente
   - Librerie nell'elenco librerie

   Se qualcuno di questi oggetti non esiste o l'utente non dispone dell'autorizzazione adeguata, viene visualizzato un messaggio nella parte inferiore del pannello di accesso e l'utente non può collegarsi. Se l'autorizzazione per tali oggetti viene verificata con esito positivo, il lavoro viene avviato sul sistema.

Nota: l'autorizzazione sull'unità di stampa e sulla coda lavori non viene verificata fino quando l'utente non tenta di utilizzarle.

Una volta avviato il lavoro, questi passi vengono eseguiti prima che l'utente visualizzi il primo pannello o menu:

1. Se la voce di instradamento per il lavoro specifica un programma utente, il normale controllo dell'autorizzazione viene effettuato sul programma, sulla libreria del programma e sugli oggetti utilizzati dal programma. Se l'autorizzazione non è adeguata, viene inviato un messaggio all'utente sul pannello Accesso e il lavoro viene terminato.
2. Se la voce di instradamento specifica il processore dei comandi (QCMD):
   a. Il controllo dell'autorizzazione viene effettuato per il programma del processore QCMD, la libreria del programma e per gli oggetti utilizzati, come descritto nel passo 1.
   b. L'autorizzazione dell'utente sul Programma di gestione tasto di attenzione e sulla libreria viene controllata. Se l'autorizzazione non è adeguata, viene inviato un messaggio all'utente e viene scritta una registrazione lavori. Il processo prosegue.

      Se l'autorizzazione è adeguata, il programma di gestione tasto di attenzione viene attivato. Il programma non viene avviato fino a quando l'utente non preme il tasto di Attenzione per la prima volta. In quel momento, il normale controllo dell'autorizzazione viene effettuato sugli oggetti utilizzati dal programma.
   c. Il normale controllo dell'autorizzazione viene eseguito per il programma iniziale (e gli oggetti associati) specificato nel profilo utente. Se l'autorizzazione è adeguata, il programma viene avviato. Se l'autorizzazione non è adeguata, viene inviato un messaggio all'utente e viene scritta una registrazione lavori. Il lavoro termina.
   d. Il normale controllo dell'autorizzazione viene eseguito per il menu iniziale (e gli oggetti associati) specificato nel profilo utente. Se l'autorizzazione è adeguata, il menu viene visualizzato. Se l'autorizzazione non è adeguata, viene inviato un messaggio all'utente e viene scritta una registrazione lavori. Il lavoro termina.

Avvio di un lavoro batch

Questo argomento include una descrizione di un'attività di sicurezza eseguita quando si avvia un lavoro batch.

Poiché esistono diversi metodi per inoltrare i lavori e specificare gli oggetti utilizzati dal lavoro, di seguito vengono presentate solo delle informazioni guida. Questo esempio utilizza un lavoro inoltrato da un lavoro interattivo utilizzando il comando di inoltro del lavoro (SBMJOB).

Quando si immette il comando SBMJOB, questo controllo viene eseguito prima che il lavoro venga aggiunto alla coda lavori:

1. Se si specifica un profilo utente sul comando SBMJOB, è necessario disporre dell'autorizzazione *USE sul profilo utente.
2. L'autorizzazione viene controllata per gli oggetti specificati come parametri sul comando SBMJOB e nella descrizione lavoro. L'autorizzazione viene controllata per il profilo utente nel quale verrà eseguito il lavoro.
3. Se il livello di sicurezza è 40 o 50 e il comando SBMJOB specifica USER(*JOBD), l'utente che inoltra il lavoro deve disporre dell'autorizzazione *USE sul profilo utente nella descrizione del lavoro.
4. Se un oggetto non esiste o se l'autorizzazione non è adeguata, viene inviato un messaggio all'utente e il lavoro non viene inoltrato.

Quando il sistema seleziona il lavoro dalla coda lavori e tenta di avviare il lavoro, la sequenza di controllo dell'autorizzazione è simile a quella per l'avvio di un lavoro interattivo.

Autorizzazione adottata e lavori batch

È possibile modificare i parametri per un lavoro batch quando è in esecuzione nell'autorizzazione adottata.

Quando si avvia un nuovo lavoro, viene creato un nuovo stack di chiamata per il lavoro. L'autorizzazione adottata non può avere effetto fino a quando il primo programma non viene aggiunto allo stack di chiamata. L'autorizzazione adottata non può essere utilizzata per ottenere l'accesso agli oggetti, come ad esempio una coda di emissione o una descrizione lavoro, che vengono aggiunti alla struttura lavoro prima che il lavoro venga instradato. Per questo motivo, anche se il lavoro interattivo è in esecuzione nell'autorizzazione adottata quando si inoltra un lavoro, tale autorizzazione adottata non viene utilizzata quando si controlla l'autorizzazione per gli oggetti sulla richiesta SBMJOB.

È possibile modificare le caratteristiche di un lavoro batch quando questo è in attesa di essere eseguito, utilizzando il comando CHGJOB (Modifica lavoro). Consultare Comandi lavoro per l'autorizzazione necessaria per modificare i parametri di un lavoro.

Stazioni di lavoro

Il sistema esegue il controllo autorizzazione per una stazione di lavoro all'accesso.

Una *descrizione dell'unità* contiene informazioni su una particolare unità o unità logica collegata al sistema. Quando ci si collega al sistema, la stazione di lavoro viene collegata alla descrizione dell'unità fisica o virtuale. Per collegarsi con esito positivo, è necessario disporre dell'autorizzazione *CHANGE per la descrizione dell'unità.

Il valore di sistema QLMTSECOFR (limitazione responsabile riservatezza) controlla se gli utenti con autorizzazione speciale *ALLOBJ o *SERVICE devono essere autorizzati specificatamente sulle descrizioni dell'unità.

La Figura 28 a pagina 216 mostra la logica in base alla quale si determina se un utente è autorizzato ad accedere ad un'unità:

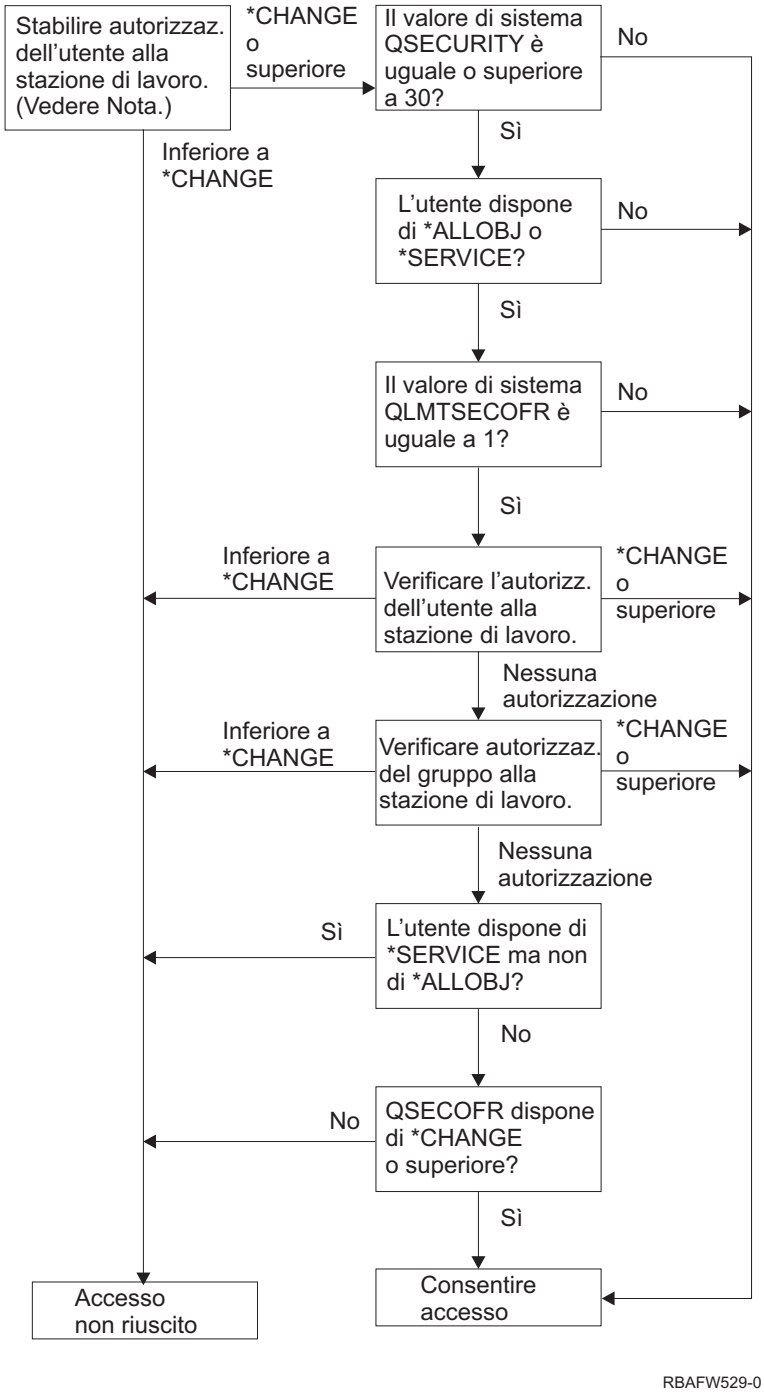


Figura 28. Controllo autorizzazione per le stazioni di lavoro

Nota: il normale controllo dell'autorizzazione viene eseguito per stabilire se l'utente dispone almeno dell'autorizzazione *CHANGE sulla descrizione dell'unità. L'autorizzazione *CHANGE può essere rilevata utilizzando le seguenti autorizzazioni:

- L'autorizzazione speciale *ALLOBJ dal profilo utente, profilo di gruppo o profili di gruppo supplementari.
- L'autorizzazione privata sulla descrizione dell'unità nel profilo utente, profilo di gruppo o profili di gruppo supplementari.
- L'autorizzazione su un elenco di autorizzazioni utilizzato per proteggere la descrizione dell'unità.

- L'autorizzazione ad un elenco di autorizzazioni utilizzato per proteggere l'autorizzazione pubblica.

Il controllo dell'autorizzazione per la descrizione dell'unità viene eseguita prima che i programmi si trovino nello stack di chiamata per il lavoro; per questo motivo, l'autorizzazione adottata non viene applicata.

Descrizione del controllo dell'autorizzazione per le stazioni di lavoro

Il sistema determina l'autorizzazione dell'utente sulla stazione di lavoro. (Consultare nota 1) Se l'autorizzazione è inferiore a *CHANGE, l'accesso non riesce. Se l'autorizzazione è *CHANGE o superiore, verificare che il livello di sicurezza sul sistema sia 30 o maggiore. In caso contrario, l'utente è abilitato ad eseguire l'accesso.

Se il livello di sicurezza è 30 o superiore, il sistema controlla se l'utente dispone dell'autorizzazione speciale *ALLOBJ o *SERVICE. Se l'utente non dispone di alcuna di queste autorizzazioni speciali, l'accesso può essere effettuato.

Se l'utente dispone delle autorizzazioni speciali *ALLOBJ o *SERVICE, il sistema controlla se il valore di sistema QLMTSECOFR è impostato su 1. Nel caso in cui non fosse impostato su 1, l'accesso è consentito.

Se il valore di sistema QLMTSECOFR è impostato su 1, il sistema verificherà l'autorizzazione utente sulla stazione di lavoro. Se l'autorizzazione dell'utente è *CHANGE o superiore, l'accesso è consentito. Se l'autorizzazione dell'utente è inferiore a *CHANGE, l'accesso non riesce. Se l'utente non dispone di un'autorizzazione sulla stazione di lavoro, il sistema controlla l'autorizzazione gruppo dell'utente sulla stazione di lavoro.

Se l'autorizzazione gruppo dell'utente è *CHANGE o superiore, l'accesso è consentito. Se l'autorizzazione gruppo dell'utente è inferiore a *CHANGE, l'accesso non riesce. Se il gruppo dell'utente non dispone di alcuna autorizzazione per la stazione di lavoro, il sistema controlla se l'utente dispone dell'autorizzazione speciale *SERVICE ma non dell'autorizzazione speciale *ALLOBJ.

Se l'utente dispone dell'autorizzazione speciale *SERVICE ma non dell'autorizzazione speciale *ALLOBJ, l'accesso non riesce. Se l'utente dispone dell'autorizzazione speciale *ALLOBJ, il sistema controlla se QSECOFR dispone dell'autorizzazione *CHANGE o superiore.

Se QSECOFR non dispone dell'autorizzazione *CHANGE o superiore, l'accesso non riesce. Se QSECOFR dispone dell'autorizzazione *CHANGE o superiore, l'accesso è consentito.

I profili utente del responsabile della riservatezza (QSECOFR), del servizio (QSRV) e del servizio di base (QSRVBAS) sono sempre abilitati ad accedere alla console. Il valore di sistema QCONSOLE (console) viene utilizzato per determinare l'unità che rappresenta la console. Se il profilo QSRV o QSRVBAS tenta di stabilire un accesso alla console e non dispone dell'autorizzazione *CHANGE, il sistema concede al profilo l'autorizzazione *CHANGE e consente l'accesso.

Proprietà delle descrizioni unità

È possibile specificare la proprietà delle descrizioni unità per controllare l'autorizzazione alle unità.

L'autorizzazione pubblica predefinita sui comandi CRTDEVxxx è *CHANGE. Le unità vengono create nella libreria QSYS, che viene fornita con un valore CRTAUT *SYSVAL. Il valore fornito per il valore di sistema QCRTAUT è *CHANGE.

Per limitare gli utenti che possono collegarsi ad una stazione di lavoro, impostare l'autorizzazione pubblica per la stazione di lavoro su *EXCLUDE e fornire l'autorizzazione *CHANGE a utenti o gruppi specifici.

Al responsabile della riservatezza (QSECOFR) non viene fornita specificatamente l'autorizzazione a delle unità. Se il valore di sistema QLMTSECOFR è impostato su 1 (YES), è necessario fornire l'autorizzazione *CHANGE per le unità al responsabile della riservatezza. Chiunque dispone dell'autorizzazione *OBJMGT e *CHANGE su un'unità, può fornire l'autorizzazione *CHANGE ad un altro utente.

Se una descrizione dell'unità viene creata dal responsabile della riservatezza, quest'ultimo possiede tale unità per la quale gli viene specificatamente assegnata l'autorizzazione *ALL. Quando il sistema configura automaticamente le unità, la maggior parte delle unità sono di proprietà del profilo QPGMR. Le unità create dal programma QLUS (unità di tipo *APPC) sono di proprietà del profilo QSYS.

Se si intende utilizzare il valore di sistema QLMTSECOFR per limitare i collegamenti da parte del responsabile della riservatezza, ogni unità creata deve essere di proprietà di un profilo diverso da QSECOFR.

Per modificare la proprietà di una descrizione dell'unità video, l'unità deve essere accesa e attivata. Collegarsi all'unità e modificare la proprietà utilizzando il comando CHGOBJOWN. Se non si è collegati all'unità, è necessario assegnare l'unità prima di modificarne la proprietà, mediante il comando Assegnazione oggetto (ALCOBJ). È possibile assegnare l'unità solo se nessuno la sta utilizzando. Una volta modificata la proprietà, annullare l'assegnazione dell'unità utilizzando il comando Disallocazione oggetto (DLCOBJ).

File di visualizzazione pannello di accesso

Il responsabile di sistema può modificare il pannello di accesso del sistema per aggiungere il testo o il logo della società al pannello.

Durante la modifica del file di visualizzazione del pannello di accesso, è necessario che l'amministratore di sistema sia certo di non modificare i nomi dei campi o le lunghezze buffer del file di visualizzazione quando si aggiunge un testo al file di visualizzazione. La modifica dei nomi dei campi o delle lunghezze del buffer potrebbero causare un errore nell'accesso.

Modifica visualizzazione pannello di collegamento

È possibile modificare il codice origine per il file di visualizzazione del collegamento per modificare il pannello di collegamento.

Il codice origine per il file di visualizzazione del collegamento viene fornito con il sistema operativo. L'origine viene fornita nel file QSYS/QAWTSSRC. Questo codice origine può essere modificato per aggiungere del testo alla schermata del pannello di collegamento. I nomi dei campi e le lunghezze dei buffer non devono essere modificati.

Origine file di visualizzazione per il pannello accesso

)È necessario copiare il file origine appropriato per creare la propria visualizzazione pannello di accesso.

L'origine per il file di visualizzazione dell'accesso viene fornita come membro (QDSIGNON o QDSIGNON2) nel file fisico QSYS/QAWTSSRC. QDSIGNON contiene l'origine per l'origine del pannello di accesso utilizzato quando il valore di sistema QPWDLVL è impostato su 0 o 1. Il membro QDSIGNON2 contiene l'origine del pannello di accesso utilizzato quando il valore di sistema QPWDLVL è impostato su 2 o 3.

Il file QSYS/QAWTSSRC viene **cancellato e ripristinato** ogni volta che si installa il sistema operativo i5/OS. Se si intende creare la propria versione del pannello di accesso, è necessario copiare prima il membro del file di origine corretto, QDSIGNON o QDSIGNON2, sul proprio file di origine e apportare delle modifiche alla copia presente nel file di origine.

Modifica file pannello di accesso

Questo argomento comprende la procedura di modifica del file pannello di accesso.

Per modificare il formato del pannello di accesso, attenersi alla seguente procedura:

1. Creare un file di visualizzazione del collegamento modificato.

   Per gestire i campi più piccoli, è possibile modificare un campo nascosto nel file di visualizzazione denominato UBUFFER. UBUFFER ha una lunghezza di 128 byte ed è considerato come l'ultimo campo nel file di visualizzazione. Questo campo può essere modificato in modo che agisca come buffer di immissione/emissione; in tal modo i dati specificati in questo campo del pannello saranno disponibili per i programmi delle applicazioni al momento dell'avvio del lavoro interattivo. È possibile modificare il campo UBUFFER in modo che contenga tutti i campi più piccoli necessari qualora si soddisfino i seguenti requisiti:

   - I nuovi campi devono seguire tutti gli altri campi nel file di visualizzazione. La posizione dei campi sul pannello non è importante fino a quando l'ordine in cui appaiono nelle DDS (data description specification) soddisfa questo requisito.
   - La lunghezza totale deve essere 128. Se la lunghezza dei campi supera 128, alcuni dati non verranno inoltrati all'applicazione.
   - Tutti i campi devono essere campi immissione/emissione (immettere B nell'origine DDS) o campi nascosti (immettere H nell'origine DDS).
2. L'ordine in cui vengono dichiarati i campi nel file di visualizzazione del collegamento non deve essere modificato. La posizione in cui vengono visualizzati nel pannello può essere modificata. Non modificare i nomi dei campi esistenti nell'origine per il file di visualizzazione del pannello di collegamento.
3. Non modificare la dimensione totale dei buffer di immissione o di emissione. È possibile che si verifichino dei problemi seri qualora si modifichi l'ordine o la dimensione dei buffer.
4. Non utilizzare la funzione di aiuto delle DDS (data descriptions specifications) nel file di visualizzazione del collegamento.
5. Modificare la descrizione di un sottosistema per utilizzare il file di visualizzazione modificato invece del valore di sistema predefinito QSYS/QDSIGNON. È possibile modificare le descrizioni del sottosistema per quei sottosistemi in cui si desidera utilizzare il nuovo pannello. Per modificare la descrizione del sottosistema, attenersi alla seguente procedura:
   a. Utilizzare il comando CHGSBSD (Modifica descrizione sottosistema).
   b. Specificare il nuovo file di visualizzazione sul parametro SGNDSPF.
   c. Utilizzare una versione di verifica di un sottosistema per controllare la validità del pannello prima di tentare di modificare il sottosistema di controllo.
6. Verificare la modifica.
7. Modificare le altre descrizioni del sottosistema.

Note:

1. La lunghezza del buffer per il file di visualizzazione deve essere 318. Qualora fosse inferiore a 318, il sottosistema utilizza il pannello di collegamento predefinito QDSIGNON nella libreria QSYS quando il valore di sistema QPWDLVL è impostato su 0 o 1 e QDSIGNON2 nella libreria QSYS quando QPWDLVL è impostato su 2 o 3.
2. La riga del copyright non può essere cancellata.

Descrizioni sottosistema

Le descrizioni sottosistema eseguono diverse funzioni sul sistema.

Controllo descrizioni sottosistema:

- Modalità di inserimento dei lavori nel sistema
- Modalità di avvio dei lavori
- Caratteristiche delle prestazioni dei lavori

Solo alcuni utenti possono essere autorizzati alla modifica delle descrizioni del sottosistema e le modifiche devono essere controllate molto attentamente.

Concetti correlati

"Accesso senza ID utente e parola d'ordine" a pagina 17
Il livello di sicurezza determina la modalità di controllo, da parte del sistema, dell'accesso senza un ID utente e una parola d'ordine.

Controllo dell'inserimento dei lavori nel sistema

È possibile utilizzare le descrizioni sottosistema per controllare la modalità di inserimento dei lavori nel sistema.

Diverse descrizioni del sottosistema vengono fornite con il sistema. Una volta modificato il livello di sicurezza (valore di sistema QSECURITY) sul livello 20 o uno superiore, non è consentito l'accesso sprovvisto di ID utente e parola d'ordine nei sottosistemi forniti da IBM.

Tuttavia, è possibile eseguire la definizione della descrizione di un sottosistema e di una combinazione della descrizione del lavoro che consente l'accesso predefinito (senza ID utente e parola d'ordine) anche se rappresenta un rischio per la sicurezza. Quando il sistema instrada un lavoro interattivo, viene considerata la stazione di lavoro presente nella descrizione del sottosistema per una descrizione lavoro. Se la descrizione del lavoro specifica USER(*RQD), l'utente deve immettere un ID utente valido (e una parola d'ordine) sul pannello Accesso. Se la descrizione del lavoro specifica un profilo utente nel campo *Utente*, chiunque può premere il tasto Invio per collegarsi come tale utente.

A livelli di sicurezza 30 e superiori, il sistema registra una voce (immettere AF, sottotipo S) nel giornale di controllo, se si tenta l'accesso predefinito e la funzione di controllo è attiva. Al livello di sicurezza 40 e superiore, il sistema non consente l'accesso predefinito, anche se esiste una combinazione di voci di stazioni di lavoro e descrizioni lavoro che lo consentirebbe. Consultare "Accesso senza ID utente e parola d'ordine" a pagina 17 per ulteriori informazioni.

Accertarsi che tutte le voci delle stazioni di lavoro per i sistemi interattivi facciano riferimento alle descrizioni del lavoro con USER(*RQD). Controllare l'autorizzazione per modificare le descrizioni del lavoro e monitorare le modifiche apportate alle descrizioni del lavoro. Se la funzione di controllo è attiva, il sistema scrive una voce di giornale di tipo JD ogni volta che il parametro USER in una descrizione lavoro viene modificato.

Le voci delle comunicazioni in una descrizione del sottosistema controllano la modalità di inserimento dei lavori delle comunicazioni nel sistema. Una voce delle comunicazioni punta ad un profilo utente predefinito, che consente l'avvio di un lavoro senza un ID utente e la parola d'ordine. Questo rappresenta un rischio per la sicurezza. Valutare le voci delle comunicazioni sul sistema e utilizzare gli attributi di rete per controllare la modalità di inserimenti dei lavori delle comunicazioni nel sistema. "Attributi di rete" a pagina 229 tratta gli attributi di rete che sono importanti per la sicurezza.

Descrizioni lavoro

Una descrizione lavoro è uno strumento variabile per la sicurezza e la gestione del lavoro.

È possibile inoltre impostare la descrizione del lavoro per un gruppo di utenti che necessitano dello stesso elenco di librerie iniziale, coda di emissione e coda lavori. È possibile impostare una descrizione lavoro per un gruppo di lavori batch con requisiti simili.

Una descrizione lavoro rappresenta inoltre un possibile pericolo per la sicurezza. In alcuni casi, una descrizione lavoro che specifica un nome profilo per il parametro USER può permettere ad un lavoro di immettersi nel sistema senza il controllo della sicurezza appropriata. "Controllo dell'inserimento dei lavori nel sistema" a pagina 220 tratta come impedire ciò per i lavori interattivi e di comunicazioni.

Quando si inoltra un lavoro batch, il lavoro potrebbe essere eseguito utilizzando un profilo diverso dall'utente che ha inoltrato il lavoro. Il profilo può essere specificato sul comando SBMJOB oppure potrebbe provenire dal parametro USER della descrizione lavoro. Se il sistema è ad un livello di sicurezza (valore di sistema QSECURITY) 30 o inferiore, l'utente che inoltra un lavoro necessita dell'autorizzazione sulla descrizione del lavoro ma non sul profilo utente specificato sulla descrizione del lavoro. Questo rappresenta un rischio per la sicurezza. Al livello della sicurezza 40 e superiore, il mittente necessita dell'autorizzazione sia sulla descrizione del lavoro che sul profilo utente.

Ad esempio:

- USERA non è autorizzato al file PAYROLL.
- USERB dispone dell'autorizzazione *USE sul file PAYROLL e sul programma PRLIST, che elenca il file PAYROLL.
- La descrizione del lavoro PRJOBD specifica USER(USERB). L'autorizzazione pubblica per PRJOBD è *USE.

Al livello di sicurezza 30 o inferiore, USERA può elencare il file payroll inoltrando un lavoro batch:

```
SBMJOB RQSDTA("Call PRLIST") JOBD(PRJOBD) +
                       USER(*JOBD)
```

È possibile impedire questo inconveniente utilizzando un livello di sicurezza 40 e superiore oppure controllando l'autorizzazione alle descrizioni lavoro che specificano un profilo utente.

Alcune volte, è necessario immettere un nome profilo utente specifico in una descrizione lavoro affinché determinati tipi di lavoro batch funzionino correttamente. Ad esempio, la descrizione del lavoro QBATCH viene fornita con USER(QPGMR). Questa descrizione lavoro viene fornita con l'autorizzazione pubblica *EXCLUDE.

Se il sistema è ad un livello di sicurezza 30 o inferiore, ogni utente sul sistema che dispone dell'autorizzazione per il comando Inoltro lavoro (SBMJOB) o per i comandi di avvio del programma di lettura e che dispone dell'autorizzazione *USE per la descrizione lavoro QBATCH, può inoltrare il lavoro con il profilo utente del programmatore (QPGMR), se l'utente dispone dell'autorizzazione per il profilo QPGMR. Al livello della sicurezza 40 e superiore, viene richiesta anche l'autorizzazione *USE sul profilo QPGMR.

Coda messaggi dell'operatore di sistema

È possibile specificare le autorizzazioni per controllare l'accesso alla coda messaggi dell'operatore di sistema

Il menu Operational Assistant (ASSIST) di i5/OS fornisce un'opzione per la gestione del sistema, degli utenti e delle unità. Il menu Gestione del sistema, utenti ed unità fornisce un'opzione per la gestione dei messaggi dell'operatore di sistema. È possibile desiderare di impedire agli utenti di rispondere ai messaggi nella coda messaggi QSYSOPR (operatore di sistema). Risposte non corrette ai messaggi dell'operatore di sistema possono causare problemi al sistema.

Per rispondere ai messaggi sono necessarie le autorizzazioni *USE e *ADD alla coda messaggi. La rimozione dei messaggi richiede le autorizzazioni *USE e *DLT (Consultare Comandi messaggi.) Fornire l'autorizzazione per rispondere e rimuovere i messaggi in QSYSOPR solo agli utenti con responsabilità di operatore di sistema. L'autorizzazione pubblica per QSYSOPR dovrebbe essere *OBJOPR e *ADD, che consente di aggiungere nuovi messaggi a QSYSOPR.

Attenzione: tutti i lavori devono poter aggiungere nuovi messaggi alla coda messaggi QSYSOPR. Non impostare l'autorizzazione pubblica per QSYSOPR *EXCLUDE.

Elenchi librerie

L'**elenco librerie** per un lavoro indica le librerie in cui effettuare le ricerche e l'ordine in cui le ricerche devono essere effettuate.

Quando un programma specifica un oggetto, l'oggetto può essere specificato con un nome qualificato, che comprende sia il nome dell'oggetto che il nome della libreria. In alternativa, la libreria per l'oggetto può essere specificata come *LIBL (elenco librerie). Le ricerche vengono effettuate nelle librerie presenti nell'elenco librerie, in ordine, fino a quando l'oggetto non viene trovato.

La Tabella 123 riepiloga le parti dell'elenco librerie e le procedure di creazione delle parti durante un lavoro. Le sezioni seguenti trattano i rischi e le misure di protezione per gli elenchi di librerie.

Tabella 123. Parti dell'elenco librerie. Le ricerche nell'elenco librerie vengono eseguite in questa sequenza:

Parte	Come viene creata
15 voci parte sistema	Inizialmente creata utilizzando il valore di sistema QSYSLIBL. Può essere modificata durante l'esecuzione di un lavoro con il comando CHGSYSLIBL.
2 voci parte libreria prodotto	Spazio vuoto iniziale. Una libreria viene aggiunta alla parte della libreria del prodotto dell'elenco librerie quando si esegue un comando o un menu che è stato creato con una libreria nel parametro PRDLIB. La libreria rimane nella parte della libreria del prodotto dell'elenco librerie fino a quando il comando o il menu non termina.
1 voce libreria corrente	Specificata nel profilo utente o sul pannello Accesso. Può essere modificata quando si esegue un comando o un menu che specifica una libreria per il parametro CURLIB. Può essere modificata nel lavoro con il comando CHGCURLIB.
20 voci parte utente	Create inizialmente utilizzando l'elenco librerie iniziale dalla descrizione del lavoro dell'utente. Se la descrizione del lavoro specifica *SYSVAL, si utilizza il valore di sistema QUSRLIBL. Durante un lavoro, la parte utente dell'elenco di librerie può essere modificata con i comandi ADDLIBLE, RMVLIBLE, CHGLIBL e EDTLIBL.

Concetti correlati

"Sicurezza libreria ed elenchi di librerie" a pagina 146
Quando una libreria viene aggiunta ad un elenco di librerie dell'utente, l'autorizzazione di cui dispone l'utente sulla libreria viene memorizzata con le informazioni dell'elenco di librerie.

"Pianificazione delle librerie" a pagina 241
Una libreria è come un indirizzario utilizzato per individuare gli oggetti nella libreria. Molti fattori influenzano la scelta su come raggruppare le informazioni relative all'applicazione in librerie e su come gestire queste librerie.

Rischi sicurezza degli elenchi librerie

Questo argomento fornisce esempi specifici dei possibili rischi relativi alla sicurezza degli elenchi librerie e spiega come evitarli.

Gli elenchi librerie rappresentano un potenziale rischio per la sicurezza. Se un utente è in grado di modificare la sequenza delle librerie sull'elenco librerie o di aggiungere ulteriori librerie all'elenco, l'utente è in grado di eseguire funzioni che interrompono i requisiti di sicurezza.

"Sicurezza libreria ed elenchi di librerie" a pagina 146 fornisce alcune informazioni generali sui problemi associati agli elenchi delle librerie.

Questa sezione fornisce due esempi di come le modifiche apportate ad un elenco di librerie possono interrompere i requisiti della sicurezza.

Modifica nella funzione

Questo esempio illustra il rischio di una modifica nella funzione quando si richiama un programma nella libreria.

La Figura 29 mostra una libreria delle applicazioni. Il Programma A richiama il Programma B, che si suppone sia in LIBA. Il Programma B esegue gli aggiornamenti del File A. Il Programma B viene richiamato senza un nome qualificato in modo che vengano eseguite delle ricerche nell'elenco delle librerie fino a quando non si trova il Programma B.

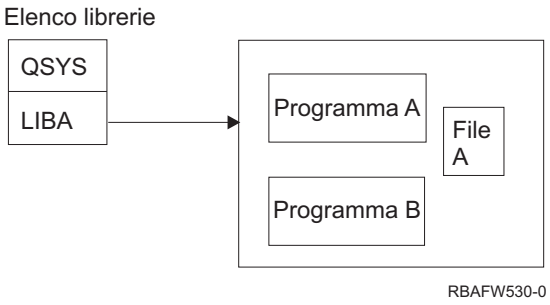


Figura 29. Ambiente supposto elenco libreria

Un programmatore oppure un altro utente esperto potrebbe inserire un altro Programma B nella libreria LIBB. Il programma di sostituzione potrebbe eseguire funzioni diverse, come ad esempio la copia di informazioni confidenziali o l'aggiornamento di file in maniera non corretta. Se LIBB è inserita in testa a LIBA nell'elenco di librerie, il Programma B di sostituzione viene eseguito al posto del Programma B originale, poiché il programma viene richiamato senza un nome qualificato:

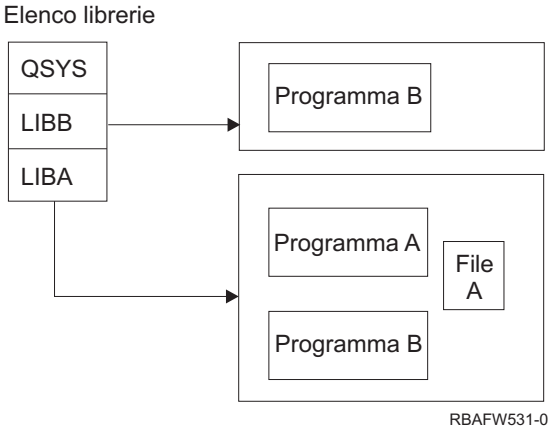


Figura 30. Ambiente attuale elenco libreria

Accesso non autorizzato alle informazioni

L'esempio illustra il rischio potenziale di un accesso non autorizzato alle informazioni presenti nella libreria.

Supponiamo che il Programma A nella Figura 29 adotti l'autorizzazione di USER1, che dispone dell'autorizzazione *ALL sul File A. Supponiamo che il Programma B venga richiamato dal Programma A

(l'autorizzazione adottata continua ad essere applicata). Un utente esperto può creare un Programma B di sostituzione che richiama semplicemente il processore del comando. L'utente dovrebbe avere una riga comandi e l'accesso completo al File A.

Suggerimenti per la parte di sistema dell'elenco librerie

Questo argomento fornisce i suggerimenti per la parte di sistema dell'elenco librerie.

La parte del sistema dell'elenco di librerie è stata concepita per le librerie fornite da IBM. Le librerie delle applicazioni attentamente controllate possono essere inserite anche nella parte di sistema dell'elenco di librerie. La parte di sistema dell'elenco di librerie rappresenta il rischio maggiore per la sicurezza, poiché le ricerche vengono effettuate prima nelle librerie presenti in questa parte dell'elenco.

Solo un utente con l'autorizzazione speciale *ALLOBJ e *SECADM può modificare il valore di sistema QSYSLIBL. Controllare e monitorare le modifiche apportate alla parte di sistema dell'elenco di librerie. Di seguito vengono riportate delle linee guida per l'aggiunta di librerie:

- Solo le librerie che vengono controllate specificatamente possono essere inserite in questo elenco.
- Il pubblico non dovrebbe disporre dell'autorizzazione *ADD su queste librerie.
- Alcune librerie fornite da IBM, quale ad esempio QGPL, vengono fornite con l'autorizzazione pubblica *ADD per motivi di produzione. Monitorare regolarmente gli oggetti (soprattutto i programmi, i file di origine e i comandi) che vengono aggiunti a queste librerie.

Il comando CHGSYSLIBL viene inviato con l'autorizzazione pubblica *EXCLUDE. Solo gli utenti che dispongono dell'autorizzazione *ALLOBJ possono utilizzare il comando, a meno che non si concede l'autorizzazione ad altri utenti. Se la libreria di sistema deve essere modificata temporaneamente durante un lavoro, è possibile utilizzare la tecnica descritta nell'argomento "Modifica elenco librerie di sistema" a pagina 243.

Suggerimenti per la libreria prodotto

In questo argomento vengono forniti i suggerimenti per la protezione della libreria del prodotto.

Le ricerche vengono effettuate prima nella parte della libreria prodotto dell'elenco di librerie e poi nella parte utente. Un utente esperto potrebbe creare un comando o un menu che inserisce una libreria prodotto nell'elenco librerie. Ad esempio, questa istruzione CMDX, che esegue il programma PGMA:

```
CRTCMD CMDX PGM(PGMA) PRDLIB(LIBB)
```

Fino a quando CMDX è in esecuzione, LIBB è nella parte prodotto dell'elenco librerie.

Utilizzare questi accorgimenti per proteggere la parte prodotto dell'elenco librerie:

- Controllare l'autorizzazione sui comandi Creazione comando (CRTCMD), Modifica comando (CHGCMD), Creazione menu (CRTMNU) e Modifica menu (CHGMNU).
- Quando si creano i comandi e i menu, specificare PRDLIB(*NONE), che elimina le voci attualmente presenti nella parte prodotti dell'elenco di librerie. Questo consente di impedire le ricerche nelle librerie sconosciute in testa alla libreria prevista quando si esegue il comando o il menu.

  Nota: il valore predefinito utilizzato quando si crea un comando o un menu è PRDLIB(*NOCHG). *NOCHG indica che quando si esegue il comando o il menu, la parte della libreria dei prodotti dell'elenco di librerie non viene modificata.

Suggerimenti per la libreria corrente

Questo argomento fornisce suggerimenti per garantire la sicurezza del sistema quando si utilizza la libreria corrente.

La libreria corrente può essere utilizzata da strumenti di supporto alla decisione, come ad esempio Query/400. I programmi query creati da un utente sono, per impostazione predefinita, inseriti nella libreria corrente dell'utente. Quando si crea un menu o un comando, è possibile specificare una librerie corrente da utilizzare quando il menu è attivo.

La libreria corrente fornisce all'utente e al programmatore un metodo semplice che consente di creare nuovi oggetti, quali ad esempio i programmi query, senza doversi preoccupare della posizione di destinazione. Tuttavia, la libreria corrente pone un rischio per la sicurezza, poiché le ricerche vengono effettuate prima nella libreria e poi nella parte utente dell'elenco librerie. È possibile prendere diverse precauzioni per proteggere la sicurezza del sistema mentre si sta utilizzando ancora le funzioni della libreria corrente:

- Specificare *YES per il campo *Possibilità limitate* nel profilo utente. Ciò impedisce ad un utente di modificare la libreria corrente sul pannello Accesso o utilizzando il comando CHGPRF.
- Limitare l'autorizzazione sui comandi Modifica libreria corrente (CHGCURLIB), Creazione menu (CRTMNU), Modifica menu (CHGMNU), Creazione comando (CRTCMD) e Modifica comando (CHGCMD).
- Utilizzare la tecnica descritta in "Controllo elenco librerie utente" a pagina 243 per impostare la libreria corrente durante l'elaborazione dell'applicazione.

Suggerimenti per la parte utente dell'elenco librerie

In questo argomento vengono forniti i suggerimenti per il controllo della parte utente dell'elenco librerie.

La parte utente dell'elenco librerie spesso si modifica più delle altre parti ed è più difficile da controllare. Molti programmi delle applicazioni modificano l'elenco librerie. Le descrizioni dei lavori coinvolgono inoltre l'elenco di librerie per un lavoro.

Di seguito vengono riportate alcune alternative per il controllo della parte utente dell'elenco librerie per accertarsi che le librerie non autorizzate con i file e i programmi di sostituzione non vengano utilizzate durante l'elaborazione:

- Limitare gli utenti delle applicazioni di produzione ad un ambiente di menu. Impostare il campo *Possibilità limitate* nei profili utente su *YES, per limitare gli utenti nell'inserimento dei comandi. "Pianificazione dei menu" a pagina 245 fornisce un esempio di tale ambiente.
- Utilizzare i nomi qualificati (oggetto e libreria) nelle applicazioni. Ciò impedisce che il sistema effettui le ricerche nell'elenco di librerie per trovare un oggetto.
- Controllare la possibilità di modificare le descrizioni dei lavori, poiché la descrizione del lavoro imposta l'elenco di librerie iniziale per un lavoro.
- Utilizzare il comando Aggiunta voce elenco librerie (ADDLIBLE) all'inizio del programma per assicurarsi che gli oggetti desiderati siano all'inizio della parte utente dell'elenco librerie. Una volta completato il programma, la libreria può essere rimossa.

  Se la libreria è già presente nell'elenco di librerie, ma non si è certi se si trova all'inizio dell'elenco, è necessario rimuovere la libreria e aggiungerla. Se la sequenza dell'elenco di librerie è importante per altre applicazioni sul sistema, utilizzare il metodo successivo.
- Utilizzare un programma che richiama e salva l'elenco di librerie per un lavoro. Sostituire l'elenco librerie con l'elenco desiderato per l'applicazione. Una volta terminata l'applicazione, riportare l'elenco di librerie all'impostazione originale. Consultare "Controllo elenco librerie utente" a pagina 243 per un esempio di questa tecnica.

Stampa

È possibile controllare la sicurezza delle code di emissione sul sistema.

La maggior parte delle informazioni stampate sul sistema, viene ripristinata come file di spool su una coda di emissione mentre è in attesa della stampa. A meno che non si controlli la sicurezza delle code di emissione sul sistema, gli utenti non autorizzati possono visualizzare, stampare e persino copiare le informazioni confidenziali in attesa di essere stampate.

Un metodo per la protezione dell'emissione confidenziale consiste nel creare una coda di emissione speciale. Inviare l'emissione confidenziale alla coda di emissione e controllare chi può visualizzare e manipolare i file di spool sulla coda di emissione.

Per stabilire la direzione dell'emissione, il sistema controlla il file della stampante, gli attributi del lavoro, il profilo utente, la descrizione dell'unità della stazione di lavoro e il valore di sistema dell'unità di stampa (QPRTDEV), in sequenza. Se si utilizzano i valori predefiniti, viene utilizzata la coda di emissione associata alla stampante QPRTDEV. L'argomento Advanced Function Presentation fornisce esempi su come indirizzare l'emissione ad una particolare coda di emissione.

Protezione file di spool

È possibile specificare diversi parametri per controllare la sicurezza di un file di spool.

Un file di spool è un tipo di oggetto speciale sul sistema. Non è possibile concedere e revocare direttamente l'autorizzazione per poter visualizzare e manipolare un file di spool. L'autorizzazione su un file di spool viene controllata da diversi parametri sulla coda di emissione che conserva il file di spool.

Quando si crea un file di spool, l'utente è il proprietario di quel file. È sempre possibile visualizzare e manipolare i file di spool di proprietà, senza considerare come viene definita l'autorizzazione per la coda di emissione. È necessario disporre dell'autorizzazione *READ per aggiungere le nuove voci ad una coda di emissione. Se l'autorizzazione su una coda di emissione viene rimossa, è possibile accedere ancora alle voci possedute su tale coda, utilizzando il comando Gestione file di spool (WRKSPLF).

I parametri della sicurezza per una coda di emissione vengono specificati utilizzando il comando Creazione coda emissione (CRTOUTQ) o Modifica coda emissione (CHGOUTQ). È possibile visualizzare i parametri della sicurezza di una coda di emissione utilizzando il comando Gestione descrizione coda di emissione (WRKOUTQD).

Attenzione: un utente con l'autorizzazione speciale *SPLCTL può eseguire tutte le funzioni su tutte le voci, senza tenere conto di come viene definita la coda di emissione. Alcuni parametri sulla coda di emissione consentono ad un utente con autorizzazione speciale *JOBCTL di visualizzare il contenuto delle voci sulla coda di emissione.

Parametro DSPDTA (visualizzazione dati) della coda di emissione

È possibile specificare il parametro DSPDTA (visualizzazione dati) per proteggere il contenuto di un file di spool.

Il parametro DSPDTA determina l'autorizzazione richiesta per eseguire le seguenti funzioni sui file di spool posseduti da altri utenti:

- Visualizzare il contenuto di un file di spool (comando DSPSPLF)
- Copia file di spool (comando CPYSPLF)
- Invio file in spool (comando SNDNETSPLF)
- Spostare un file di spool su un'altra coda di emissione (comando CHGSPLFA)

Valori possibili per DSPDTA	
***NO**	Un utente non può visualizzare, inviare o copiare i file di spool di proprietà di altri utenti, a meno che l'utente non disponga delle seguenti autorizzazioni: • Autorizzazione speciale *JOBCTL se il parametro OPRCTL è *YES. • Autorizzazione *READ, *ADD e *DLT sulla coda di emissione se il parametro *AUTCHK è *DTAAUT. • Proprietà della coda di emissione se il parametro *AUTCHK è *OWNER.
***YES**	Ogni utente con l'autorizzazione *READ sulla coda di emissione può visualizzare, copiare o inviare i dati dei file di spool di proprietà di altri.
***OWNER**	Solo il proprietario di un file di spool o un utente con l'autorizzazione *SPLCTL (controllo di spool) può visualizzare, copiare inviare o spostare il file. Se il valore OPRCTL è *YES, gli utenti con l'autorizzazione speciale *JOBCTL possono conservare, modificare, cancellare e rilasciare i file di spool sulla coda di emissione ma non possono visualizzare, copiare, inviare o spostare i file di spool. Ciò consente agli operatori di gestire le voci su una coda di emissione senza poter visualizzarne il contenuto.

Parametro Autorizzazione da verificare (AUTCHK) della coda di emissione

È possibile utilizzare il parametro Autorizzazione da verificare (AUTCHK) per controllare l'autorizzazione dell'utente a modificare o cancellare un file di spool sul proprio sistema.

Il parametro AUTCHK determina se l'autorizzazione *READ, *ADD e *DLT sulla coda di emissione consente ad un utente di modificare e cancellare i file di spool di proprietà di altri utenti.

Valori possibili per AUTCHK	
***OWNER**	Solo l'utente che possiede la coda di emissione può modificare o cancellare i file di spool di proprietà di altri.
***DTAAUT**	Specifica che ogni utente con autorizzazione *READ, *ADD e *DLT sulla coda di emissione può modificare o cancellare i file di spool di proprietà di altri.

Parametro Controllo operatore (OPRCTL) della coda di emissione

Il parametro Controllo operatore (OPRCTL) stabilisce se un utente con l'autorizzazione speciale *JOBCTL può controllare la coda di emissione.

Valori possibili per OPRCTL	
***YES**	Un utente con l'autorizzazione speciale *JOBCTL può eseguire tutte le funzioni sui file di spool, a meno che il valore di DSPDTA non sia *OWNER. Se il valore di DSPDTA è *OWNER, l'autorizzazione speciale *JOBCTL non consente all'utente di visualizzare, copiare, inviare o spostare i file di spool.
***NO**	L'autorizzazione speciale *JOBCTL non fornisce all'utente l'autorizzazione per eseguire le operazioni sulla coda di emissione. Le normali regola di autorizzazione si applicano all'utente.

Coda di emissione e autorizzazioni parametro richieste per la stampa

Questo argomento include le informazioni di riferimento sui parametri della coda di emissione e sulle autorizzazioni richieste per eseguire le funzioni di gestione di stampa.

La Tabella 124 a pagina 228 mostra quale combinazione di parametri coda di emissione e autorizzazione sulla coda di emissione è necessaria per eseguire le funzioni di gestione della stampa sul sistema. Per alcune funzioni, viene elencata più di una combinazione. Il proprietario di un file di spool può eseguire sempre tutte le funzioni su quel file. Per ulteriori informazioni consultare "Comandi programma di scrittura" a pagina 526.

L'autorizzazione e i parametri della coda di emissione per tutti i comandi associati ai file di spool, vengono elencati in "Comandi file di spool" a pagina 510. I comandi della coda di emissione vengono elencati in "Comandi coda di emissione" a pagina 482.

Attenzione: Un utente con l'autorizzazione speciale *SPLCTL (controllo spool) non è soggetto ad alcuna limitazione di autorizzazione associata alle coda di emissione. L'autorizzazione speciale *SPLCTL consente all'utente di eseguire tutte le operazioni sulle code di emissione. Valutare attentamente la possibilità di fornire l'autorizzazione speciale *SPLCTL a ciascun utente.

Tabella 124. Autorizzazione richiesta per eseguire le funzioni di stampa

Funzione di stampa	Parametri coda di emissione			Autorizzazione coda di emissione	Autorizzaz. speciale
	DSPDTA	AUTCHK	OPRCTL		
Aggiungere i file di spool alla coda [1]				*READ	Nessuna
			*YES		*JOBCTL
Visualizzare un elenco dei file di spool (comando WRKOUTQ [2])				*READ	Nessuna
			*YES		*JOBCTL
Visualizzare, copiare o inviare file di spool (DSPSPLF, CPYSPLF, SNDNETSPLF, SNDTCPSP[2])	*YES			*READ	Nessuna
	*NO	*DTAAUT		*READ, *ADD, *DLT	Nessuna
	*NO	*OWNER		Proprietario [3]	Nessuna
	*YES		*YES		*JOBCTL
	*NO		*YES		*JOBCTL
	*OWNER				
Modificare, cancellare, conservare e rilasciare il file di spool (CHGSPLFA, DLTSPLF, HLDSPLF, RLSSPLF [2])		*DTAAUT		*READ, *ADD, *DLT	Nessuna
		*OWNER		Proprietario [3]	Nessuna
			*YES		*JOBCTL
Modificare, cancellare, conservare e rilasciare la coda di emissione (CHGOUTQ, CLROUTQ, HLDOUTQ, RLSOUTQ [2])		*DTAAUT		*READ, *ADD, *DLT	Nessuna
		*OWNER		Proprietario [3]	Nessuna
			*YES		*JOBCTL
Avviare un programma di scrittura per la coda (STRPRTWTR, STRRMTWTR [2])		*DTAAUT		*CHANGE	Nessuna
			*YES		*JOBCTL

[1] Questa è l'autorizzazione richiesta per indirizzare l'emissione su una coda di emissione.

[2] Utilizzare questi comandi o le opzioni equivalenti da un pannello.

[3] È necessario essere il proprietario della coda di emissione.

[4] Richiede inoltre l'autorizzazione *USE alla descrizione dell'unità di stampa.

[5] *CHGOUTQ richiede l'autorizzazione *OBJMGT sulla coda di emissione, oltre alle autorizzazioni *READ, *ADD e *DLT.

Esempi: Coda di emissione

Questi esempi dimostrano come impostare i parametri della sicurezza per le code di emissione in modo da soddisfare requisiti diversi.

- Creare una coda di emissione a scopo generale. Tutti gli utenti sono abilitati alla visualizzazione di tutti i file di spool. Gli operatori di sistema possono gestire la coda e modificare i file di spool:

```
CRTOUTQ OUTQ(QGPL/GPOUTQ) DSPDTA(*YES) +
        OPRCTL(*YES) AUTCHK(*OWNER) AUT(*USE)
```

- Creare una coda di emissione per un'applicazione. Solo i membri del profilo gruppo GRPA sono autorizzati all'utilizzo della coda di emissione. Tutti gli utenti autorizzati della coda di emissione sono autorizzati alla visualizzazione di tutti i file di spool. Gli operatori di sistema non sono autorizzati a gestire la coda di emissione:

```
CRTOUTQ OUTQ(ARLIB/AROUTQ) DSPDTA(*YES) +
        OPRCTL(*NO) AUTCHK(*OWNER) AUT(*EXCLUDE)
GRTOBJAUT OBJ(ARLIB/AROUTQ) OBJTYP(*OUTQ) +
        USER(GRPA)  AUT(*CHANGE)
```

- Creare una coda di emissione confidenziale per i responsabili della riservatezza da utilizzare durante la stampa delle informazioni sui profili utente e le autorizzazioni. La coda di emissione viene creata dal profilo QSECOFR che è anche il proprietario.

```
CRTOUTQ OUTQ(QGPL/SECOUTQ) DSPDTA(*OWNER) +
        AUTCHK(*DTAAUT) OPRCTL(*NO) +
        AUT(*EXCLUDE)
```

  Anche se i responsabili della riservatezza di un sistema dispongono dell'autorizzazione speciale *ALLOBJ, essi non sono in grado di accedere ai file di spool di proprietà di altri sulla coda di emissione SECOUTQ.

- Creare una coda di emissione condivisa dagli utenti che stampano file e documenti confidenziali. Gli utenti possono gestire solo i loro file di spool. Gli operatori di sistema possono gestire i file di spool, ma non possono visualizzare il contenuto dei file.

```
CRTOUTQ OUTQ(QGPL/CFOUTQ) DSPDTA(*OWNER) +
        AUTCHK(*OWNER) OPRCTL(*YES) AUT(*USE)
```

Attributi di rete

Gli attributi di rete controllano le modalità di comunicazione del sistema con altri sistemi.

Alcuni attributi di rete controllano la modalità di elaborazione dei lavori da parte delle richieste remoto e la modalità di gestione delle informazioni di accesso. Questi attributi di rete coinvolgono direttamente la sicurezza sul sistema e vengono trattati negli argomenti seguenti:

- Azione lavoro (JOBACN)
- Accesso richiesta Client (PCSACC)
- Accesso richiesta DDM (DDMACC)

Vengono visualizzati i possibili valori per ciascun attributo di rete. Il valore predefinito è sottolineato. Per impostare il valore di un attributo di rete, utilizzare il comando Modifica attributo di rete (CHGNETA).

Attributo di rete JOBACN (azione lavoro)

L'attributo di rete JOBACN determina come il sistema elabora le richieste in entrata per l'esecuzione dei lavori.

Valori possibili per JOBACN:	
***REJECT**	Il flusso di immissione viene rifiutato. Un messaggio che descrive il flusso di immissione viene inviato sia al mittente che al destinatario preposto.
***FILE**	Il flusso di immissione viene archiviato sulla coda dei file di rete per l'utente ricevente. Questo utente può visualizzare, annullare o ricevere il flusso di immissione in un file di database oppure inoltrarlo ad una coda lavori. Un messaggio che afferma che il flusso di immissione è stato archiviato sia al mittente che al ricevente.

Valori possibili per JOBACN:	
***SEARCH**	La tabella dei lavori di rete controlla le azioni utilizzando il valori presenti nella tabella.

Suggerimenti:

Se non si prevede la ricezione di richieste di lavori remote sul sistema, impostare l'attributo di rete JOBACN su *REJECT.

Informazioni correlate

SNA Distribution Services

Attributo di rete PCSACC (Accesso richiesta client)

L'attributo di rete PCSACC determina stabilisce come il programma su licenza System i Access per Windows elabora richieste di accesso agli oggetti provenienti da personal computer collegati.

L'attributo di rete PCSACC controlla se i lavori del personal computer possono accedere agli oggetti sulla piattaforma System i, ma non controlla se il personal computer può utilizzare l'emulazione della stazione di lavoro.

Nota: l'attributo di rete PCSACC controlla solo i client DOS e OS/2. Non influenza altri client System i Access .

Valori possibili per PCSACC:	
***REJECT**	System i Access rifiuta ogni richiesta, proveniente dal personal computer, di accesso agli oggetti sulla piattaforma System i. Un messaggio di errore viene inviato all'applicazione PC.
***OBJAUT**	I programmi System i Access presenti sul sistema verificano le normali autorizzazioni oggetto per ciascun oggetto richiesto da un programma PC. Ad esempio, se è richiesto il trasferimento file, viene controllata l'autorizzazione alla copia dei dati dal file di database.
***REGFAC**	Il sistema utilizza la funzione di registrazione del sistema per stabilire il programma di uscita (se presente) da eseguire. Se non viene definito alcun programma di uscita per un punto di uscita ed è stato specificato questo valore, si utilizza *OBJAUT.
nome- programma- qualificato	Il programma System i Access richiama questo programma di uscita scritto dall'utente per stabilire se rifiutare o meno la richiesta PC. Il programma di uscita viene richiamato solo se il normale controllo dell'autorizzazione per l'oggetto ha esito positivo. Il programma System i Access inoltra le informazioni sull'utente e la funzione richiesta al programma di uscita. Il programma restituisce un codice che indica se la richiesta deve essere accettata o rifiutata. Se il codice di ritorno indica che la richiesta deve essere rifiutata o se si verifica un errore, un messaggio di errore viene inviato al personal computer.

Rischi e suggerimenti

Utilizzare le istruzioni presenti in questo argomento per proteggere i file sul sistema.

Le normali misure di sicurezza sul sistema potrebbero non essere sufficienti se il programma System i è installato sul sistema. Ad esempio, se un utente dispone dell'autorizzazione *USE su un file e l'attributo di rete PCSACC è *OBJAUT, l'utente può utilizzare il programma System i Access e un programma sul personal computer per trasferire quell'intero file al personal computer. L'utente può quindi copiare i dati su un'unità minidisco o nastro del PC e rimuoverlo dall'ubicazione.

Sono disponibili diversi metodi per impedire ad un utente System i con autorizzazione *USE su un file, di copiare il file:

- Impostare LMTCPB(*YES) nel profilo utente.
- Limitare l'autorizzazione ai comandi che copiano i file.
- Limitare l'autorizzazione sui comandi utilizzati da System i Access.
- Non fornire all'utente l'autorizzazione *ADD su ciascuna libreria. L'autorizzazione *ADD viene richiesta per creare un nuovo file in una libreria.
- Non fornire all'utente l'accesso all'unità *SAVRST.

Nessuno di questi metodi è adatto per l'utente PC del programma su licenza System i Access. L'utilizzo di un programma di uscita per la verifica di tutte le richieste rappresenta l'unica misura di protezione adeguata.

Il programma System i Access inoltra le informazioni per i seguenti tipi di accesso al programma di uscita dell'utente richiamato dall'attributo di rete PCSACC:

- Trasferimento file
- Stampa virtuale
- Messaggio
- Cartella condivisa

Informazioni correlate

Programmazione: iSeries Access

Attributo di rete DDMACC (Accesso richiesta DDM)

L'attributo di rete DDMACC (Accesso richiesta DDM) determina come il sistema elabora le richieste da altri sistemi per l'accesso ai dati utilizzando il DDM (distributed data management) o la funzione del database relazionale distribuita.

Valori possibili per DDMACC:	
***REJECT**	Il sistema non consente le richieste DDM o DRDA dai sistemi remoti. *REJECT non impedisce il funzionamento di questo sistema come sistema richiedente e l'invio di richieste ad altri sistemi server.
***OBJAUT**	Le richieste remote vengono controllate dall'autorizzazione oggetto sul sistema.
nome- programma- qualificato	Questo programma di uscita scritto dall'utente viene richiamato dopo la verifica della normale autorizzazione oggetto. Il programma di uscita viene richiamato solo per i file DDM, non per le funzioni del database relazionale distribuite. Al programma di uscita viene inoltrato un elenco parametri, creato dal sistema remoto, che identifica l'utente del sistema locale e la richiesta. Il programma valuta la richiesta e invia un codice di ritorno, concedendo o negando l'accesso richiesto.

Informazioni correlate

DDMACC parameter considerations

Operazioni di salvataggio e di ripristino

La funzione di salvataggio degli oggetti dal sistema o di ripristino degli oggetti sul sistema rappresenta un rischio per la sicurezza della propria azienda.

Ad esempio, i programmatori spesso dispongono dell'autorizzazione *OBJEXIST sui programmi poiché questa autorizzazione viene richiesta per la ricompilazione di un programma (e cancellare la vecchia copia). L'autorizzazione *OBJEXIST viene anche richiesta per il salvataggio di un oggetto. Per questo

motivo, il programmatore tipico può creare una copia su nastro dei programmi, che potrebbe rappresentare un investimento finanziario importante.

Un utente che possiede l'autorizzazione *OBJEXIST su un oggetto può inoltre ripristinare una nuova copia di un oggetto su un oggetto esistente. Nel caso di un programma, il programma ripristinato potrebbe essere stato creato su un sistema diverso. Potrebbe eseguire funzioni diverse. Ad esempio, si presupponga che il programma originale abbia gestito dati confidenziali. La nuova versione potrebbe eseguire le stesse funzioni, ma potrebbe inoltre scrivere una copia di informazioni riservate su un file segreto nella libreria personale del programmatore. Il programmatore non necessita dell'autorizzazione ai dati riservati poiché gli utenti regolari del programma accederanno ai dati.

Limitazione delle operazioni di salvataggio e di ripristino

È possibile limitare le operazioni di salvataggio e di ripristino per proteggere il sistema.

È possibile controllare la funzione di salvataggio e di ripristino degli oggetti in diversi modi:

- Limitare l'accesso fisico alle unità di salvataggio e di ripristino, come ad esempio le unità nastro e le unità ottiche.
- Limitare l'autorizzazione agli oggetti delle descrizioni dell'unità per le unità di salvataggio e di ripristino. Per salvare un oggetto su un'unità nastro, è necessario disporre dell'autorizzazione *USE sulla descrizione dell'unità per l'unità nastro.
- Limitare i comandi di salvataggio e di ripristino. Questo consente all'utente di controllare i dati salvati dal sistema e ripristinati sul sistema mediante tutte le interfacce, compresi i file di salvataggio. Consultare "Esempio: Limitazione dei comandi di salvataggio e di ripristino" per un esempio su come procedere. Il sistema imposta i comandi di ripristino su PUBLIC(*EXCLUDE) quando si installa il sistema.
- Fornire l'autorizzazione speciale *SAVSYS solo ad utenti affidabili.

Esempio: Limitazione dei comandi di salvataggio e di ripristino

Questo argomento mostra un esempio di limitazione dei comandi di salvataggio e di ripristino.

È possibile attenersi alla seguente procedura per limitare i comandi di salvataggio e ripristino sul proprio sistema:

1. Per creare un elenco di autorizzazioni che l'utente può utilizzare per fornire l'autorizzazione sui comandi agli operatori di sistema, immettere il seguente esempio:
   ```
   CRTAUTL AUTL(SRLIST) TEXT('Save and Restore List')
   AUT(*EXCLUDE)
   ```
2. Per utilizzare l'elenco di autorizzazioni per proteggere i comandi di salvataggio, immettere il seguente esempio:
   ```
   GRTOBJAUT OBJ(SAV*) OBJTYPE(*CMD) AUTL(SRLIST)
   ```
3. Per accertarsi che l'autorizzazione *PUBLIC provenga dall'elenco di autorizzazioni, immettere il seguente esempio:
   ```
   GRTOBJAUT OBJ(SAV*) OBJTYPE(*CMD) USER(*PUBLIC)
      AUT(*AUTL)
   ```
4. Per utilizzare l'elenco di autorizzazioni per proteggere i comandi di ripristino, immettere il seguente esempio:
   ```
   GRTOBJAUT OBJ(RST*) OBJTYPE(*CMD) AUTL(SRLIST)
   ```
5. Per accertarsi che l'autorizzazione *PUBLIC provenga dall'elenco di autorizzazioni, immettere il seguente esempio:
   ```
   GRTOBJAUT OBJ(RST*) OBJTYPE(*CMD) USER(*PUBLIC)
      AUT(*AUTL)
   ```

6. Sebbene gli operatori di sistema responsabili del salvataggio del sistema dispongano dell'autorizzazione speciale *SAVSYS, ora devono disporre dell'autorizzazione esplicita sui comandi SAVxxx. Per eseguire ciò, aggiungere gli operatori di sistema all'elenco di autorizzazioni:

   ```
   ADDAUTLE AUTL(SRLIST) USER(USERA USERB) AUT(*USE)
   ```

   Nota: è possibile fare in modo che gli operatori di sistema dispongano dell'autorizzazione solo sui comandi di salvataggio. In questo caso, proteggere i comandi di salvataggio e di ripristino con due elenchi di autorizzazioni separati.

7. Per limitare le API di salvataggio e di ripristino e proteggerle con un elenco di autorizzazioni, immettere i seguenti comandi:

   ```
   GRTOBJAUT OBJ(QSRSAVO) OBJTYPE(*PGM) AUTL(SRLIST)
   GRTOBJAUT OBJ(QSRSAVO) OBJTYPE(*PGM) USER(*PUBLIC)
      AUT(*AUTL)
   GRTOBJAUT OBJ(QSRLIB01) OBJTYPE(*SRVPGM) AUTL(SRLIST)
   GRTOBJAUT OBJ(QSRLIB01) OBJTYPE(*SRVPGM) USER(*PUBLIC)
      AUT(*AUTL)
   GRTOBJAUT OBJ(QSRRSTO) OBJTYPE(*PGM) AUTL(SRLIST)
   GRTOBJAUT OBJ(QSRRSTO) OBJTYPE(*PGM) USER(*PUBLIC)
      AUT(*AUTL)
   ```

Ottimizzazione prestazioni

Il controllo e l'ottimizzazione delle prestazioni non sono compiti del responsabile della riservatezza. Tuttavia, il responsabile della riservatezza dovrebbe accertarsi che gli utenti non stanno modificando le caratteristiche delle prestazioni del sistema per velocizzare i propri lavori a scapito di altri.

Diversi oggetti di gestione dei lavori coinvolgono le prestazioni dei lavori nel sistema:

- La classe imposta la priorità di esecuzione e il tempo per un lavoro.
- La voce di instradamento nella descrizione del sottosistema stabilisce la classe e il lotto di memoria utilizzati dal lavoro.
- La descrizione del lavoro può determinare la coda di emissione, la priorità di emissione, la coda lavori e la priorità del lavoro.

Gli utenti esperti con autorizzazione appropriata possono creare il proprio ambiente sul sistema e garantirsi prestazioni migliori rispetto agli altri utenti. Controllare il tutto limitando l'autorizzazione alla creazione e alla modifica degli oggetti di gestione del lavoro. Impostare l'autorizzazione pubblica ai comandi di gestione del lavoro su *EXCLUDE e concedere l'autorizzazione a pochi utenti affidabili.

Le caratteristiche delle prestazioni del sistema possono essere modificate anche in modalità interattiva. Ad esempio, il pannello Gestione stato del sistema (WRKSYSSTS) può essere utilizzato per modificare la dimensione dei lotti di memoria e i livelli di attività. Inoltre, un utente con l'autorizzazione speciale *JOBCTL (controllo lavoro) può modificare la priorità di pianificazione di ogni lavoro sul sistema, sottoposto al limite di priorità (PTYLMT) nel profilo utente. Assegnare l'autorizzazione speciale *JOBCTL e PTYLMT nei profili utente con molta attenzione.

Per consentire agli utenti di visualizzare le informazioni sulle prestazioni utilizzando il comando WRKSYSSTS senza però poterle modificare, immettere:

```
GRTOBJAUT OBJ(CHGSHRPOOL) OBJTYPE(*CMD) +
          USER(*PUBLIC)   AUT(*EXCLUDE)
```

Autorizzare gli utenti responsabili dell'ottimizzazione del sistema alla modifica delle caratteristiche delle prestazioni, immettendo:

```
GRTOBJAUT OBJ(CHGSHRPOOL) OBJTYPE(*CMD) +
          USER(USRTUNE)   AUT(*USE)
```

Limitazione dei lavori in batch

È possibile creare o modificare i comandi per eseguire alcuni lavori solo in ambiente batch.

Ad esempio, è possibile eseguire alcuni prospetti oppure compilare i programmi in batch. Un lavoro eseguito in batch spesso influenza le prestazioni del sistema in maniera meno significativa rispetto allo stesso lavoro eseguito in maniera interattiva.

Ad esempio, per limitare il comando che esegue un programma RPTA ai soli lavori batch:

- Creare un comando che esegua RPTA e specificare che il comando può essere eseguito solo in batch:
  ```
  CRTCMD CMD(RPTA) PGM(RPTA) ALLOW(*BATCH *BPGM)
  ```

Per limitare le compilazioni alla sola modalità batch, eseguire quanto riportato per il comando di creazione per ciascuno tipo di programma:

```
CHGCMD CMD(CRTxxxPGM) ALLOW(*BATCH *BPGM)
```

Capitolo 7. Progettazione sicurezza

Questa sezione contiene delle istruzioni utili agli sviluppatori delle applicazioni e ai gestori di sistemi per includere la sicurezza come parte dell'intero progetto. Inoltre, contiene esempi di tecniche che è possibile utilizzare per raggiungere obbiettivi relativi alla sicurezza sul sistema.

La protezione delle informazioni è una parte importante di molte applicazioni. È necessario prendere in considerazione la sicurezza, insieme ad altri requisiti, nel momento in cui viene progettata l'applicazione. Ad esempio, quando si stabilisce come organizzare le informazioni sulle applicazioni in librerie, tentare di bilanciare i requisiti di sicurezza con altre considerazioni, quali il ripristino, la copia di riserva e le prestazioni dell'applicazione.

Alcun i degli esempi in questa sezione contengono programmi di esempio. Questi programmi sono inclusi solo a scopo illustrativo. Molti di questi programmi non potranno essere eseguiti, non potranno effettuare una compilazione e non includono una gestione dei messaggi e un ripristino errori.

L'argomento Plan and set up system security nell'Information center è rivolto all'amministratore della riservatezza. Contiene moduli, esempi e istruzioni sulla pianificazione della sicurezza per le applicazioni già sviluppate. Se si è responsabili della progettazione di un'applicazione, potrebbe risultare utile riesaminare i moduli e gli esempi riportati nell'argomento Plan and set up system security per dettagli. Questa serie di aiuti possono risultare utili per vedere l'applicazione nell'ottica di un amministratore della riservatezza e per capire di quali informazioni è necessario disporre.

Anche l'argomento Plan and set up system security nell'Information center utilizza una serie di applicazioni di esempio per un'azienda fittizia denominata Azienda di giocattoli JKL. Questa sezione riporta delle considerazioni sulla progettazione per la stessa serie di applicazioni di esempio. La Figura 31 mostra il rapporto tra i gruppi di utenti, le applicazioni e le librerie per l'azienda di giocattoli JKL:

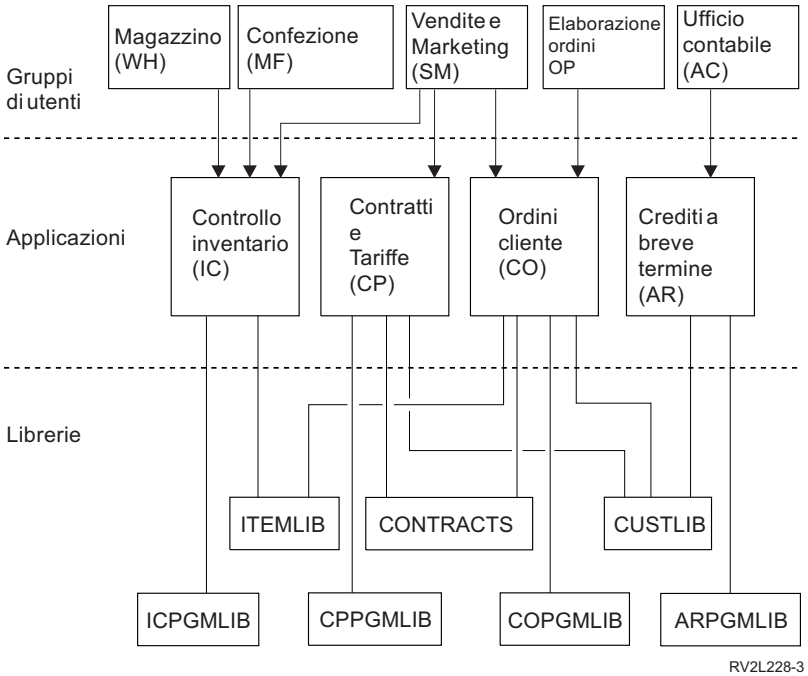


Figura 31. Applicazioni di esempio

Descrizione del grafico

Questo grafico mostra il modo in cui cinque serie di gruppi di utenti accedono alle applicazioni e alle librerie sul sistema in un'azienda di giocattoli denominata JKL. I gruppi di utenti includono il Magazzino, la Produzione, le Vendite, il Marketing, l'Elaborazione ordini e la Contabilità. Questi gruppi utente dispongono di accessi diversi alle differenti applicazioni riportate nel seguente elenco.

- I gruppi utenti Magazzino, Produzione, Vendite e Marketing possono tutti accedere alle applicazioni di Controllo inventario.
- I gruppi di utenti Vendite e Marketing dispongono inoltre dell'accesso alle applicazioni Contratti e Tariffe e all'applicazione Ordini cliente.
- Il gruppo di utenti Elaborazione ordini dispone inoltre dell'accesso all'applicazione Ordini cliente.
- Il gruppo di utenti Contabilità ha accesso solo all'applicazione Crediti a breve termine.

Informazioni correlate

Scenarios for HTTP Server

Consigli generali per la struttura della sicurezza

Se la struttura della sicurezza è semplice risulterà più facile gestirla e controllarla. Inoltre, in questo modo miglioreranno le prestazioni dell'applicazione e delle procedure per la copia di riserva.

Segue un elenco di consigli generali per la struttura della sicurezza:

- Utilizzare la sicurezza delle risorse insieme ai metodi disponibili, quali le capacità limitate nel profilo utente e la limitazione degli utenti a una serie di menu, per proteggere le informazioni.

  Attenzione: se si utilizza un prodotto come System i Access o se si dispone di linee di comunicazione collegate al sistema, non fare affidamento solo sulla limitazione delle possibilità nel profilo utente e nel controllo accesso menu. È necessario utilizzare la sicurezza delle risorse per proteggere gli oggetti che non si desidera siano accessibili attraverso queste interfacce.
- Proteggere solo quegli oggetti che necessitano realmente di protezione. Analizzare una libreria per determinare quali oggetti, ad esempio file di dati, siano riservati e proteggano quegli oggetti. Utilizzare un'autorizzazione pubblica per altri oggetti, quali le aree dati e le code messaggi.
- Passare dal generale al particolare:
  - Pianificare la sicurezza per le librerie e gli indirizzari. Occuparsi dei singoli oggetti solo quando necessario.
  - Pianificare prima di tutto l'autorizzazione pubblica, seguita dall'autorizzazione di gruppo e dalla singola autorizzazione.
- Rendere l'autorizzazione pubblica per i nuovi oggetti in una libreria (parametro CRTAUT) uguale all'autorizzazione pubblica definita per la maggior parte degli oggetti esistenti nella libreria.
- Per rendere l'operazione di controllo più facile e migliorare le prestazioni per il controllo dell'autorizzazione, non definire un'autorizzazione privata inferiore a un'autorizzazione pubblica per un oggetto.
- Utilizzare gli elenchi di autorizzazioni per raggruppare gli oggetti con gli stessi requisiti di sicurezza. Gli elenchi di autorizzazioni sono più facili da gestire rispetto alle singole autorizzazioni e forniscono assistenza nel ripristino delle informazioni relative alla sicurezza.

Concetti correlati

Capitolo 5, "Sicurezza delle risorse", a pagina 141
Questa sezione descrive ognuno dei componenti della sicurezza delle risorse e spiega come partecipino alla protezione delle informazioni sul sistema. Inoltre, questo capitolo spiega come utilizzare i comandi CL e i pannelli per impostare la sicurezza delle risorse sul sistema.

Pianificazione delle modifiche al livello di una parola d'ordine

È necessario pianificare con attenzione la modifica dei livelli delle parole d'ordine. È 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 aver 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, anche 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 accesso, deve essere aggiornato per gestire le 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 l'algoritmo per il livello 2 o 3 di QPWDLVL, anche se i caratteri specifici immessi sono corretti, non verranno accettati. Ciò si applica anche a qualsiasi accesso peer da System i a System i che utilizza i valori codificati per eseguire l'autenticazione da un sistema ad un altro.

Il problema è dato dal fatto che alcuni prodotti interessati (ad es. IBM Toolbox per Java) vengono 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 ad un sistema, che non ha bisogno di comunicare con il Supporto IBM System i per risorse di rete di Windows Network Neighborhood (NetServer), di eliminare le parole d'ordine NetServer. 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 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, l'amministratore di sistema dovrebbe utilizzare il comando PRTUSRPRF TYPE(*PWDLVL) per individuare tutti i profili utente che non dispongono di una parola d'ordine utilizzabile al livello 2. A seconda dei profili individuati, l'amministratore dovrebbe 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 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 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 risponde alla seguente descrizione, 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.

- Il profilo utente non dispone di una parola d'ordine utilizzabile ai livelli 2 e 3.
- Il profilo utente non dispone di una parola d'ordine utilizzabile ai livelli 0 e 1.
- L'utente accede tramite un prodotto che invia parole d'ordine con testo in chiaro.

Gli accessi successivi verranno convalidati rispetto alle parole d'ordine di livello 2.

Qualsiasi client che utilizza la sostituzione della parola d'ordine non funzionerà correttamente al livello QPWDLVL 2 se il client 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 che non è stato aggiornato nel nuovo schema di sostituzione parola d'ordine.

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

- TELNET
- System iAccesso
- server host System i
- QFileSrv.400
- Supporto dio stampa System i NetServer
- DDM
- DRDA
- SNA LU6.2

Si consiglia vivamente di salvare i dati di sicurezza prima di passare a QPWDLVL 2. Ciò può essere utile per facilitare il ritorno a QPWDLVL 0 o 1 nel caso diventi necessario.

| Evitare di modificare i valori di sistema parola d'ordine, come QPWDMINLEN, QPWDMAXLEN e
| QPWDRULES, prima di aver verificato 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 in 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 NetServer sono ancora supportate al livello QPWDLVL 2, quindi qualsiasi funzione/servizio che richieda una parola d'ordine NetServer dovrebbe ancora funzionare correttamente.

Una volta acquisita familiarità con l'esecuzione del sistema al livello QPWDLVL 2, è possibile modificare i valori di sistema della parola d'ordine per utilizzare parole d'ordine più lunghe. Tuttavia, è necessario essere consapevoli che le parole d'ordine più lunghe provocano 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. Questo profilo utente non potrà accedere 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 vengono specificate parole d'ordine che superano i 14 caratteri, la parola d'ordine 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 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 prendere in considerazione il passaggio a QPWDLVL 3 per ottimizzare la protezione di sicurezza della parola d'ordine.

Al livello QPWDLVL 3, tutte le parole d'ordine NetServer vengono eliminate quindi un sistema non dovrebbe essere portato al livello QPWDLVL 3 fino a quando non sarà più necessario l'utilizzo di parole d'ordine 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 di QPWDLVL 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 configurare nuovamente un valore inferiore di QPWDLV.

Considerazioni per passare da QPWDLVL 3 a 2

Tale modifica è relativamente semplice. Una volta impostato QPWDLVL su 2, l'amministratore deve stabilire se è necessario qualche profilo utente per contenere parole d'ordine NetServer o 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 parole d'ordine NetServer e di livello 0 o 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 accedere 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 utilizzare il comando 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 richiede una parola d'ordine una volta modificato QPWDLVL, accertarsi della creazione di una parola d'ordine di livello 0 e 1 per il profilo 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 provoca la modifica, da parte del sistema, della parola d'ordine utilizzabile ai livelli 2 e 3 e inoltre il sistema crea 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.
  - È 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 può risultare nella 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 può provocare 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 NetServer vengono eliminate quando la modifica in QPWDLVL 1 diviene effettiva (al successivo IPL).

Considerazioni per passare da QPWDLVL 2 a 0

Le considerazioni sono uguali a quelle già effettuate per la modifica da QPWDLVL 2 a 1 ad eccezione del fatto che tutte le parole d'ordine NetServer vengono conservate quando la modifica diventa effettiva.

Considerazioni per passare da QPWDLVL 1 a 0

Dopo aver modificato QPWDLVL in 0, l'utente dovrebbe utilizzare i comandi DSPAUTUSR o PRTUSRPRF per individuare qualsiasi profilo utente che non disponga di una parola d'ordine NetServer. Se il profilo utente richiede una parola d'ordine NetServer, questa può essere creata modificando la parola d'ordine dell'utente o accedendo tramite un meccanismo che presenti la parola d'ordine con testo in chiaro.

Quindi, è possibile modificare QPWDLVL in 0.

Pianificazione delle librerie

Una libreria è come un indirizzario utilizzato per individuare gli oggetti nella libreria. Molti fattori influenzano la scelta su come raggruppare le informazioni relative all'applicazione in librerie e su come gestire queste librerie.

La sicurezza della libreria diventa effettiva solo se vengono rispettate le regole riportate di seguito:

- Le librerie contengono gli oggetti con requisiti di sicurezza simili.
- Gli utenti non possono aggiungere nuovi oggetti alle librerie limitate. Le modifiche apportate ai programmi nelle librerie vengono controllate. Ossia, le librerie dell'applicazione dispongono dell'autorizzazione pubblica *USE o *EXCLUDE a meno che gli utenti debbano creare gli oggetti direttamente nella libreria.
- Vengono controllati gli elenchi librerie.

Per accedere a un oggetto, è necessario disporre dell'autorizzazione per l'oggetto stesso e alla libreria contenete l'oggetto. È possibile limitare l'accesso a un oggetto limitando l'oggetto stesso, la libreria contenente l'oggetto o entrambi.

L'autorizzazione *USE per una libreria consente di trovare gli oggetti nella libreria. L'autorizzazione per l'oggetto determina *in che modo* sia possibile utilizzare l'oggetto. L'autorizzazione *USE a una libreria è sufficiente per eseguire molte operazioni sugli oggetti nella libreria.

L'utilizzo dell'autorizzazione pubblica per gli oggetti e la limitazione dell'accesso alle librerie potrebbe essere una tecnica di sicurezza efficace e semplice. L'inserimento dei programmi in una libreria separata da altri oggetti dell'applicazione potrebbe inoltre semplificare la pianificazione della sicurezza. Questo si può notare specialmente se i file vengono condivisi da più di un'applicazione. È possibile utilizzare l'autorizzazione alle librerie contenenti i programmi dell'applicazione per controllare chi può eseguire funzioni dell'applicazione.

Seguono due esempi di utilizzo della sicurezza della libreria per le applicazioni dell'azienda di giocattoli JKL. (Consultare la Figura 31 a pagina 235 per un diagramma delle applicazioni).

- Le informazioni nella libreria CONTRACTS sono considerate riservate. L'autorizzazione pubblica per tutti gli oggetti nella libreria è sufficiente per eseguire le funzioni dell'applicazione Tariffe e Contratti (*CHANGE). L'autorizzazione pubblica per la libreria CONTRACTS è *EXCLUDE. Solo agli utenti o ai gruppi autorizzati per l'applicazione Contratti e Tariffe viene concessa l'autorizzazione *USE per la libreria.
- L'azienda di giocattoli SKL è una piccola azienda con un approccio non limitato alla sicurezza, ad eccezione delle informazioni sul contratto e sulle tariffe. Tutti gli utenti di sistema possono visualizzare le informazioni sui clienti e sull'inventario, anche se solo gli utenti autorizzati possono modificare tali informazioni. Le librerie CUSTLIB e ITEMLIB e gli oggetti nelle librerie, dispongono dell'autorizzazione pubblica *USE. Gli utenti possono visualizzare le informazioni in queste librerie attraverso l'applicazione principale o utilizzando una query SQL. Le librerie di programma dispongono dell'autorizzazione pubblica *EXCLUDE. Solo gli utenti che dispongono dell'autorizzazione per modificare le informazioni sull'inventario hanno accesso a ICPGMLIB. I programmi che modificano le informazioni sull'inventario utilizzano l'autorizzazione del proprietario dell'applicazione (OWNIC) e quindi dispongono dell'autorizzazione *ALL per i file nella libreria ITEMLIB.

Concetti correlati

"Sicurezza libreria" a pagina 145
È possibile utilizzare la sicurezza libreria per proteggere le informazioni.

Riferimenti correlati

"Elenchi librerie" a pagina 222
L'**elenco librerie** per un lavoro indica le librerie in cui effettuare le ricerche e l'ordine in cui le ricerche devono essere effettuate.

Informazioni correlate

Scenarios for HTTP Server

Pianificazione delle applicazioni per evitare profili grandi

Per ridurre gli impatti sulle prestazioni e la sicurezza del sistema, è necessario pianificare attentamente le applicazioni, per evitare profili grandi.

A causa degli impatti che potrebbero influire sulle prestazioni e sulla sicurezza, eseguire le seguenti azioni per evitare che i profili si riempiano troppo:

- Non fare in modo che un solo profilo contenga tutto il contenuto sul sistema.

  Creare profili speciali che possano contenere le applicazioni. I profili proprietario specifici di un'applicazione rendono più semplice il processo di ripristino e di spostamento delle applicazioni tra sistemi. Inoltre, le informazioni sulle autorizzazioni private sono distribuite su più profili, il che migliora le prestazioni. Mediante l'utilizzo di alcuni profili proprietario, è possibile fare in modo che un profilo non diventi troppo grande a causa della proprietà di troppi oggetti. Inoltre, i profili proprietario consentono di adottare l'autorizzazione del profilo proprietario piuttosto che di un profilo più potente che fornisce un'autorizzazione non necessaria.
- Evitare di utilizzare applicazioni appartenenti ai profili utente forniti da IBM, quali QSECOFR o QPGMR.

  Tali profili dispongono di un numero elevato di oggetti forniti da IBM e possono diventare difficili da gestire. Se ci sono applicazioni appartenenti ai profili utente forniti da IBM è possibile che si verifichino problemi relativi alla sicurezza quando si sposta un'applicazione da un sistema a un altro. Le applicazioni appartenenti ai profili utente forniti da IBM possono anche influire sulle prestazioni dei comandi, come CHKOBJITG e WRKOBJOWN.
- Utilizzare gli elenchi di autorizzazioni per proteggere gli oggetti.

  Se si stanno concedendo autorizzazioni private a molti oggetti per alcuni utenti, è necessario utilizzare un elenco di autorizzazioni per proteggere gli oggetti. Gli elenchi di autorizzazioni causeranno la visualizzazione di una voce autorizzazione privata per l'elenco di autorizzazioni nel profilo utente piuttosto che una voce autorizzazione privata per ogni oggetto. Nel profilo del proprietario oggetto, gli elenchi di autorizzazione creano una voce oggetto autorizzato per ogni utente con autorizzazione all'elenco di autorizzazioni.

Elenchi librerie

L'elenco librerie per un lavoro rappresenta un rischio per la sicurezza e contemporaneamente fornisce flessibilità. Questo rischio è particolarmente importante se si utilizza un'autorizzazione pubblica per gli oggetti e si fa affidamento alla sicurezza della libreria come metodo principale per proteggere le informazioni. In questo caso, un utente che dispone dell'accesso alla libreria può accedere senza alcun controllo alle informazioni nella libreria.

Per evitare di mettere a rischio la sicurezza degli elenchi librerie, nelle applicazioni è possibile specificare nomi qualificati. Quando viene specificato il nome oggetto e la libreria, il sistema non ricerca l'elenco librerie. Ciò impedisce a un possibile intruso di utilizzare l'elenco librerie per evitare la sicurezza.

Tuttavia, altri requisiti sulla struttura dell'applicazione potrebbero impedire l'utilizzo dei nomi qualificati. Se le applicazioni fanno affidamento su elenchi librerie, le tecniche riportate di seguito possono ridurre i rischi per la sicurezza.

Nota: utilizzando i codici di esempio, si accettano i termini presenti nel Capitolo 10, "Informazioni sull'esonero di responsabilità e licenza codice", a pagina 329.

Controllo elenco librerie utente

Come precauzione per la sicurezza, assicurarsi che la parte utente dell'elenco librerie disponga delle voci corrette nella sequenza prevista prima di eseguire un lavoro. Un metodo per effettuare ciò è quello di utilizzare un programma CL per salvare l'elenco librerie dell'utente, sostituirlo con l'elenco desiderato e ripristinarlo alla fine dell'applicazione.

Segue un programma di esempio per effettuare ciò:

Nota: utilizzando i codici di esempio, si accettano i termini presenti nel Capitolo 10, "Informazioni sull'esonero di responsabilità e licenza codice", a pagina 329.

```
          PGM
          DCL      &USRLIBL *CHAR LEN(2750)
          DCL      &CURLIB  *CHAR LEN(10)
          DCL      &ERROR *LGL
          DCL      &CMD *CHAR LEN(2800)
          MONMSG   MSGID(CPF0000)  +
                   EXEC(GOTO SETERROR)
          RTVJOBA  USRLIBL(&USRLIBL) +
                   CURLIB(&CURLIB)
          IF COND(&CURLIB=('*NONE')) +
             THEN(CHGVAR &CURLIB '*CRTDFT  ')
          CHGLIBL  LIBL(QGPL) CURLIB(*CRTDFT)
          /*********************************/
          /*                               */
          /*     Elaborazione normale      */
          /*                               */
          /*********************************/
          GOTO     ENDPGM
SETERROR: CHGVAR   &ERROR '1'
ENDPGM:   CHGVAR   &CMD +
                           ('CHGLIBL LIBL+
                           (' *CAT &USRLIBL *CAT')  +
                           CURLIB(' *CAT &CURLIB *TCAT ' )')
                   CALL    QCMDEXC PARM(&CMD 2800)
                   IF      &ERROR SNDPGMMSG MSGID(CPF9898) +
                           MSGF(QCPFMSG) MSGTYPE(*ESCAPE) +
                           MSGDTA('The xxxx error occurred')
                   ENDPGM
```

Figura 32. Programma per la sostituzione e il ripristino di un elenco librerie

Note:

1. A prescindere dall'esito dell'esecuzione del programma (normale o anomala), l'elenco librerie viene riportato al ruolo che svolgeva prima del richiamo del programma. Per questa ragione la gestione errori include il ripristino dell'elenco librerie.
2. Poiché il comando CHGLIBL richiede un elenco di nomi libreria, non è possibile eseguirlo direttamente. Perciò il comando RTVJOBA, richiama le librerie utilizzate per creare il comando CHGLIBL come variabile. La variabile viene inoltrata come parametro alla funzione QCMDEXC.
3. Se si arriva a una situazione imprevista (ad esempio, un programma utente, un menu che consente l'immissione di comandi o il pannello Immissione comando) nel mezzo di un programma, il programma dovrebbe sostituire l'elenco librerie per assicurare un controllo adeguato.

Modifica elenco librerie di sistema

L'utente potrebbe dover modificare anche la parte di sistema dell'elenco librerie per proteggere il sistema.

Se l'applicazione deve aggiungere voci alla parte di sistema dell'elenco librerie, è possibile utilizzare un programma CL simile a quello mostrato nella Figura 32, con le seguenti modifiche:

- Invece di utilizzare il comando RTVJOBA, utilizzare il comando RTVSYSVAL (Richiamo valori di sistema) per richiamare il valore del valore di sistema QSYSLIB.
- Utilizzare il comando CHGSYSLIBL (Modifica elenco librerie sistema) per modificare la parte di sistema dell'elenco librerie nel valore desiderato.
- Alla fine del programma, utilizzare nuovamente il comando CHGSYSLIBL per ripristinare la parte di sistema dell'elenco librerie al valore originale.
- Il comando CHGSYSLIBL viene fornito con l'autorizzazione pubblica *EXCLUDE. Per utilizzare questo comando nel programma, effettuare una delle seguenti operazioni:
  - Fornire al proprietario del programma l'autorizzazione *USE per il comando CHGSYSLIBL e utilizzare l'autorizzazione adottata.
  - Fornire agli utenti che stanno eseguendo il programma l'autorizzazione *USE al comando CHGSYSLIBL.

Descrizione della sicurezza libreria

Nel ruolo di sviluppatore dell'applicazione, è necessario fornire informazioni sulla libreria per l'amministratore della riservatezza. L'amministratore della riservatezza utilizza queste informazioni per stabilire come proteggere la libreria e i relativi oggetti.

È necessario conoscere le seguenti informazioni:

- Funzioni dell'applicazione che aggiungono oggetti alla libreria.
- Se gli oggetti nella libreria vengono cancellati durante l'elaborazione dell'applicazione.
- A quale profilo appartiene la libreria e i relativi oggetti.
- Se la libreria deve essere inclusa negli elenchi librerie.

La Figura 33 riporta un formato di esempio per fornire queste informazioni:

Nome libreria: `ITEMLIB`

Autorizzazione pubblica per la libreria: `*EXCLUDE`

Autorizzazione pubblica per gli oggetti nella libreria: `*CHANGE`

Autorizzazione pubblica per i nuovi oggetti (CRTAUT): `*CHANGE`

Proprietario libreria: `OWNIC`

Includere agli elenchi librerie? `No. La libreria viene aggiunta all'elenco librerie da un programma dell'applicazione iniziale o da un programma query iniziale.`

Elencare le funzioni che richiedono l'autorizzazione *ADD alla libreria:

`Nessun oggetto viene aggiunto alla libreria durante l'elaborazione normale dell'applicazione.` Elencare gli oggetti che richiedono l'autorizzazione *OBJMGT o *OBJEXIST e le funzioni che necessitano di tali autorizzazioni:

`Tutti i file di lavoro, di cui il nome inizia con i caratteri ICWRK, vengono eliminati alla fine del mese. Richiede l'autorizzazione *OBJMGT.`

Figura 33. Formato per la descrizione della sicurezza libreria

Pianificazione dei menu

I menu sono un ottimo metodo per fornire un accesso controllato sul sistema. È possibile utilizzare i menu per limitare un utente a una serie di funzioni controllate specificando le capacità limitate e un menu iniziale nel profilo utente.

Per utilizzare i menu come strumento di controllo accesso, seguire queste istruzioni quando si progettano:

- Non fornire una riga comandi per i menu progettati per gli utenti limitati.
- Evitare che ci siano funzioni con requisiti di sicurezza differenti sullo stesso menu. Ad esempio, se alcuni delle applicazioni possono solo vedere le informazioni e non modificarle, fornire un menu che disponga solo di opzioni di stampa e di visualizzazione per tali utenti.
- Assicurarsi che la serie di menu fornisca tutti i collegamenti necessari tra i menu in modo tale che l'utente non necessiti di una riga comandi per richiederne uno.
- Fornire accesso a poche funzioni di sistema, quale la visualizzazione di un'emissione di stampa. Il menu di sistema ASSIST fornisce questa funzione e può essere definito nel profilo utente come programma di gestione tasto di attenzione. Se il profilo utente dispone di una classe *USER e ha funzioni limitate, l'utente non è in grado di visualizzare l'emissione o i lavori di altri utenti.
- Fornire l'accesso agli strumenti di supporto alla scelta dai menu. L'argomento "Utilizzo dell'autorizzazione adottata nella struttura del menu" a pagina 246 fornisce un esempio di come effettuare ciò.
- Presumere di controllare l'accesso al menu Richiesta sistema o ad alcune opzioni su questo menu.
- Per gli utenti che possono eseguire solo una singola funzione, evitare completamente i menu e specificare un programma iniziale nel profilo utente. Specificare *SIGNOFF come menu iniziale.

Ad esempio, presso l'azienda di giocattoli JKL, tutti gli utenti visualizzano un menu di interrogazione che consente l'accesso a molti file. Per gli utenti che non possono modificare le informazioni, questo è il menu iniziale. L'opzione di ritorno sul menu scollega l'utente. Per gli altri utenti, questo menu viene richiamato da un'opzione di interrogazione dai menu delle applicazioni. Premendo F12 (Ritorna), l'utente ritorna al menu di chiamata. Poiché viene utilizzata la sicurezza libreria per le librerie di programma, questo menu e i programmi da esso richiamati vengono conservati nella libreria QGPL:

```
 INQMENU       Menu di interrogazione

         1. Descrizioni voce
         2. Item Balances
         3. Informazioni cliente
         4. Query
         5. Office

Immissione opzione ==>
F1=Aiuto  F12=Ritorna
```

Figura 34. Menu di interrogazione di esempio

Nota: utilizzando i codici di esempio, si accettano i termini presenti nel Capitolo 10, "Informazioni sull'esonero di responsabilità e licenza codice", a pagina 329.

Concetti correlati

"Menu richiesta sistema" a pagina 250
Un utente può utilizzare le funzioni di richiesta sistema per sospendere il lavoro corrente e visualizzare il menu Richiesta sistema. Il menu Richiesta sistema consente di inviare e visualizzare messaggi, effettuare un trasferimento a un secondo lavoro o terminare il lavoro corrente. Questo potrebbe rappresentare un rischio per la sicurezza poiché l'autorizzazione pubblica per il menu Richiesta sistema è *USE quando viene fornito un sistema.

Riferimenti correlati

"Possibilità limitate" a pagina 90
È possibile utilizzare il campo Possibilità limitate per limitare la possibilità dell'utente di immettere comandi e di sovrascrivere il programma iniziale, il menu iniziale, la libreria corrente e il programma di gestione dei tasti di attenzione specificati nel profilo utente. Questo campo consente di impedire agli utente di fare esperimenti sul sistema.

Informazioni correlate

Scenarios for HTTP Server

Descrizione della sicurezza menu

Nel ruolo di sviluppatore dell'applicazione, è necessario fornire informazioni su un menu per l'amministratore della riservatezza. L'amministratore della riservatezza utilizza queste informazioni per decidere chi deve avere accesso al menu e quali autorizzazioni sono richieste.

Esempi del tipo di informazioni di cui ha bisogno l'amministratore della riservatezza:

- Se le opzioni di menu richiedono autorizzazioni speciali, quali *SAVSYS o *JOBCTL.
- Se le opzioni di menu richiamano i programmi che adottano un'autorizzazione.
- Quale autorizzazione per gli oggetti è necessaria per ogni opzione di menu. È necessario solamente identificare quelle autorizzazioni maggiori rispetto all'autorizzazione pubblica normale.

La Figura 35 mostra un formato di esempio per fornire queste informazioni.

Nome menu: MENU1 Libreria QGPLNumero opzione: 3 Descrizione: Query

Programma richiamato: QRYSTART Libreria: QGPL

Autorizzazione adottata: QRYUSR

Autorizzazione speciale richiesta: Nessuna

Autorizzazioni oggetto richieste: l'utente deve disporre dell'autorizzazione *USE per il programma QRYSTART. QRYUSR deve disporre dell'autorizzazione *USE per le librerie contenenti i file da sottoporre a query. L'utente, QRYUSR o il pubblico deve disporre dell'autorizzazione *USE per i file sottoposti a query.

Figura 35. Formato per i requisiti sicurezza menu

Utilizzo dell'autorizzazione adottata nella struttura del menu

La disponibilità degli strumenti di supporto scelte, quale Query/400, mette in discussione la struttura della sicurezza. Non esiste alcun metodo nelle definizioni della sicurezza delle risorse che consenta a un utente di disporre di autorizzazioni differenti per un file in circostanze diverse. Tuttavia, l'utilizzo dell'autorizzazione adottata consente di definire l'autorizzazione per soddisfare requisiti differenti.

Ad esempio, è possibile che si desideri che gli utenti visualizzino le informazioni nei file utilizzando uno strumento di query ma è necessario assicurarsi che i file vengano modificati solo dai programmi dell'applicazione sottoposti a verifica.

Nota: "Oggetti che adottano l'autorizzazione del proprietario" a pagina 160 descrive la funzione dell'autorizzazione adottata. "Diagramma di flusso 8: come controllare l'autorizzazione adottata" a pagina 195 descrive in che modo il sistema effettua una verifica per l'autorizzazione adottata.

La Figura 36 a pagina 247 mostra un menu iniziale di esempio che utilizza un'autorizzazione adottata per fornire un accesso controllato ai file che utilizzando gli strumenti di query:

```
MENU1         Menu iniziale

        1.  Controllo inventario (ICSTART)
        2.  Ordini cliente   (COSTART)
        3.  Query             (QRYSTART)
        4.  Office            (OFCSTART)

(nessuna riga comandi)
```

Figura 36. Menu iniziale di esempio

I programmi che iniziano le applicazioni (ICSTART e COSTART) adottano l'autorizzazione di un profilo che possiede gli oggetti dell'applicazione. I programmi aggiungono le librerie dell'applicazione all'elenco librerie e visualizzano il menu dell'applicazione iniziale. Segue un esempio del programma Controllo inventario (ICSTART).

Nota: utilizzando i codici di esempio, si accettano i termini presenti nel Capitolo 10, "Informazioni sull'esonero di responsabilità e licenza codice", a pagina 329.

```
PGM
ADDLIBLE ITEMLIB
ADDLIBLE ICPGMLIB
GO ICMENU
RMVLIBLE ITEMLIB
RMVLIBLE ICPGMLIB
ENDPGM
```

Figura 37. Programma dell'applicazione iniziale di esempio

Il programma che avvia la Query (QRYSTART) adotta l'autorizzazione di un profilo (QRYUSR) fornito per consentire l'accesso ai file per le query. La Figura 38 mostra il programma QRYSTART:

```
PGM
ADDLIBLE ITEMLIB
ADDLIBLE CUSTLIB
STRQRY
RMVLIBLE ITEMLIB
RMVLIBLE CUSTLIB
ENDPGM
```

Figura 38. Programma di esempio per la Query con l'autorizzazione adottata

Il sistema menu utilizza tre tipi di profili utente, mostrati nella Tabella 125. La Tabella 126 a pagina 248 descrive gli oggetti utilizzati dal sistema menu.

Tabella 125. Profili utente per il sistema menu

Tipo di profilo	Descrizione	Parola d'ordine	Possibilità limitate	Autorizzazioni speciali	Menu iniziale
Proprietario applicazione	È proprietario degli oggetti applicazione e dispone dell'autorizzazione *ALL. OWNIC è proprietario dell'applicazione Controllo inventario.	*NONE	Non applicabili	Come richiesto da applicazione	Non applicabili
Utente applicazione [1]	Profilo di esempio per qualsiasi utente che utilizza il sistema menu	Sì	*YES	Nessuna	MENU1
Profilo query	Utilizzato per fornire accesso alle librerie per la query	*NONE	Non applicabili	Nessuna	Non applicabili

Tabella 125. Profili utente per il sistema menu (Continua)

Tipo di profilo	Descrizione	Parola d'ordine	Possibilità limitate	Autorizzazioni speciali	Menu iniziale
[1]	La libreria corrente specificata nel profilo utente dell'applicazione viene utilizzata per memorizzare le query create. Il programma di gestione del tasto attenzione è *ASSIST, e fornisce accesso all'utente alle funzioni di base del sistema.				

Tabella 126. Oggetti utilizzati dal sistema menu

Nome oggetto	Proprietario	Autorizzaz. pubblica	Autorizzazioni private	Informazioni aggiuntive
MENU1 nella libreria QGPL	Vedere la nota	*EXCLUDE	Autorizzazione *USE per tutti gli utenti che hanno l'autorizzazione a utilizzare il menu	Nella libreria QGPL, poiché gli utenti non dispongono dell'autorizzazione alle librerie dell'applicazione
Programma ICSTART in QGPL	OWNIC	*EXCLUDE	Autorizzazione *USE per gli utenti che dispongono dell'autorizzazione all'applicazione Controllo inventario	Creato con USRPRF(*OWNER) per adottare l'autorizzazione OWNIC
Programma QRYSTART in QGPL	QRYUSR	*EXCLUDE	Autorizzazione *USE per gli utenti che dispongono dell'autorizzazione per creare o eseguire le query	Creato con USRPRF(*OWNER) per adottare l'autorizzazione QRYUSR
ITEMLIB	OWNIC	*EXCLUDE	QRYUSR dispone dell'autorizzazione *USE	
ICPGMLIB	OWNIC	*EXCLUDE		
File disponibili per la Query in ITEMLIB	OWNIC	*USE		
File non disponibili per la Query in ITEMLIB	OWNIC	*EXCLUDE		
Programmi in ICPGMLIB	OWNIC	*USE		
Nota: è possibile creare un profilo proprietario speciale per gli oggetti utilizzati da più applicazioni.				

Quando USERA seleziona l'opzione 1 (Controllo inventario) dal MENU1, viene eseguito il programma ICSTART. Il programma adotta l'autorizzazione OWNIC, fornendo all'autorizzazione *ALL agli oggetti di controllo inventario in ITEMLIB e ai programmi in ICPGMLIB. USERA è inoltre autorizzato ad apportare modifiche ai file di controllo inventario mentre utilizza le opzioni dall'ICMENU.

Quando USERA esce da ICMENU e ritorna al MENU1, le librerie ITEMLIB e ICPGMLIB vengono rimosse dall'elenco librerie USERA e il programma ICSTART viene rimosso dallo stack di chiamata. USERA non è più in esecuzione sotto l'autorizzazione adottata.

Quando USERA seleziona l'opzione 3 (Query) dal MENU1, viene eseguito il programma QRYSTART. Il programma adotta l'autorizzazione QRYUSR, fornendo l'autorizzazione *USE alla libreria ITEMLIB. L'autorizzazione pubblica per i file in ITEMLIB determina quali file USERA sono consentiti per la query.

Questa tecnica ha il vantaggio di ridurre il numero di autorizzazioni private e fornisce prestazioni ottimali durante il controllo dell'autorizzazione:

- Gli oggetti nelle librerie dell'applicazione non dispongono di autorizzazioni private. Per alcune funzioni dell'applicazione, è più opportuno utilizzare l'autorizzazione pubblica. Se l'autorizzazione

pubblica non è appropriata, viene utilizzata l'autorizzazione proprietario. "Caso 8: Autorizzazione adottata senza autorizzazione privata" a pagina 205 mostra le fasi di verifica dell'autorizzazione.

- L'accesso ai file per la query utilizza l'autorizzazione pubblica per i file. Il profilo QRYUSR dispone di un'autorizzazione specifica solo per la libreria ITEMLIB.
- Per impostazione predefinita, qualsiasi programma query creato viene sostituito nella libreria corrente dell'utente. L'utente deve essere il proprietario della libreria corrente e tale utente deve disporre dell'autorizzazione *ALL.
- Gli utenti singoli devono disporre solo dell'autorizzazione per MENU1, ICSTART e QRYSTART.

Prendere in considerazione questi rischi e queste precauzioni quando si utilizzano queste tecniche:

- USERA dispone dell'autorizzazione *ALL per tutti gli oggetti di controllo inventario dall'ICMENU. Assicurarsi che il menu non consenta l'accesso a una riga comandi o non consenta l'utilizzo di funzioni di aggiornamento o di cancellazione non desiderate.
- Molti strumenti di supporto scelte consentono l'accesso a una riga comandi. Il profilo QRYUSR deve essere utilizzato da un utente con funzioni limitate e senza autorizzazioni speciali per evitare che vengano utilizzate funzioni non autorizzate.

Concetti correlati

"Pianificazione della sicurezza file" a pagina 252
Le informazioni contenute nei file di database sono spesso quelle più importanti nel sistema. La sicurezza delle risorse consente di controllare chi è in grado di visualizzare, modificare e cancellare le informazioni su un file.

Come ignorare l'autorizzazione adottata

La tecnica di utilizzare l'autorizzazione adottata nella struttura del menu richiede che l'utente ritorni al menu iniziale prima di eseguire delle query. Se si desidera sfruttare l'opportunità di avviare una query dai menu dell'applicazione e da un menu iniziale, è possibile impostare il programma QRYSTART per ignorare l'autorizzazione adottata.

La Figura 39 mostra un menu dell'applicazione che include il programma QRYSTART:

```
ICMENU      Menu Controllo inventario

            1.  Operazioni (ICPGM1)
            2.  Ricevute (ICPGM2)
            3.  Acquisti (ICPGM3)
            4.  Query  (QRYSTART)

(nessuna riga comandi)
```

Figura 39. Menu dell'applicazione di esempio con la query

Le informazioni sull'autorizzazione per il programma QRYSTART sono uguali a quelle mostrate nella Tabella 126 a pagina 248. Il programma viene creato con il parametro (USEADPAUT) dell'autorizzazione adottata impostato su *NO, per ignorare l'autorizzazione adottata di precedenti programmi nello stack.

Seguono dei confronti degli stack di chiamata quando USERA seleziona la query dal MENU1 (consultare la Figura 36 a pagina 247) e dal ICMENU:

Stack di chiamata quando la query viene selezionata dal MENU1

- MENU1 (nessuna autorizzazione adottata)
- QRYSTART (autorizzazione adottata QRYUSR)

Stack di chiamata quando la query viene selezionata da ICMENU

- MENU1 (nessuna autorizzazione adottata)
- ICMENU (autorizzazione adottata OWNIC)
- QRYSTART (autorizzazione adottata QRYUSR)

Specificando il programma QRYSTART con USEADPAUT(*NO), l'autorizzazione di qualsiasi precedente programma nello stack non viene utilizzata. Ciò consente a USERA di eseguire una query da ICMENU senza disporre dell'autorizzazione di modificare e cancellare i file. Questo poiché l'autorizzazione OWNIC non viene utilizzata dal programma QRYSTART.

Quando USERA termina la query e ritorna a ICMENU, l'autorizzazione adottata è nuovamente attiva. L'autorizzazione adottata viene ignorata solo finché il programma QRYSTART rimane attivo.

Se l'autorizzazione pubblica per il programma QRYSTART è *USE, specificare USEADPAUT(*NO) come precauzione per la sicurezza. In questo modo gli utenti che dispongono dell'autorizzazione adottata non potranno richiamare il programma QRYSTART ed eseguire funzioni non autorizzate.

Anche il menu di interrogazione (Figura 34 a pagina 245) nell'azienda di giocattoli JKL utilizza questa tecnica, poiché può essere richiamato dai menu in librerie di applicazione differenti. Esso adotta l'autorizzazione QRYUSR e ignora altre autorizzazioni adottate nello stack di chiamata.

Concetti correlati

"Programmi che ignorano l'autorizzazione adottata" a pagina 164
È possibile specificare il parametro dell'autorizzazione adottata (USEADPAUT) per controllare se un programma utilizza l'autorizzazione adottata.

Riferimenti correlati

"Diagramma di flusso 8: come controllare l'autorizzazione adottata" a pagina 195
Se si rileva un'autorizzazione insufficiente durante il controllo dell'autorizzazione utente, il sistema controlla l'autorizzazione adottata.

Informazioni correlate

Scenarios for HTTP Server

Menu richiesta sistema

Un utente può utilizzare le funzioni di richiesta sistema per sospendere il lavoro corrente e visualizzare il menu Richiesta sistema. Il menu Richiesta sistema consente di inviare e visualizzare messaggi, effettuare un trasferimento a un secondo lavoro o terminare il lavoro corrente. Questo potrebbe rappresentare un rischio per la sicurezza poiché l'autorizzazione pubblica per il menu Richiesta sistema è *USE quando viene fornito un sistema.

Il modo più semplice per impedire agli utenti non autorizzati di accedere a questo menu è di limitare l'autorizzazione sul gruppo pannelli QGMNSYSR:

- Per impedire a utenti specifici di visualizzare il menu Richiesta sistema, specificare l'autorizzazione *EXCLUDE per tali utenti:

```
GRTOBJAUT OBJ(QSYS/QGMNSYSR) +
          OBJTYPE(*PNLGRP)   +
          USER(USERA) AUT(*EXCLUDE)
```

- Per impedire a parte degli utenti di visualizzare il menu Richiesta sistema, revocare l'autorizzazione pubblica e concedere l'autorizzazione *USE a utenti specifici:

```
RVKOBJAUT OBJ(QSYS/QGMNSYSR) +
          OBJTYPE(*PNLGRP)   +
          USER(*PUBLIC) AUT(*ALL)
GRTOBJAUT OBJ(QSYS/QGMNSYSR) +
          OBJTYPE(*PNLGRP)   +
          USER(USERA) AUT(*USE)
```

Alcuni dei comandi effettivi utilizzati per il menu Richiesta sistema arrivano dal messaggio CPX2313 nel file di messaggi QCPFMSG. I comandi vengono definiti con un nome libreria dal messaggio CPX2373. I valori nel messaggio CPX2373 per ogni comando sono *NLVLIBL o *SYSTEM. Un utente potrebbe utilizzare il comando OVRMSGF (Sovrascrittura file di messaggi) per modificare i comandi utilizzati dalle opzioni del menu Richiesta sistema.

Ogni volta che si preme un tasto di richiesta del sistema, il sistema modifica automaticamente il profilo utente corrente del lavoro nel profilo utente iniziale del lavoro. Ciò avviene in modo che l'utente non disponga di alcuna ulteriore autorizzazione sul menu di richiesta del sistema o nel programma di uscita dal programma di richiesta presistema. Una volta completata la funzione di richiesta del sistema, il profilo utente corrente del lavoro viene modificato nel valore che aveva prima che venisse premuto il tasto di richiesta del sistema.

È possibile impedire agli utenti di selezionare opzioni specifiche dal menu Richiesta sistema limitando l'autorizzazione per i comandi associati. La Tabella 127 mostra i comandi associati alle opzioni di menu:

Tabella 127. Opzioni e comandi per il menu richiesta sistema

Opzione	Comando
1	TFRSECJOB (Trasferimento a lavoro secondario)
2	ENDRQS (Fine richiesta)
3	DSPJOB (Visualizzazione lavoro)
4	DSPMSG (Visualizzazione messaggio)
5	SNDMSG (Invio messaggio)
6	DSPMSG (Visualizzazione messaggio)
7	DSPWSUSR (Visualizzazione utente stazione di lavoro)
10	TFRPASTHR (Avvio richiesta sistema per il precedente sistema). (Vedere la nota che segue).
11	TFRPASTHR (Trasferimento al precedente sistema). (Vedere la nota che segue).
12	Visualizzazione opzioni di emulazione 3270 (Vedere la nota che segue).
13	TFRPASTHR (Avvio richiesta sistema nel sistema principale). (Vedere la nota che segue).
14	TFRPASTHR (Trasferimento al sistema principale). (Vedere la nota che segue).
15	TFRPASTHR (Trasferimento al sistema finale). (Vedere la nota che segue).
80	DSCJOB (Disconnessione lavoro)
90	SIGNOFF (Scollegamento)

Note:

1. Le opzioni 10, 11, 13, 14 e 15 vengono visualizzate se il pass-through di una stazione video è stato avviato con il comando STRPASTHR (Avvio pass-through). Le opzioni 10, 13 e 14 vengono visualizzate solo sul sistema di destinazione.
2. L'opzione 12 viene visualizzata solo quando l'emulazione 3270 è attiva.
3. Alcune delle opzioni presentano delle limitazioni per l'ambiente System/36.

Ad esempio, per impedire agli utenti non autorizzati di effettuare un trasferimento a un lavoro interattivo alternativo, revocare l'autorizzazione pubblica per il comando TFRSECJOB (Trasferimento a lavoro secondario) e fornire l'autorizzazione solo a utenti specifici:

```
RVKOBJAUT OBJ(TFRSECJOB) OBJTYPE(*CMD)
          USER(*PUBLIC) AUT(*ALL)
GRTOBJAUT OBJ(TFRSECJOB) OBJTYPE(*CMD)
          USER(USERA) AUT(*USE)
```

Se un utente seleziona un'opzione che necessita di autorizzazione, viene visualizzato un messaggio.

Se si desidera impedire agli utenti di utilizzare alcuni comandi nel menu Richiesta sistema ma si desidera che essi abbiano l'autorizzazione per eseguire un comando in un'ora specifica (come allo scollegamento), è possibile creare un programma CL che adotti l'autorizzazione di un utente autorizzato e che esegua il comando.

Concetti correlati

"Pianificazione dei menu" a pagina 245
I menu sono un ottimo metodo per fornire un accesso controllato sul sistema. È possibile utilizzare i menu per limitare un utente a una serie di funzioni controllate specificando le capacità limitate e un menu iniziale nel profilo utente.

Pianificazione della sicurezza comando

Quando si riceve il sistema, l'autorizzazione ad utilizzare i comandi è impostata in modo tale da rispettare la sicurezza di molte installazioni. Alcuni comandi possono essere eseguiti solo dal responsabile della riservatezza. Altri utenti richiedono un'autorizzazione speciale, quale *SAVSYS. Molti comandi possono essere utilizzati da qualsiasi utente sul sistema. È possibile modificare l'autorizzazione per i comandi per soddisfare i requisiti sulla sicurezza.

Ad esempio, è possibile che si voglia impedire alla maggior parte degli utenti sul sistema di gestire le comunicazioni. È possibile impostare l'autorizzazione pubblica su *EXCLUDE per tutti i comandi relativi alla gestione degli oggetti di comunicazione, quali i comandi CHGCTLxxx, CHGLINxxx e CHGDEVxxx.

Se si desidera verificare quali comandi possono essere eseguiti dagli utenti, è possibile utilizzare l'autorizzazione oggetto per i comandi stessi. Ogni comando sul sistema dispone del tipo oggetto *CMD e può essere autorizzato per un utente specifico o pubblico. Per eseguire un comando, l'utente necessita dell'autorizzazione *USE a tale comando. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 elenca tutti i comandi inviati con l'autorizzazione pubblica impostata su *EXCLUDE.

Se si utilizza la libreria System/38, è necessario inoltre limitare i comandi rilevanti per la sicurezza nella libreria. O è possibile limitare l'accesso all'intera libreria. Se si utilizza una o più NLV (National Language Version) del programma su licenza i5/OS sul sistema, è necessario inoltre limitare i comandi nelle librerie QSYSxxx aggiuntive sul sistema.

Un altro metodo per garantire la sicurezza è quello di modificare i valori predefiniti per alcuni comandi. Il comando CHGCMDDFT (Modifica valori predefiniti) consente di effettuare questa operazione.

Pianificazione della sicurezza file

Le informazioni contenute nei file di database sono spesso quelle più importanti nel sistema. La sicurezza delle risorse consente di controllare chi è in grado di visualizzare, modificare e cancellare le informazioni su un file.

Se gli utenti richiedono un'autorizzazione differente per i file a seconda della situazione, è possibile utilizzare l'autorizzazione adottata.

Per i file critici sul sistema, conservare un record di quali utenti dispongono di autorizzazione su un file. Se si utilizza l'autorizzazione gruppo e gli elenchi di autorizzazioni, è necessario tenere traccia degli utenti che dispongono di autorizzazione su quei metodi e degli utenti che dispongono di autorizzazione diretta. Se si utilizza un'autorizzazione adottata, è possibile elencare i programmi che adottano l'autorizzazione di un utente particolare utilizzando il comando DSPPGMADP) (Visualizzazione adozione programma).

È inoltre possibile utilizzare la funzione di registrazione su giornale sul sistema per monitorare l'attività su un file critico. Sebbene la funzione primaria del giornale sia quella di ripristinare le informazioni, è

possibile utilizzarlo come strumento di sicurezza. Contiene un record che tiene traccia degli utenti che accedono ad un file e nel modo in cui vi accedono. È possibile utilizzare il comando DSPJRN (Visualizzazione giornale) per visualizzare periodicamente un esempio di voci di giornale.

Riferimenti correlati

"Utilizzo dell'autorizzazione adottata nella struttura del menu" a pagina 246
La disponibilità degli strumenti di supporto scelte, quale Query/400, mette in discussione la struttura della sicurezza. Non esiste alcun metodo nelle definizioni della sicurezza delle risorse che consenta a un utente di disporre di autorizzazioni differenti per un file in circostanze diverse. Tuttavia, l'utilizzo dell'autorizzazione adottata consente di definire l'autorizzazione per soddisfare requisiti differenti.

Protezione dei file logici

La sicurezza delle risorse su un sistema supporta la sicurezza di livello campo di un file. È inoltre possibile utilizzare i file logici per proteggere record o campi specifici in un file.

È possibile utilizzare un file logico per specificare una sottoserie di *record* a cui un utente può accedere (utilizzando la logica di selezione e di omissione). Pertanto, è possibile impedire a utenti specifici di accedere a diversi tipi di record. È possibile utilizzare un file logico per specificare una sottoserie di *campi* in un record a cui può accedere un utente. Pertanto, è possibile impedire a utenti specifici di accedere a diversi campi in un record.

Un file logico non contiene dati. È una vista particolare di uno o più file fisici che contiene i dati. Per fornire accesso alle informazioni definite da un file logico è necessario disporre dell'autorizzazione ai dati per entrambi i file logici e per i file fisici associati.

La Figura 40 mostra un esempio di un file fisico e tre differenti file logici associati ad esso.

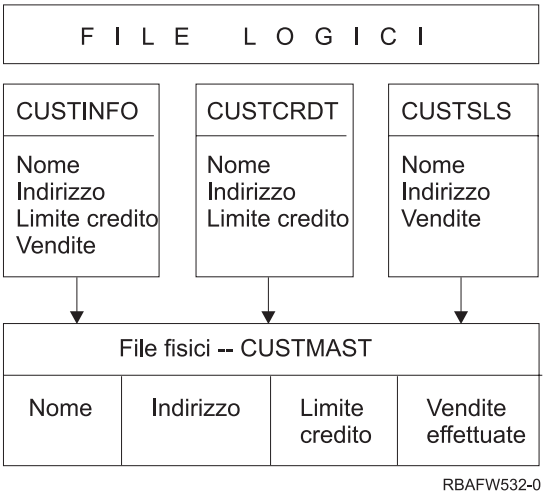


Figura 40. Utilizzo di un file logico per la sicurezza

I membri del reparto vendite (profilo gruppo DPTSM) sono in grado di visualizzare tutti i campi ma non possono modificare il limite di credito. I membri del reparto crediti a breve termine (profilo gruppo DPTAR) sono in grado di visualizzare tutti i campi ma non possono modificare i campi relativi alle vendite. L'autorizzazione al file fisico appare come la seguente:

Tabella 128. Esempio di file fisico: file CUSTMAST

Autorizzazione	**Utenti: *PUBLIC**
Autorizzazioni oggetto	

Tabella 128. Esempio di file fisico: file CUSTMAST (Continua)

Autorizzazione	**Utenti: *PUBLIC**
*OBJOPR	
*OBJMGT	
*OBJEXIST	
*OBJALTER	
*OBJREF	
Autorizzazioni dati	
*READ	X
*ADD	X
*UPD	X
*DLT	X
*EXECUTE	X
*EXCLUDE	

L'utente con autorizzazione pubblica dovrebbe avere l'autorizzazione a tutti i dati ma nessuna autorizzazione operativa sull'oggetto per il file fisico CUSTMAST. L'utente con autorizzazione pubblica non può accedere direttamente al file CUSTMAST perché è necessaria l'autorizzazione *OBJOPR per aprire il file. L'autorizzazione dell'utente pubblico rende l'autorizzazione a tutti i dati potenzialmente disponibile per gli utenti del file logico.

L'autorizzazione per i file logici appare come la seguente:

```
                          Visualizzazione autorizzazione oggetto

Oggetto . . . . . :   CUSTINFO      Proprietario. . . . . :   OWNAR
  Libreria  . . . . :   CUSTLIB       Gruppo principale  . . . :   *NONE
Tipo oggetto  . . . . :   *FILE         Unità ASP . . . . . :   *SYSBAS

Oggetto protetto da elenco di autorizzazioni . . . . . :   *NONE

                        Autorizzazione
Utente        Gruppo   oggetto
*PUBLIC     *USE
```

```
                          Visualizzazione autorizzazione oggetto

Oggetto . . . . . :   CUSTCRDT      Proprietario  . . . . . :   OWNAR
  Libreria  . . . . :   CUSTLIB       Gruppo principale  . . . :   DPTAR
Tipo oggetto  . . . . :   *FILE         Unità ASP . . . . . :   *SYSBAS

Oggetto protetto da elenco di autorizzazioni . . . . . :   *NONE

                        Autorizzazione
Utente        Gruppo   oggetto
DPTAR                   *CHANGE
*PUBLIC     *USE
```

```
                          Visualizzazione autorizzazione oggetto

Oggetto . . . . . :   CUSTSLS       Proprietario  . . . . . :   OWNSM
  Libreria  . . . . :   CUSTLIB      Gruppo principale  . . . :   DPTSM
Tipo oggetto  . . . . :   *FILE        Unità ASP . . . . . :   *SYSBAS

Oggetto protetto da elenco di autorizzazioni . . . . . :   *NONE

                       Autorizzazione
Utente        Gruppo   oggetto
DPTSM                   *CHANGE
*PUBLIC     *USE
```

Non è necessario che il profilo gruppo, quale DPTSM, sia il gruppo principale per il file logico per far funzionare questo schema di autorizzazioni. Tuttavia, utilizzando l'autorizzazione del gruppo principale non sarà necessario ricercare le autorizzazioni private sia per l'utente che tenta di accedere al file che per il gruppo dell'utente. "Caso 2: Utilizzo autorizzazione gruppo principale" a pagina 200 mostra in che modo l'utilizzo dell'autorizzazione del gruppo principale influisca con il processo di controllo dell'autorizzazione.

È possibile specificare le autorizzazioni di dati per i file logici iniziando con la V3R1 del programma su licenza i5/OS. Quando un file logico precedente alla versione V3R1 viene ripristinato su un sistema V3R1 o successivo, il sistema converte i file logici al primo accesso del file logico. Il sistema fornisce tutte le autorizzazioni per i dati.

Per utilizzare i file logici come strumento di sicurezza, effettuare quanto segue:

- Concedere tutte le autorizzazioni dati ai sottostanti file fisici.
- Revocare *OBJOPR dai file fisici. In questo modo si impedisce agli utenti non autorizzati di accedere direttamente ai file fisici.
- Concedere le autorizzazioni dati appropriate ai file logici. Revocare tutte le autorizzazioni non desiderate.
- Concedere l'autorizzazione *OBJOPR ai file logici.

Informazioni correlate

DB2 Universal Database for iSeries

Sovrascrittura dei file

È possibile utilizzare i comandi di sovrascrittura per fare in modo che un programma utilizzi un file differente con lo stesso formato.

Ad esempio, presupporre che un programma nell'applicazione Contratti e Tariffe nell'azienda di giocattoli JKL scriva le informazioni sulle tariffe su un file di lavoro prima di apportare le modifiche alle tariffe. Un utente con accesso a una riga comandi che ha intenzione di rilevare informazioni private potrebbe utilizzare un comando di sovrascrittura per fare in modo che il programma scriva i dati su un file differente in una libreria controllata dall'utente.

È possibile assicurarsi che il programma elabori i file corretti utilizzando i comandi di sovrascrittura con SECURE(*YES) prima dell'esecuzione del programma, in tal modo tali file sono protetti dagli effetti dei comandi di sovrascrittura file precedentemente richiamati. Se si utilizza SECURE(*NO), tali file non sono protetti da altre sovrascritture file. I relativi valori possono essere sovrascritti dagli effetti dei comandi di sovrascrittura file precedentemente richiamati.

Sicurezza file e SQL

È necessario prestare attenzione alla sicurezza file quando si utilizza un programma CL che adotta l'autorizzazione per avviare una SQL o un Query Manager. Entrambi questi programmi query consentono agli utenti di specificare un nome file. Pertanto, l'utente può accedere a qualsiasi file per cui il profilo adottato dispone di autorizzazione.

L'SQL (Structured Query Language) utilizza file a riferimento incrociato per tenere traccia dei file di database e dei relativi rapporti. Viene fatto riferimento a tali file come catalogo SQL. L'autorizzazione pubblica per il catalogo SQL è *READ. Ciò significa che qualsiasi utente che dispone dell'accesso all'interfaccia SQL può visualizzare i nomi e le descrizioni testo per tutti i file sul sistema. Il catalogo SQL non influenza l'autorizzazione normale necessaria per accedere al contenuto dei file di database.

Pianificazione dei profili di gruppo

Il profilo di gruppo è uno strumento utile da utilizzare quando diversi utenti dispongono di requisiti sulla sicurezza simili. È possibile creare direttamente file di gruppo o rendere un profilo esistente un profilo di gruppo. Quando si utilizzano profili di gruppo, è possibile gestire in maniera più efficiente l'autorizzazione e ridurre il numero di singole autorizzazioni private per gli oggetti.

I file di gruppo sono particolarmente utili quando i requisiti del lavoro e i membri del gruppo cambiano. Ad esempio, se i membri di un reparto sono responsabili di un'applicazione, è possibile impostare un profilo di gruppo per il reparto. Quando gli utenti si uniscono o lasciano il reparto, il campo del profilo di gruppo nei relativi profili utente può essere modificato. Questo è un metodo di gestione più semplice rispetto alla rimozione di singole autorizzazioni dai profili utente.

Un profilo di gruppo è semplicemente un tipo speciale di profilo utente. Diventa un profilo di gruppo quando si verifica una delle seguenti situazioni:

- Un altro profilo lo indica come profilo di gruppo
- L'utente gli assegna un numero di identificazione gruppo (gid).

Ad esempio:

1. Creare un profilo denominato GRPIC:
   ```
   CRTUSRPRF GRPIC
   ```
2. Quando il profilo viene creato, è un profilo ordinario e non un profilo di gruppo.
3. Indicare GRPIC come il profilo di gruppo per un altro profilo di gruppo:
   ```
   CHGUSRPRF USERA GRPPRF(GRPIC)
   ```
4. Il sistema ora considera il GRPIC come profilo di gruppo e gli assegna un gid.

Concetti correlati

"Profili di gruppo" a pagina 5
Un *profilo di gruppo* è un tipo speciale di profilo utente. Piuttosto che fornire l'autorizzazione a ciascun utente singolarmente, è possibile utilizzare un profilo di gruppo per definire l'autorizzazione per un gruppo di utenti.

Considerazioni per gruppi principali per gli oggetti

Qualsiasi oggetto sul sistema può disporre di un gruppo principale. L'autorizzazione del gruppo principale fornisce prestazioni migliori se il gruppo principale è il primo gruppo per molti utenti di un oggetto.

Spesso, un gruppo di utenti è responsabile di alcune informazioni relative al sistema, quali le informazioni sul cliente. Tale gruppo necessita di più autorizzazioni per visualizzare le informazioni rispetto agli utenti di sistema. Utilizzando l'autorizzazione del gruppo principale, è possibile impostare questo tipo di schema di autorizzazioni senza influenzare le prestazioni del controllo dell'autorizzazione.

Attività correlate

"Caso 2: Utilizzo autorizzazione gruppo principale" a pagina 200
Questo caso illustra come utilizzare l'autorizzazione gruppo principale.

Considerazioni per profili di più gruppi

Utilizzando i profili di gruppo, è possibile gestire in maniera più efficiente l'autorizzazione e ridurre il numero di singole autorizzazioni private per gli oggetti. Tuttavia, un utilizzo non appropriato dei profili di gruppo potrebbe avere un effetto negativo sulle prestazioni del controllo autorizzazione. Questo argomento fornisce alcuni consigli sull'utilizzo di profili di più gruppi.

Un utente può essere membro di un massimo di 16 gruppi: il primo gruppo (parametro GRPPRF nel profilo utente) e di 15 gruppi supplementari (parametro SUPGRPPRF nel profilo utente).

Seguire questi consigli quando si utilizzano profili di più gruppi:

- Tentare di utilizzare più gruppi insieme all'autorizzazione del gruppo principale ed eliminare l'autorizzazione privata per gli oggetti.
- Pianificare attentamente la sequenza con cui i profili di gruppo verranno assegnati a un utente. Il primo gruppo dell'utente deve essere relativo all'assegnazione principale dell'utente e agli oggetti utilizzati più frequentemente. Ad esempio, un utente denominato WAGNERB effettua un lavoro di inventario regolarmente ed occasionalmente effettua un lavoro di immissione ordini. Il profilo necessario per l'autorizzazione inventario (DPTIC) dovrebbe essere il primo gruppo del WAGNERB. Il profilo necessario per un lavoro di immissione ordini (DPTOE) dovrebbe essere il primo gruppo supplementare del WAGNERB.

  Nota: la sequenza in cui vengono specificate le autorizzazioni private per un oggetto non influenza il controllo dell'autorizzazione.
- Se si desidera utilizzare più gruppi, studiare il processo di controllo autorizzazione descritto in "Controllo dell'autorizzazione da parte del sistema" a pagina 182. Comprendere in che modo l'utilizzo di più gruppi insieme ad altre tecniche di autorizzazione, quali gli elenchi di autorizzazioni, potrebbe influenzare le prestazioni del sistema.

Raggruppamento di autorizzazioni speciali per i membri del profilo di gruppo

Le autorizzazioni speciali sono cumulative per gli utenti che sono membri di più gruppi.

Le autorizzazioni speciali dei profili di gruppo sono disponibili per i membri di tale gruppo. I profili utente membri di uno o più gruppi dispongono di proprie autorizzazioni speciali, oltre alle autorizzazioni speciali dei profili di gruppo di cui è membro un utente. Le autorizzazioni speciali sono cumulative per gli utenti che sono membri di più gruppi. Ad esempio, presupporre che il profilo GROUP1 disponga dell'autorizzazione speciale *JOBCTL, il profilo GROUP3 di *AUDIT e il profilo GROUP16 di *IOSYSCFG. Un profilo utente che dispone di tutti e tre i profili come profili di gruppo dispone delle autorizzazioni speciali *JOBCTL, *AUDIT e *IOSYSCFG.

Nota: se un membro di un gruppo è proprietario di un programma, il programma adotta solo l'autorizzazione del proprietario. Le autorizzazioni del proprietario del gruppo non vengono adottate.

Utilizzo di un profilo individuale come profilo di gruppo

Si consiglia di creare i profili come profili di gruppo piuttosto che rendere profili esistenti profili di gruppo.

È possibile che un utente specifico disponga di tutte le autorizzazioni necessarie per un gruppo di utenti e che sia tentato di rendere il profilo utente un profilo di gruppo. Tuttavia, l'utilizzo di singoli profili come profili di gruppo potrebbe causare dei problemi in futuro:

- Se l'utente il cui profilo viene utilizzato come profilo di gruppo modifica le responsabilità, è necessario indicare un nuovo profilo come profilo di gruppo, modificare le autorizzazioni e trasferire il proprietario dell'oggetto.
- A tutti i membri del gruppo viene automaticamente concessa l'autorizzazione per qualsiasi oggetto creato dal profilo di gruppo. L'utente il cui profilo è il profilo di gruppo non è più in grado di gestire oggetti privati, a meno che tale utente non escluda in maniera specifica altri utenti.

Tentare di pianificare in anticipo i profili di gruppo. Creare profili di gruppo specifici con la parola d'ordine *NONE. Se dopo l'esecuzione di un'applicazione ci si rende conto che un utente dispone di autorizzazioni che dovrebbero appartenere a un gruppo di utenti, effettuare quanto segue:

1. Creare un profilo di gruppo.
2. Utilizzare il comando GRTUSRAUT per fornire le autorizzazioni dell'utente al profilo utente.
3. Rimuovere le autorizzazioni private dall'utente, poiché non sono più necessarie. Utilizzare il comando RVKOBJAUT o EDTOBJAUT.

Confronto tra i profili di gruppo e gli elenchi di autorizzazioni

I profili di gruppo vengono utilizzati per semplificare la gestione dei profili utente con requisiti di sicurezza simili. Gli elenchi di autorizzazioni vengono utilizzati per proteggere gli oggetti con requisiti di sicurezza simili.

La Tabella 129 mostra le caratteristiche dei due metodi.

Tabella 129. Confronto tra l'elenco autorizzazioni e il profilo di gruppo

Voce confrontata	Elenco di autorizzazioni	Profilo di gruppo
Utilizzato per proteggere più oggetti	Sì	Sì
L'utente può appartenere a più di uno	Sì	Sì
L'autorizzazione privata sovrascrive altre autorizzazioni	Sì	Sì
All'utente deve essere assegnata indipendentemente l'autorizzazione	Sì	No
Le autorizzazioni specificate sono le stesse per tutti gli oggetti	Sì	No
L'oggetto può essere protetto da più di uno	No	Sì
L'autorizzazione può essere specificata quando viene creato l'oggetto	Sì	Sì[1]
Può proteggere tutti i tipi di oggetti	No	Sì
L'associazione all'oggetto viene cancellata quando viene cancellato l'oggetto	Sì	Sì
L'associazione all'oggetto viene salvata quando viene salvato l'oggetto	Sì	Sì [2]

[1] È possibile fornire al profilo di gruppo l'autorizzazione quando viene creato un oggetto utilizzando il parametro GRPAUT nel profilo dell'utente che crea l'oggetto.

[2] L'autorizzazione del gruppo principale viene salvata con l'oggetto. Le autorizzazioni gruppo private vengono salvate se è specificato PVTAUT(*YES) sul comando di salvataggio.

Per l'elenco di autorizzazioni della voce ″L'autorizzazione può essere specificata quando viene creato l'oggetto″:

- Per assegnare un elenco di autorizzazioni a un oggetto basato su una libreria, specificare AUT (*LIBCRTAUT) sul comando CRTxxxx e CRTAUT (nome-elenco-autorizzazioni) per la libreria. Alcuni oggetti, come ad esempio gli elenchi di convalida, non possono utilizzare un valore di *LIBCRTAUT nel comando CRT.
- Per assegnare un elenco di autorizzazioni a un oggetto basato su un indirizzario, specificare il valore *INDIR per i parametri DTAAUT e OBJAUT sul comando MKDIR. In questo modo, l'elenco di autorizzazioni protegge sia l'indirizzario principale che quello nuovo. Il sistema non consente di specificare un elenco di autorizzazioni arbitrario quando viene creato un oggetto.

Pianificazione della sicurezza per i programmatori

I programmatori sono un problema per il responsabile della riservatezza. Grazie alle loro conoscenze, potrebbero essere in grado di superare le procedure di sicurezza non progettate attentamente.

I programmatori possono superare la sicurezza per accedere ai dati di cui hanno necessità per effettuare delle verifiche. Inoltre, possono evitare le normali procedure che assegnano le risorse di sistema per rendere migliori le prestazioni relative ai propri lavori. Spesso, la sicurezza viene vista dai programmatori come ostacolo per eseguire le attività richieste dai relativi lavori, quale la verifica delle applicazioni. Tuttavia, se ai programmatori si fornisce troppa autorizzazione per il sistema, è possibile che si vadano a danneggiare i principi di sicurezza relativi alla separazione delle mansioni. Inoltre, si consente a un programmatore di installare programmi non autorizzati.

Seguire queste istruzioni quando si imposta un ambiente per i programmatori delle applicazioni:

- Non concedere tutte le autorizzazioni ai programmatori. Se è necessario fornire ai programmatori autorizzazioni speciali, concedere loro solo l'autorizzazione speciale richiesta per eseguire lavori o attività assegnati al programmatore.
- Non utilizzare il profilo utente QPGMR come profilo di gruppo per i programmatori.
- Utilizzare le librerie di verifica e non consentire l'accesso alle librerie di produzione.
- Creare le librerie del programmatore e utilizzare un programma che adotti l'autorizzazione per copiare i dati di produzione selezionati sulle librerie del programmatore per effettuare la verifica.
- Se le prestazioni interattive risultano un problema, modificare i comandi per la creazione dei programmi in modo da poterli eseguire in batch:

  ```
  CHGCMD CMD(CRTxxxPGM) ALLOW(*BATCH *BPGM)
  ```

- Effettuare il controllo della sicurezza della funzione dell'applicazione prima di spostare le applicazioni o le modifiche dei programmi dalle librerie di verifica a quelle di produzione.
- Utilizzare la tecnica del profilo di gruppo una volta sviluppata l'applicazione. Fare in modo che tutti i programmi dell'applicazione appartengano a un profilo di gruppo. Rendere i programmatori che lavorano sull'applicazione membri del gruppo e definire i profili utente del programmatore in modo che il relativo gruppo possieda tutti i nuovi oggetti creati (OWNER(*GRPPRF)). Quando un programmatore viene spostato da un progetto a un altro, è possibile modificare le informazioni sul gruppo nel profilo del programmatore. Consultare "Proprietà gruppo degli oggetti" a pagina 154 per ulteriori informazioni.
- Sviluppare un piano per assegnare la proprietà delle applicazioni quando vengono spostate nella produzione. Per controllare le modifiche apportate a un'applicazione di produzione, tutti gli oggetti dell'applicazione, inclusi i programmi, devono essere di proprietà del profilo utente designato per l'applicazione.

  Gli oggetti dell'applicazione non devono appartenere a un programmatore poiché quest'ultimo può accedervi senza controlli in un ambiente di produzione. Il profilo che gestisce l'applicazione potrebbe essere il profilo di un singolo responsabile per l'applicazione o potrebbe essere un profilo specificamente creato come proprietario dell'applicazione.

Gestione dei file di origine

Per proteggere le informazioni sul sistema, è necessario pianificare attentamente la sicurezza dei file di origine.

I file di origine sono importanti per l'integrità del sistema. Potrebbero inoltre costituire un assetto aziendale notevole, se sono state sviluppate o acquisite applicazioni personalizzate. I file di origine devono essere protetti come qualsiasi altro file importante sul sistema. Si consiglia di posizionare i file di origine in librerie separate e di controllare gli utenti che hanno l'autorizzazione per aggiornarli e spostarli nella produzione.

Quando viene creato un file di origine sul sistema, l'autorizzazione pubblica predefinita è *CHANGE. Ciò consente a tutti gli utenti di aggiornare qualsiasi membro di origine. Per impostazione predefinita, solo il proprietario del file di origine o un utente con un'autorizzazione speciale di *ALLOBJ può aggiungere o rimuovere i membri. In molti casi, questa autorizzazione predefinita per i file fisici di origine deve essere modificata. I programmatori che lavorano su un'applicazione necessitano dell'autorizzazione *OBJMGT per i file di origine per aggiungere nuovi membri. L'autorizzazione pubblica deve essere ridotta a *USE o *EXCLUDE, a meno che i file di origine non si trovino in una libreria controllata.

Protezione dei file jar e dei file di classe Java nell'IFS

Per eseguire un programma Java, sarà necessaria l'autorizzazione alla lettura (*R) per ogni file jar e di classe Java più l'autorizzazione all'esecuzione (*X) per ogni indirizzario nel percorso ai file jar e di classe Java. Se si utilizzano i file jar e i file di classe Java nell'IFS, è necessario proteggerli tramite le normali autorizzazioni all'oggetto.

Per proteggere i file Java, utilizzare il comando CHGAUT per proteggere gli indirizzari nel percorso e i file con attributi di autorizzazione all'oggetto. È possibile che sia necessaria l'autorizzazione alla lettura (*R) per i file jar e di classe Java per eseguire un programma Java. È possibile acquisire tale autorizzazione dall'autorizzazione pubblica del file o dall'autorizzazione privata. Un elenco di autorizzazioni è utile nell'impostazione di un'autorizzazione privata per un gruppo di utenti. Non fornire ad alcun utente l'autorizzazione alla scrittura (*W) dei file, a meno che a tali utenti sia consentito modificare il file.

È possibile utilizzare il parametro CHKPATH (livello di controllo sicurezza del percorso classe) sul comando RUNJVA per verificare che un'applicazione Java in esecuzione utilizzi i file corretti di CLASSPATH. È possibile utilizzare un valore CHKPATH(*SECURE) per impedire l'esecuzione di un programma Java se uno o più messaggi di avvertenza vengono inviati per ogni indirizzario presente nel CLASSPATH che dispone dell'autorizzazione pubblica alla scrittura.

Pianificazione della sicurezza per i programmatori di sistema o per i manager

È possibile limitare l'autorizzazione fornita ai programmatori di sistema o ai manager per proteggere i file sul sistema.

Per la maggior parte dei sistemi esiste un responsabile delle funzioni di manutenzione. Questa persona monitorizza l'utilizzo delle risorse del sistema, in particolare la memoria del disco, per assicurarsi che gli utenti rimuovano regolarmente oggetti non utilizzati per liberare spazio. I programmatori di sistema necessitano di un'autorizzazione ampia per osservare tutti gli oggetti sul sistema. Tuttavia, non è necessario che visualizzino il contenuto di tali oggetti.

È possibile utilizzare l'autorizzazione adottata per fornire una serie di comandi di visualizzazione per i programmatori di sistema, piuttosto che fornire autorizzazioni speciali nei profili utente.

Ad esempio, è possibile che Sue e Fred siano in grado di creare e modificare i profili utente senza fornire loro autorizzazioni speciali. Ciò è reso possibile eseguendo la seguente procedura.

1. Scrivere un comando o un programma che sia front end al comando CRT/CHGUSRPRF.
2. Fare in modo che il comando o il programma adotti un profilo in grado di eseguire le creazioni e le modifiche.
3. Autorizzare Sue e Fred al programma.

Quindi Sue e Fred possono eseguire l'attività solo tramite l'applicazione.

Utilizzo elenchi di convalida

Gli oggetti dell'elenco di convalida forniscono alle applicazioni un metodo per memorizzare in modo sicuro le informazioni di autenticazione utente.

Ad esempio, l'ICS (Internet Connection Server) utilizza gli elenchi di convalida per eseguire il concetto di un Utente internet. L'ICS può eseguire l'autenticazione di base prima di utilizzare una pagina Web. L'autenticazione di base richiede che gli utenti forniscano delle informazioni di autenticazione, quale la parola d'ordine, il PIN o il numero di account. È possibile memorizzare in maniera sicura il nome dell'utente e le informazioni di autenticazione in un elenco di convalida. L'ICS può utilizzare le informazioni nell'elenco di convalida piuttosto che richiedere agli utenti dell'ICS un ID utente e una parola d'ordine System i.

È possibile concedere o negare l'accesso a un utente internet al sistema dal server Web. Tuttavia, l'utente non dispone di autorizzazione a nessuna delle risorse System i o autorizzazione per collegarsi o eseguire lavori. Un profilo utente System i non viene mai creato per utenti internet.

Per creare e cancellare gli elenchi di convalida, è possibile utilizzare i comandi CL CRTVLDL (Creazione elenco di convalida) e DLTVLDL (Cancellazione elenco di convalida). Vengono inoltre fornite le API (Application Programming Interfaces) per consentire alle applicazioni di aggiungere, modificare, rimuovere, verificare (autenticare) e trovare le voci in un elenco di convalida.

Gli oggetti elenco di convalida sono disponibili per tutte le applicazioni da utilizzare. Ad esempio, se un'applicazione richiede una parola d'ordine, è possibile memorizzare le parole d'ordine dell'applicazione in un oggetto elenco di convalida piuttosto che sul file di database. L'applicazione può utilizzare le API dell'elenco di convalida per verificare una parola d'ordine dell'utente. Poiché l'elenco di convalida è codificato, questo sistema è più sicuro rispetto all'utilizzo della sola applicazione per verificare la parola d'ordine dell'utente.

È possibile memorizzare le informazioni di autenticazione in formato decodificabile. Se l'utente dispone della sicurezza appropriata, le informazioni di autenticazione possono essere decodificate e restituite all'utente.

Riferimenti correlati

"Conservazione sicurezza server (QRETSVRSEC)" a pagina 34
Il valore di sistema Conservazione sicurezza server (QRETSVRSEC) determina se le informazioni di autenticazione decodificabili associate ai profili utente o alle voci dell'elenco di convalida (*VLDL) possono essere conservate sul sistema host. Tale impostazione non comprende la parola d'ordine del profilo utente System i.

Informazioni correlate

Application programming interfaces

Limitazione dell'accesso a una funzione del programma

La limitazione dell'accesso a una funzione del programma consente di definire quale utente può utilizzare l'applicazione, le parti di un'applicazione o le funzioni di un programma.

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. La funzione passa attraverso i seguenti processi per effettuare la verifica.

- 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

La limitazione dell'accesso a una funzione del programma consente alle API di eseguire le seguenti attività: Per utilizzare tale funzione 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'utente esegue l'applicazione, prima che l'applicazione invochi il blocco di codice, l'applicazione richiama l'API di controllo utilizzo per verificare che l'utente disponga dell'autorizzazione di utilizzare la funzione associata al blocco di codice. 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.

Il responsabile di sistema specifica a chi è consentito o negato l'accesso a una funzione. L'amministratore può utilizzare il comando WRKFCNUSG (Gestione informazioni sull'utilizzo della funzione) per gestire l'accesso alle funzioni del programma o utilizzare la gestione applicazione in System i Navigator.

Informazioni correlate

Gestione applicazioni

Capitolo 8. Copia di riserva e ripristino delle informazioni sulla sicurezza

Il salvataggio delle informazioni sulla sicurezza è importante come il salvataggio dei dati. In alcune situazioni, potrebbe risultare necessario ripristinare i profili utente, le autorizzazioni oggetto e i dati sul sistema. Se le informazioni sulla sicurezza non sono salvate, è possibile che sia necessario creare nuovamente manualmente i profili utente e le autorizzazioni oggetto. Questa operazione richiederà del tempo, potrebbero verificarsi errori e si potrebbe influenzare la stabilità della sicurezza.

Questo argomento include le informazioni sui seguenti argomenti:

- Come salvare e ripristinare le informazioni sulla sicurezza
- In che modo la sicurezza influenza il salvataggio e il ripristino degli oggetti
- Le questioni di sicurezza associate all'autorizzazione speciale *SAVSYS

Per pianificare procedure adeguate per la copia di riserva e il ripristino per le informazioni sulla sicurezza è necessario conoscere il modo in cui le informazioni vengono memorizzate, salvate e ripristinate.

La Tabella 130 mostra i comandi utilizzati per salvare e ripristinare le informazioni sulla sicurezza. Le sezioni che seguono mostrano nei dettagli come salvare e ripristinare le informazioni sulla sicurezza.

Tabella 130. Come salvare e ripristinare le informazioni sulla sicurezza

	Comandi di salvataggio e ripristino utilizzati					
Informazioni sulla sicurezza salvate o ripristinate	**SAVSECDTA SAVSYS**	**SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG**	**RSTUSRPRF**	**RSTOBJ RSTLIB RSTDLO RSTCFG**	**RSTAUT**	**RSTDFROBJ**
Profili utente	X		X			
Proprietario oggetto [1]		X		X		X
Gruppo principale [1]		X		X		X
Autorizzazioni pubbliche [1]		X		X		X
Autorizzazioni private[3]	X	X	X	X	X	X
Elenchi di autorizzazioni	X		X			
Archivi autorizzazioni	X		X			
Collegamento all'elenco di autorizzazioni e agli archivi autorizzazioni		X		X		
Valore di controllo oggetto		X		X		
Informazioni sulla registrazione della funzione [2]		X		X		
Informazioni sull'utilizzo della funzione	X		X		X	
Elenchi di convalida		X		X		
Voci autenticazione server	X		X			

Tabella 130. Come salvare e ripristinare le informazioni sulla sicurezza (Continua)

Informazioni sulla sicurezza salvate o ripristinate	Comandi di salvataggio e ripristino utilizzati					
	SAVSECDTA SAVSYS	**SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG**	**RSTUSRPRF**	**RSTOBJ RSTLIB RSTDLO RSTCFG**	**RSTAUT**	**RSTDFROBJ**
[1] I comandi SAVSECDTA, SAVSYS e RSTUSRPRF salvano e ripristinano la proprietà, il gruppo principale, l'autorizzazione del gruppo principale e l'autorizzazione pubblica per i seguenti tipi di oggetto: profilo utente (*USRPRF), elenco di autorizzazioni (*AUTL) e archivio autorizzazioni (*AUTHLR).						
[2] L'oggetto da salvare/ripristinare è QUSEXRGOBJ, immettere *EXITRG nella libreria QUSRSYS.						
[3] Le autorizzazioni private per tutti gli oggetti vengono salvate con SAVSECDTA. RSTUSRPRF ripristina le informazioni sulle autorizzazioni necessarie per ripristinare le autorizzazioni private. Le autorizzazioni private vengono ripristinate con RSTAUT. Le autorizzazioni private per gli oggetti singoli possono essere salvate con i comandi SAV, SAVLIB, SAVOBJ e SAVCHGOBJ. Le autorizzazioni private per gli oggetti singoli possono essere ripristinate con i comandi RST, RSTLIB e RSTOBJ se sono state salvate con il comando di salvataggio.						

Informazioni correlate

Copia di riserva e ripristino

PDF Copia di riserva e ripristino

Come memorizzare le informazioni sulla sicurezza

Per pianificare procedure adeguate per la copia di riserva e il ripristino per le informazioni sulla sicurezza è necessario conoscere il modo in cui le informazioni vengono memorizzate e salvate.

Le informazioni sulla sicurezza vengono memorizzate con gli oggetti, i profili utente e gli elenchi di autorizzazioni:

Informazioni sull'autorizzazione memorizzate con l'oggetto:

- Autorizzazione pubblica
- Nome proprietario
- Autorizzazione del proprietario per l'oggetto
- Nome gruppo principale
- Autorizzazione del gruppo principale per l'oggetto
- Nome elenco di autorizzazioni
- Valore di controllo oggetto
- Se è presente un'autorizzazione privata
- Se un'autorizzazione privata è inferiore rispetto a quella pubblica

Informazioni sull'autorizzazione memorizzate con il profilo utente:

- *Informazioni di intestazione*:
  - Gli attributi del profilo utente mostrati sul pannello Creazione profilo utente.
  - L'uid e il gid.
- *Informazioni sull'autorizzazione privata*:
  - Autorizzazione privata per gli oggetti. Ciò include l'autorizzazione privata negli elenchi di autorizzazioni.
- *Informazioni sulla proprietà*:

  - Elenco di oggetti di proprietà dell'utente
  - Per ogni oggetto di proprietà dell'oggetto, un elenco di utenti con autorizzazione privata per l'oggetto.
- *Informazioni sul gruppo principale*:
  - Elenco di oggetti per cui il profilo è il gruppo principale.
- *Informazioni sul controllo*:
  - Valore di controllo azione
  - Valore di controllo oggetto
- *Informazioni sull'utilizzo della funzione*:
  - Impostazioni sull'utilizzo per le funzioni registrate.
- *Informazioni autenticazione server*:
  - Voci di autenticazione server.

Informazioni sull'autorizzazione memorizzate con gli elenchi di autorizzazioni:

- Le informazioni sull'autorizzazione normale memorizzate in qualsiasi oggetto, quale l'autorizzazione pubblica e il proprietario.
- Elenco di tutti gli oggetti protetti dall'elenco di autorizzazioni.

Concetti correlati

"Informazioni aggiuntive associate a un profilo utente" a pagina 123
Questo argomento discute le autorizzazioni private, informazioni sull'oggetto posseduto e informazioni sull'oggetto del gruppo principale associate al profilo utente.

Salvataggio delle informazioni sulla sicurezza

Le informazioni sulla sicurezza vengono salvate diversamente nel supporto magnetico di salvataggio rispetto a come vengono salvate sul sistema. Quando si salvano i profili utente, le informazioni sull'autorizzazione privata memorizzate con il profilo utente vengono formattate in una tabella di autorizzazioni.

Una tabella di autorizzazioni viene creata e salvata per ogni profilo utente che dispone di autorizzazioni private. Questa nuova formattazione e salvataggio delle informazioni sulla sicurezza potrebbe durare a lungo se sono presenti molte autorizzazioni private sul sistema.

Segue un esempio di come vengono salvate le informazioni sulla sicurezza sul supporto magnetico di salvataggio:

Informazioni sull'autorizzazione salvate con l'oggetto:

- Autorizzazione pubblica
- Nome proprietario
- Autorizzazione del proprietario per l'oggetto
- Nome gruppo principale
- Autorizzazione del gruppo principale per l'oggetto
- Nome elenco di autorizzazioni
- Autorizzazioni livello campo
- Valore di controllo oggetto
- Se è presente un'autorizzazione privata
- Se un'autorizzazione privata è inferiore rispetto a quella pubblica
- L'autorizzazione privata per l'oggetto, se PVTAUT(*YES) viene specificato sul comando SAVxxx

Informazioni sull'autorizzazione salvate con l'elenco di autorizzazioni:

- Le informazioni sull'autorizzazione normale memorizzate in qualsiasi oggetto, quale l'autorizzazione pubblica, il proprietario e il gruppo principale.

Informazioni sull'autorizzazione salvate con il profilo utente:

- Gli attributi del profilo utente mostrati sul pannello Creazione profilo utente.
- Altre informazioni sull'applicazione associate al profilo utente. Ad esempio:
  - Voci di autenticazione server
  - Voci di informazioni applicazione utente che vengono aggiunte all'API di aggiornamento informazioni applicazione utente (QsyUpdateUserApplicationInfo)

Tabella autorizzazioni salvata con il profilo utente:

- Un record per ogni autorizzazione privata del profilo utente, incluse le impostazioni sull'utilizzo per la registrazione delle funzioni.

Informazioni sulla registrazione della funzione salvate con l'oggetto QUSEXRGOBJ:

- È possibile salvare le informazioni sulla registrazione della funzione salvando l'oggetto QUSEXRGOBJ *EXITRG in QUSRSYS.

Ripristino delle informazioni sulla sicurezza

Spesso, per ripristinare il sistema è necessario ripristinare anche i dati e le informazioni sulla sicurezza associate.

Di solito, la sequenza per il ripristino è:

1. Ripristino dei profili utente e degli elenchi di autorizzazioni (RSTUSRPRF USRPRF(*ALL)).
2. Ripristino degli oggetti (RSTCFG, RSTLIB, RSTOBJ, RSTDLO o RST).
3. Ripristino delle autorizzazioni private per gli oggetti (RSTAUT).

Nota: utilizzando i codici di esempio, si accettano i termini presenti nel Capitolo 10, "Informazioni sull'esonero di responsabilità e licenza codice", a pagina 329.

Informazioni correlate

Copia di riserva e ripristino

Ripristino profili utente

È possibile che vengano apportate delle modifiche ad un profilo utente quando viene ripristinato.

Si applicano le seguenti regole:

- Se i profili sono stati ripristinati individualmente (RSTUSRPRF USRPRF(*ALL) non specificato), SECDTA(*PWDGRP) non è necessario e il profilo ripristinato non esiste sul sistema, questi campi vengono modificati in *NONE:
  - Nome profilo gruppo (GRPPRF)
  - Parola d'ordine (PASSWORD)
  - Parola d'ordine documento (DOCPWD)
  - Profili di gruppo supplementari (SUPGRPPRF)

  Le parole d'ordine del prodotto vengono modificate in *NONE, pertanto non saranno corrette dopo il ripristino di un singolo profilo utente che non era presente sul sistema.
- Se i profili sono stati ripristinati singolarmente (RSTUSRPRF USRPRF(*ALL) non è specificato) SECDTA(*PWDGRP) non è necessario e il profilo è presente sul sistema, la parola d'ordine, la parola d'ordine del documento e il profilo di gruppo non vengono modificati.

È possibile ripristinare singolarmente i profili utente e ripristinare le informazioni sul gruppo e sulla parola d'ordine dal supporto magnetico di salvataggio specificando il parametro SECDTA(*PWDGRP) sul comando RSTUSRPRF. Sono necessarie le autorizzazioni speciali *ALLOBJ e *SECADM per ripristinare le informazioni sul gruppo e sulla parola d'ordine quando si ripristinano singolarmente i profili. Le parole d'ordine del prodotto ripristinate con il profilo utente, non saranno corrette dopo il ripristino di un singolare profilo utente che era presente sul sistema, a meno che non venga specificato il parametro SECDTA(*PWDGRP) sul comando RSTUSRPRF.

- Se tutti i profili utente vengono ripristinati sul sistema, tutti i campi in qualsiasi profilo già presente sul sistema vengono ripristinati dal supporto magnetico di salvataggio, inclusa la parola d'ordine.

  Attenzione:

  1. se i profili utente vengono salvati da un sistema con un livello di parola d'ordine differente (valore di sistema QPWDLVL) rispetto al sistema ripristinato, è possibile che la parola d'ordine non sia valida sul sistema ripristinato. Ad esempio, se il profilo utente salvato apparteneva a un sistema con una parola d'ordine di livello 2, la parola d'ordine dell'utente è "Questa è la mia parola d'ordine". Questa parola d'ordine non è valida su un sistema con parola d'ordine di livello 0 o 1.
  2. tenere un record della parola d'ordine del responsabile della riservatezza (QSECOFR) associata a ogni versione delle informazioni sulla sicurezza salvate. In questo modo viene assicurata la possibilità di accedere al sistema se è necessario completare un'operazione di ripristino.

  È possibile utilizzare il DST (Dedicated Service Tool) per ripristinare la parola d'ordine per il profilo QSECOFR.
- Se un profilo è presente sul sistema, l'operazione di ripristino non modifica l'uid o il gid.
- Se un profilo non è presente sul sistema, l'uid e il gid per un profilo vengono ripristinati dal supporto magnetico di salvataggio. Se l'uid o il gid sono già presenti sul sistema, il sistema crea un nuovo valore ed emette il messaggio (CPI3810).
- L'autorizzazione speciale *ALLOBJ viene rimossa dai profili utente ripristinati su un sistema con livello di sicurezza 30 o superiore in entrambi le seguenti situazioni:
  - Il profilo è stato salvato da un sistema differente e l'utente che sta eseguendo RSTUSRPRF non dispone delle autorizzazioni speciali *ALLOBJ e *SECADM.
  - Il profilo è stato salvato dallo stesso sistema con livello di sicurezza 10 o 20.

  Attenzione: il sistema utilizza il numero di serie della macchina sul sistema e sul supporto magnetico di salvataggio per determinare se gli oggetti sono stati ripristinati sullo stesso sistema o su un sistema differente.

  L'autorizzazione speciale *ALLOBJ non viene rimossa da questi profili utente forniti da IBM:
  - profilo utente QSYS (sistema)
  - profilo utente QSECOFR (responsabile della riservatezza)
  - profilo utente QLPAUTO (installazione automatica programma su licenza)
  - profilo utente QLPINSTALL (installazione programma su licenza)

  Informazioni correlate

  Reimpostazione della parola d'ordine del profilo utente QSECOFR i5/OS

Ripristino degli oggetti

Quando si ripristina un oggetto su un sistema, il sistema utilizza le informazioni sull'autorizzazione memorizzate sull'oggetto. Questo argomento descrive le regole applicabili alle informazioni sulle autorizzazioni durante il ripristino degli oggetti.

È necessario considerare quanto segue per la sicurezza dell'oggetto ripristinato:

Proprietario oggetto:

- Se il profilo proprietario dell'oggetto esiste sul sistema, la proprietà viene ripristinata su tale profilo.
- Se il profilo proprietario non è presente sul sistema, la proprietà dell'oggetto viene fornita al profilo utente QDFTOWN (proprietario predefinito).
- Se l'oggetto è presente sul sistema e il proprietario del sistema è diverso dal proprietario sul supporto magnetico di salvataggio, l'oggetto non viene ripristinato a meno che non venga specificato ALWOBJDIF(*ALL) o ALWOBJDIF(*OWNER). In questo caso, l'oggetto viene ripristinato e viene utilizzato il proprietario sul sistema.
- Consultare "Ripristino dei programmi" a pagina 270 per ulteriori considerazione sul ripristino dei comandi.

Gruppo principale:

Per un oggetto che non è presente sul sistema:
- Se il profilo che corrisponde al gruppo principale dell'oggetto è presente sul sistema, il valore del gruppo principale e l'autorizzazione vengono ripristinati per tale oggetto.
- Se il profilo che corrisponde al gruppo principale non è presente sul sistema:
  - Il gruppo principale per l'oggetto viene impostato su nessuno.
  - L'autorizzazione del gruppo principale viene impostata su nessuna autorizzazione.

Quando viene ripristinato un oggetto esistente, il gruppo principale per l'oggetto non viene modificato dall'operazione di ripristino.

Autorizzazione pubblica:
- Se l'oggetto ripristinato non è presente sul sistema, l'autorizzazione pubblica viene impostata sull'autorizzazione pubblica dell'oggetto salvato.
- Se l'oggetto ripristinato è presente ed è stato sostituito, l'autorizzazione pubblica non viene modificata. L'autorizzazione pubblica dalla versione salvata dell'oggetto non viene utilizzata.
- Il CRTAUT per la libreria non viene utilizzato quando si ripristinano gli oggetti sulla libreria.

Elenco di autorizzazioni:
- Se un oggetto, che non sia un documento o una cartella, è già presente sul sistema ed è collegato all'elenco di autorizzazioni, il parametro ALWOBJDIF determina il risultato:
  - Se viene specificato ALWOBJDIF(*NONE), l'oggetto esistente deve avere lo stesso elenco di autorizzazioni dell'oggetto salvato. Se così non fosse, l'oggetto non viene ripristinato.
  - Se viene specificato ALWOBJDIF(*ALL) o ALWOBJDIF(*OWNER), l'oggetto viene ripristinato. L'oggetto è collegato all'elenco di autorizzazioni associato all'oggetto esistente.
- Se viene ripristinato un documento o una cartella già presente sul sistema, si utilizza l'elenco di autorizzazioni associato all'oggetto sul sistema. L'elenco di autorizzazioni dal documento o cartella salvati non viene utilizzato.
- Se l'elenco di autorizzazioni non è presente sul sistema, l'oggetto viene ripristinato senza che venga collegato a un elenco di autorizzazioni e l'autorizzazione pubblica viene modificata in *EXCLUDE.
- Se l'oggetto è stato ripristinato sullo stesso sistema in cui era stato salvato, l'oggetto viene collegato nuovamente all'elenco di autorizzazioni.
- Se l'oggetto è stato ripristinato su un sistema differente, viene utilizzato il parametro ALWOBJDIF sul comando di ripristino per determinare se l'oggetto è collegato all'elenco di autorizzazioni:
  - Se viene specificato ALWOBJDIF(*ALL) o ALWOBJDIF(*OWNER), l'oggetto viene collegato all'elenco di autorizzazioni.
  - Se viene specificato ALWOBJDIF(*NONE), l'oggetto non viene collegato all'elenco di autorizzazioni e l'autorizzazione pubblica dell'oggetto viene modificata in *EXCLUDE.

Autorizzazioni private:

- L'autorizzazione privata viene salvata con i profili utenti e con gli oggetti se si specifica PVTAUT(*YES) sul comando SAVxxx.
- Se i profili utente dispongono dell'autorizzazione privata per un oggetto ripristinato, solitamente, tali autorizzazioni private non vengono interessate. È possibile che ripristinando alcuni tipi di programmi vengano revocate le autorizzazioni private.
- Se un oggetto viene cancellato dal sistema, l'autorizzazione privata per l'oggetto non sarà più presente sul sistema. Quando un oggetto viene cancellato, tutte le autorizzazioni private per l'oggetto vengono rimosse dai profili utente. Se l'oggetto viene ripristinato da una versione di salvataggio, è possibile ripristinare le autorizzazioni private se durante il salvataggio dell'oggetto è stato specificato PVTAUT(*YES).
- Se risulta necessario recuperare le autorizzazioni private e tali autorizzazioni non sono state salvate con l'oggetto, è necessario utilizzare il comando RSTAUT (Ripristino autorizzazione). La sequenza normale è la seguente:
  1. Ripristino profili utente
  2. Ripristino oggetti
  3. Ripristino autorizzazione

Controllo oggetto:

- Se l'oggetto ripristinato non è presente sul sistema, il valore di controllo oggetto (OBJAUD) dell'oggetto salvato viene ripristinato.
- Se l'oggetto ripristinato non è presente ed è stato sostituito, il valore di controllo oggetto non viene modificato. Il valore OBJAUD della versione salvata dell'oggetto non viene ripristinato.
- Se una libreria o un indirizzario ripristinato non è presente sul sistema, il valore di creazione controllo oggetto o indirizzario (CRTOBJAUD) per la libreria o l'indirizzario viene ripristinato.
- Se una libreria o un indirizzario ripristinato è presente ed è stato sostituito, il valore CRTOBJAUD per la libreria o per l'indirizzario non viene ripristinato. Viene utilizzato il valore CRTOBJAUD per la libreria o l'indirizzario esistente.

Archivio autorizzazioni:

- Se un file viene ripristinato ed è presente un archivio autorizzazioni per tale nome file e per la libreria su cui è stato ripristinato, il file viene collegato all'archivio autorizzazioni.
- Le informazioni sull'autorizzazione associate all'archivio autorizzazioni sostituiscono l'autorizzazione pubblica e le informazioni sul proprietario salvate nel file.

Oggetti dominio utente:

Il sistema limita gli oggetti dominio utente (*USRSPC, *USRIDX e *USRQ) alle librerie specificate nel valore di sistema QALWUSRDMN. Se una libreria viene rimossa dal valore di sistema QALWUSRDMN dopo il salvataggio di un oggetto dominio utente di tipo *USRSPC, *USRIDX o *USRQ, il sistema modifica l'oggetto in dominio di sistema una volta ripristinato.

Informazioni sulla funzione della registrazione:

È possibile ripristinare le informazioni sulla registrazione della funzione mediante il ripristino dell'oggetto QUSEXRGOBJ *EXITRG su QUSRSYS. Questa operazione ripristina tutte le funzioni registrate. Le informazioni sull'utilizzo associate alle funzioni vengono ripristinate quando i profili utente e le autorizzazione vengono ripristinate.

Applicazioni che utilizzano la registrazione dei certificati:

È possibile ripristinare le applicazioni che utilizzano le informazioni sulla registrazione dei certificati mediante il ripristino dell'oggetto QUSEXRGOBJ *EXITRG su QUSRSYS. Questa operazione

ripristina tutte le applicazioni registrate. È possibile ripristinare l'associazione dell'applicazione alle relative informazioni sul certificato mediante il ripristino dell'oggetto QYCDCERTI *USRIDX su QUSRSYS.

Concetti correlati

"Ripristino dei programmi"
Il ripristino dei programmi sul sistema, programmi ottenuti da un'origine sconosciuta, potrebbe danneggiare la sicurezza. Questo argomento fornisce informazioni sui fattori che dovrebbero essere presi in considerazione durante il ripristino dei programmi.

"Ripristino degli elenchi autorizzazioni" a pagina 272
Non esiste alcun metodo per ripristinare un singolo elenco di autorizzazioni. Quando si ripristina un elenco di autorizzazioni, l'autorizzazione e il proprietario vengono stabiliti come per qualsiasi altro oggetto ripristinato.

Ripristino dell'autorizzazione

Quando le informazioni sulla sicurezza vengono ripristinate, è necessario creare nuovamente le autorizzazioni private. Quando si ripristina un profilo utente che dispone di una tabella di autorizzazioni, tale tabella viene ripristinata.

Il comando RSTAUT (Ripristino autorizzazione) crea nuovamente l'autorizzazione privata nel profilo utente utilizzando le informazioni riportate sulla tabella autorizzazioni. L'operazione di concessione autorizzazione viene eseguita per ogni autorizzazione privata nella tabella autorizzazioni. Se l'autorizzazione è stata ripristinata per molti profili e sono presenti molte autorizzazioni private nella tabella autorizzazioni, questo processo potrebbe richiedere molto tempo.

È possibile eseguire i comandi RSTUSRPRF e RSTAUT per un singolo profilo, per un elenco di profili, per un nome profilo generico o per tutti i profili. Il sistema ricerca il supporto magnetico di salvataggio o il file di salvataggio creati dal comando SAVSECDTA, dal comando SAVSYS o dall'API QSRSAVO per rilevare i profili che si desidera ripristinare.

| Se le autorizzazioni private vengono salvate con oggetti, è possibile facoltativamente ripristinarle con gli
| oggetti. Questa procedura è consigliata se si sta salvando e ripristinando un numero relativamente
| limitato di oggetti, invece dell'intero sistema.

Ripristino dell'autorizzazione campo:

È necessario seguire queste fasi per ripristinare le autorizzazioni campo private per i file di database non ancora presenti sul sistema:

- Ripristino o creazione dei profili utente necessari.
- Ripristino dei file.
- Esecuzione del comando RSTAUT (Ripristino autorizzazione).

Le autorizzazioni campo private non vengono ripristinate completamente finché non vengono stabilite nuovamente le autorizzazioni oggetto private da esse limitate.

Ripristino dei programmi

Il ripristino dei programmi sul sistema, programmi ottenuti da un'origine sconosciuta, potrebbe danneggiare la sicurezza. Questo argomento fornisce informazioni sui fattori che dovrebbero essere presi in considerazione durante il ripristino dei programmi.

È possibile che questi programmi eseguano operazioni che potrebbero non rispettare i requisiti sulla sicurezza. In particolare, è necessario prestare attenzione ai programmi che contengono istruzioni limitate, programmi che adottano la propria autorizzazione proprietario e ai programmi manomessi. Ciò include i

tipi di oggetto *PGM, *SRVPGM, *MODULE e *CRQD. È possibile utilizzare i valori di sistema QVFYOBJRST, QFRCCVNRST e QALWOBJRST per impedire che questi tipi di oggetto vengano ripristinati sul sistema.

Il sistema utilizza un valore di convalida come supporto per la protezione dei programmi. Questa valore viene memorizzato con un programma e calcolato nuovamente quando il programma viene ripristinato. Le azioni del sistema vengono determinate dal parametro ALWOBJDIF sul comando di ripristino e sul valore di sistema Forzatura conversione al ripristino (QFRCCVNRST).

Nota: i programmi contengono informazioni che consentono la nuova creazione del programma al momento del ripristino se necessario. Le informazioni necessarie per creare nuovamente il programma, rimangono con il programma anche se, a livello visivo, il programma viene rimosso. Se si verifica un errore di convalida programma al momento del ripristino dello stesso, il programma viene creato nuovamente per correggere l'errore di convalida del programma.

Ripristino di programmi che adottano l'autorizzazione del proprietario:

Quando viene ripristinato un programma che adotta l'autorizzazione del proprietario, è possibile che la proprietà e l'autorizzazione del programma vengano modificate. È necessario considerare quanto segue:

- Il profilo utente che effettua l'operazione di ripristino deve essere il proprietario del programma o deve disporre delle autorizzazioni speciali *ALLOBJ e *SECADM.
- Il profilo utente che effettua l'operazione di ripristino può ricevere l'autorizzazione per ripristinare il programma
  - essendo il proprietario del programma
  - essendo membro del profilo di gruppo a cui appartiene il programma (a meno che non si disponga dell'autorizzazione privata per il programma)
  - disponendo dell'autorizzazione speciale *ALLOBJ e *SECADM
  - essendo membro di un profilo di gruppo che dispone dell'autorizzazione speciale *ALLOBJ e *SECADM
  - eseguendo sotto l'autorizzazione adottata che corrisponde a una delle verifiche appena elencate.
- Se il profilo di ripristino non dispone di un'autorizzazione adeguata, tutte le autorizzazioni pubbliche e private per il programma vengono revocate e l'autorizzazione pubblica viene modificata in *EXCLUDE.
- Se il proprietario del programma non è presente sul sistema, la proprietà viene concessa al profilo utente QDFTOWN. L'autorizzazione pubblica viene modificata in *EXCLUDE e l'elenco di autorizzazioni viene rimosso.

Concetti correlati

"Ripristino degli oggetti" a pagina 267
Quando si ripristina un oggetto su un sistema, il sistema utilizza le informazioni sull'autorizzazione memorizzate sull'oggetto. Questo argomento descrive le regole applicabili alle informazioni sulle autorizzazioni durante il ripristino degli oggetti.

Riferimenti correlati

"Valori di sistema di ripristino relativi alla sicurezza" a pagina 44
Questo argomento descrive i valori di sistema di ripristino relativi alla sicurezza sul sistema operativo i5/OS.

Ripristino dei programmi su licenza

Questo argomento introduce le istruzioni sul ripristino dei programmi su licenza sul sistema.

Il comando RSTLICPGM (Ripristino programma su licenza) viene utilizzato per installare i programmi forniti da IBM sul sistema. Inoltre, può essere utilizzato per installare programmi non IBM creati utilizzando il programma su licenza IBM System Manager per i5/OS.

Quando il sistema viene inviato, solo gli utenti con l'autorizzazione speciale *ALLOBJ possono utilizzare il comando RSTLICPGM. La procedura RSTLICPGM richiama un programma di uscita per installare i programmi non forniti dall'IBM.

Per proteggere la sicurezza sul sistema, il programma di uscita non deve essere eseguito utilizzando un profilo che disponga dell'autorizzazione speciale *ALLOBJ. Invece di lasciare che un utente con autorizzazione *ALLOBJ esegua il comando direttamente, utilizzare un programma che adotti l'autorizzazione speciale *ALLOBJ per eseguire il comando RSTLICPGM.

Segue un esempio di questa tecnica. Il programma che deve essere installato mediante l'utilizzo del comando RSTLICPGM è denominato CPAPP (Contratti e Tariffe).

1. Creare un profilo utente con sufficiente autorizzazione per installare senza problemi l'applicazione. Non fornire a questo profilo l'autorizzazione speciale *ALLOBJ. In questo esempio, il profilo utente è denominato OWNCP.
2. Scrivere un programma per installare l'applicazione. Il questo esempio, il programma è denominato CPINST:

   Nota: utilizzando i codici di esempio, si accettano i termini presenti nel Capitolo 10, "Informazioni sull'esonero di responsabilità e licenza codice", a pagina 329.

   ```
   PGM
   RSTLICPGM CPAPP
   ENDPGM
   ```
3. Creare il programma CPINST che adotti l'autorizzazione di un utente con l'autorizzazione speciale *ALLOBJ, quale QSECOFR e autorizzare OWNCP per il programma:
   ```
   CRTCLPGM QGPL/CPINST USRPRF(*OWNER) +
            AUT(*EXCLUDE)
   GRTOBJAUT OBJ(CPINST) OBJTYP(*PGM) +
             USER(OWNCP)  AUT(*USE)
   ```
4. Collegarsi come OWNCP e richiamare il programma CPINST. Quando il programma CPINST esegue il comando RSTLICPGM, si è in esecuzione con l'autorizzazione QSECOFR. Quando il programma di uscita viene eseguito per installare i programmi CPAPP, quest'ultimo rilascia l'autorizzazione adottata. I programmi richiamati dal programma di uscita vengono eseguiti sotto l'autorizzazione di OWNCP.

Ripristino degli elenchi autorizzazioni

Non esiste alcun metodo per ripristinare un singolo elenco di autorizzazioni. Quando si ripristina un elenco di autorizzazioni, l'autorizzazione e il proprietario vengono stabiliti come per qualsiasi altro oggetto ripristinato.

Il collegamento tra gli elenchi di autorizzazioni e gli oggetti viene stabilito se gli oggetti vengono ripristinati dopo l'elenco di autorizzazioni. Le autorizzazioni private dell'utente per l'elenco vengono ripristinate utilizzando il comando RSTAUT.

Gli elenchi autorizzazioni vengono salvati sia dal comando SAVSECDTA che dal comando SAVSYS. Gli elenchi di autorizzazioni vengono ripristinati mediante il comando:

```
RSTUSRPRF USRPRF(*ALL)
```

Ripristino da un elenco di autorizzazioni danneggiato

Quando un elenco di autorizzazioni che protegge un oggetto viene danneggiato, l'accesso all'oggetto viene limitato per gli utenti che dispongono di tutte le autorizzazioni speciali all'oggetto (*ALLOBJ).

Per recuperare un elenco di autorizzazioni danneggiato, è necessario:

1. ripristinare gli utenti e le relative autorizzazioni sull'elenco di autorizzazioni;
2. ripristinare l'associazione dell'elenco di autorizzazioni agli oggetti.

Queste due fasi devono essere eseguite da un utente con autorizzazione speciale *ALLOBJ.

Concetti correlati

"Ripristino degli oggetti" a pagina 267
Quando si ripristina un oggetto su un sistema, il sistema utilizza le informazioni sull'autorizzazione memorizzate sull'oggetto. Questo argomento descrive le regole applicabili alle informazioni sulle autorizzazioni durante il ripristino degli oggetti.

Ripristino dell'elenco di autorizzazioni

Utilizzare le istruzioni presenti in questo argomento per ripristinare l'elenco di autorizzazioni.

Se le autorizzazioni degli utenti all'elenco di autorizzazioni sono note, è possibile ripristinare l'elenco di autorizzazioni attenendosi alla procedura riportata di seguito.

1. Cancellare l'elenco di autorizzazioni.
2. Creare nuovamente l'elenco di autorizzazioni.
3. Aggiungere ad esso tutti gli utenti noti.

Se non si conoscono tutte le autorizzazioni utente, è possibile ripristinare l'elenco utilizzando gli ultimi nastri SAVSYS o SAVECDTA. Per ripristinare l'elenco di autorizzazioni, effettuare quanto segue:

1. Cancellare l'elenco di autorizzazioni danneggiato utilizzando il comando DLTAUTL (Cancellazione elenco di autorizzazioni).
2. Ripristinare l'elenco di autorizzazioni ripristinando i profili utente:
   ```
   RSTUSRPRF USRPRF(*ALL)
   ```
3. Ripristinare le autorizzazioni private degli utenti sull'elenco utilizzando il comando RSTAUT.

Questa procedura ripristina i valori del profilo utente dal supporto magnetico di salvataggio. Fare riferimento a "Ripristino profili utente" a pagina 266 per ulteriori informazioni sul ripristino dei valori dei profili utenti dal supporto magnetico di salvataggio.

Ripristino dell'associazione di oggetti sull'elenco di autorizzazioni

Attenersi alla procedura contenuta in questo argomento per ripristinare l'associazione di oggetti all'elenco di autorizzazioni.

Quando l'elenco di autorizzazioni danneggiato viene cancellato, è necessario aggiungere gli oggetti protetti dall'elenco di autorizzazioni al nuovo elenco di autorizzazioni. Effettuare quanto segue:

1. Rilevare gli oggetti associati all'elenco di autorizzazioni danneggiato utilizzando il comando RCLSTG (Riacquisizione memoria). Questo comando assegna gli oggetti associati all'elenco di autorizzazioni all'elenco di autorizzazioni QRCLAUTL.
2. Utilizzare il comando DSPAUTLOBJ (Visualizzazione oggetti elenco autorizzazioni) per elencare gli oggetti associati all'elenco di autorizzazioni QRCLAUTL.
3. Utilizzare il comando GRTOBJAUT (Concessione autorizzazione oggetto) per proteggere ogni oggetto con l'elenco di autorizzazioni corretto:
   ```
   GRTOBJAUT OBJ(library-name/object-name) +
             OBJTYPE(object-type) +
             AUTL(authorization-list-name)
   ```

Se un numero elevato di oggetti viene associato all'elenco di autorizzazioni QRCLAUTL, creare un file di database specificando OUTPUT(*OUTFILE) sul comando DSPAUTLOBJ. È possibile scrivere un programma CL per eseguire il comando GRTOBJAUT per ogni oggetto nel file.

Ripristino del sistema operativo

Quando si esegue un IPL manuale sul sistema, il menu IPL o Installazione sistema fornisce un'opzione per installare il sistema operativo. La funzione DST consente di richiedere agli utenti che utilizzano

questa opzione di menu di immettere la parola d'ordine di sicurezza DST. È possibile utilizzare ciò per impedire agli utenti di ripristinare una copia non autorizzata del sistema operativo.

Per proteggere l'installazione del sistema operativo, effettuare quanto segue:

1. Eseguire un IPL manuale.
2. Dal menu IPL o Installazione sistema, selezionare DST.
3. Dal menu Utilizzo DST, selezionare l'opzione per gestire l'ambiente DST.
4. Selezionare l'opzione per modificare le parole d'ordine DST.
5. Selezionare l'opzione per modificare la sicurezza relativa all'installazione del sistema operativo.
6. Specificare 1 (Protezione).
7. Premere F3 (Fine) fino a quando non si ritorna al menu IPL o Installazione sistema.
8. Completare l'IPL manuale e riportare la chiave di blocco nella posizione originale.

Note:

1. Se non si desidera più proteggere l'installazione del sistema operativo, seguire le stesse procedure e specificare 2 (nessuna protezione).
2. È inoltre possibile impedire l'installazione del sistema operativo posizionando lo switch della chiave di blocco nella posizione normale e rimuovendo la chiave.

Autorizzazione speciale *SAVSYS

Per salvare o ripristinare un oggetto, è necessario disporre dell'autorizzazione *OBJEXIST per l'oggetto o dell'autorizzazione speciale *SAVSYS. Un utente che dispone dell'autorizzazione speciale *SAVSYS non necessita di ulteriore autorizzazione per un oggetto per salvarlo o ripristinarlo.

L'autorizzazione speciale *SAVSYS consente a un utente di salvare un oggetto e spostarlo su un sistema differente per il ripristino o di visualizzare (dump) il supporto magnetico per visualizzare i dati. Inoltre, consente a un utente di salvare un oggetto e di liberare memoria, mediante la cancellazione dei dati nell'oggetto. Quando si salvano i documenti, un utente con l'autorizzazione speciale *SAVSYS può scegliere se cancellare tali documenti. È necessario concedere con attenzione l'autorizzazione speciale *SAVSYS.

Controllo delle operazioni di salvataggio e di ripristino

Viene scritto un record di controllo sicurezza per ogni operazione di ripristino se il valore di controllo azione (valore di sistema QAUDLVL o AUDLVL nel profilo utente) include *SAVRST. Quando si utilizza un comando che ripristina un elevato numero di oggetti, quale RSTLIB, viene scritto un record di controllo per ogni oggetto ripristinato. Questa operazione potrebbe causare dei problemi con la dimensione del ricevitore del giornale di controllo, specialmente se si sta ripristinando più di una libreria.

Il comando RSTCFG non crea un record di controllo per ogni oggetto ripristinato. Se si desidera avere un record di controllo di questo comando, impostare il controllo oggetto per lo stesso comando. Verrà scritto un record di controllo ogni volta che viene eseguito il comando.

I comandi che salvano un elevato numero di oggetti, quali SAVSYS, SAVSECDTA e SAVCFG, non creano singoli record di controllo per gli oggetti salvati, anche se la funzione di controllo oggetto di tali oggetti è attivata. Per monitorare questi comandi, impostare il controllo oggetto per i comandi stessi.

Capitolo 9. Controllo della sicurezza su System i

Questa sezione descrive le tecniche per il controllo dell'efficacia della sicurezza sul proprio sistema.

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 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 in questa sezione 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 questa sezione è quello di illustrare quali informazioni sono disponibili, come ottenerle e perché sono necessarie, piuttosto che fornire direttive per la frequenza dei controlli.

Questa sezione si compone di 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 sulla sicurezza relative al sistema.

Il controllo della sicurezza implica l'utilizzo di comandi nell'ambiente System i e l'accesso a informazioni della registrazione e del giornale sul sistema. È possibile che si desideri 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 questa sezione richiedono un profilo utente con 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.

Concetti correlati

"Giornale di controllo sicurezza" a pagina 6
È possibile utilizzare i giornali di controllo sicurezza per controllare l'efficacia della sicurezza sul sistema.

Elenco di controllo per i responsabili della riservatezza e per i revisori

È possibile utilizzare l'elenco di controllo per pianificare e controllare la sicurezza del sistema.

Quando si pianifica la sicurezza, scegliere da questa raccolta gli argomenti che meglio soddisfano i requisiti per la sicurezza. Quando si controlla la sicurezza del sistema, utilizzare l'elenco per valutare i controlli in posizione e per determinare se ne sono necessari degli altri.

Ciascun elenco è utile per riesaminare le informazioni contenute in questa raccolta di argomenti. Gli elenchi contengono brevi descrizioni sulle voci, su come verificare il lavoro svolto e una descrizione delle voci da ricercare nel giornale QAUDJRN. Dettagli sulle voci sono disponibili in tutta la raccolta di argomenti.

Sicurezza fisica

È possibile utilizzare l'elenco di controllo della sicurezza fisica per pianificare o controllare la sicurezza fisica del sistema.

Nota: Consultare Planning and setting up system security per informazioni complete sul prodotto System i.

Qui viene riportato un elenco di controllo per la pianificazione della sicurezza fisica del sistema:

__ • L'unità di sistema e la console si trovano in un'ubicazione sicura.

__ • Il supporto magnetico copia di riserva è protetto da danni e da furti.

__ • L'impostazione dell'interruttore di blocco sull'unità del processore è nella posizione Protetto o Auto. Le chiavi vengono rimosse e conservate separatamente in base a rigide misure di sicurezza fisica. Consultare Planning physical security for the system unit per ulteriori informazioni sull'interruttore di blocco.

__ • L'accesso alle stazioni di lavoro ubicate in un posto pubblico è limitato. Utilizzare il comando DSPOBJAUT per visualizzare chi dispone dell'autorizzazione *CHANGE alle stazioni di lavoro. Ricercare le voci AF nel giornale di controllo con *DEVD impostato sul campo del tipo di oggetto per visualizzare i tentativi di accesso alle stazioni di lavoro limitate.

__ • L'accesso da parte di utenti con autorizzazione speciale *ALLOBJ o *SERVICE è limitato a poche stazioni di lavoro. Verificare se il valore di sistema QLMTSECOFR è 1. Utilizzare il comando DSPOBJAUT per le unità per verificare se il profilo QSECOFR dispone di autorizzazione *CHANGE.

Valori di sistema

L'impostazione della funzione di controllo per i valori di sistema consente di tenere traccia dei valori modificati sul sistema.

- I valori di sistema della sicurezza seguono delle istruzioni consigliate. Per stampare i valori di sistema della sicurezza, immettere: `WRKSYSVAL *SEC OUTPUT(*PRINT)`. Due valori di sistema importanti da controllare sono:
  - QSECURITY, il quale deve essere impostato su 40 o su un valore superiore.
  - QMAXSIGN, il quale non deve essere maggiore di 5.

  Nota: se la funzione di controllo è attiva, viene scritta una voce SV sul giornale QAUDJRN ogniqualvolta viene modificato il valore di sistema.
- Utilizzare il comando DSPSECA (Visualizzazione attributi sicurezza) per verificare i valori correnti e in sospeso di QSECURITY (livello di sicurezza) e QPWDLVL (livello parola d'ordine) e l'impostazione corrente del sistema correlato alla sicurezza (se è possibile modificare i valori).
- Riesaminare periodicamente le decisioni relative ai valori di sistema. Ciò è particolarmente importante quando viene modificato l'ambiente di sistema, ad esempio quando si effettua l'installazione di nuove applicazioni o di una rete di comunicazione.

Profili utente forniti da IBM

È possibile eseguire attività di controllo sui profili utente forniti da IBM tramite la verifica delle relative parole d'ordine.

- La parola d'ordine è stata modificata per il profilo utente QSECOFR.

  Questo profilo viene fornito con la parola d'ordine impostata su QSECOFR, in modo tale da potersi collegare per installare il sistema. La parola d'ordine deve essere modificata la prima volta che si accede al sistema e deve essere modificata periodicamente dopo l'installazione.

  Per verificare se è stata modificata, controllare l'elenco DSPAUTUSR nella data in cui la parola d'ordine QSECOFR è stata modificata e tentare di collegarsi con la parola d'ordine predefinita.
- Le parole d'ordine IBM per i DST sono state modificate.

  Gli ID utente per i programmi di manutenzione non vengono visualizzati sull'elenco DSPAUTUSR. Per verificare che gli ID utente e le parole d'ordine siano stati modificati, avviare il DST e tentare di utilizzare i valori predefiniti.
- Ad eccezione di QSECOFR, non collegarsi con profili utente forniti da IBM.

  Questi profili utente forniti da IBM sono stati progettati per contenere oggetti o per eseguire funzioni di sistema. Utilizzare un elenco DSPAUTUSR per verificare che i profili utente forniti da IBM elencati in Appendice B, "Profili utente forniti da IBM", a pagina 341, ad eccezione di QSECOFR, dispongano di una parola d'ordine corrispondente a *NONE.

Concetti correlati

"profili utente forniti da IBM" a pagina 137
Un numero di profili utente viene fornito con il software di sistema. Questi profili utente forniti da IBM vengono utilizzati come proprietari dell'oggetto per diverse funzioni di sistema. Alcune funzioni di sistema vengono anche eseguite tramite specifici profili utente forniti da IBM.

"Gestione ID utente programmi di manutenzione" a pagina 138
Sono disponibili diversi miglioramenti e aggiunte ai programmi di manutenzione di manutenzione che ne facilitano l'utilizzo e la comprensione.

Riferimenti correlati

Appendice B, "Profili utente forniti da IBM", a pagina 341
Questa sezione contiene informazioni sui profili utente forniti con il sistema. Questi profili sono utilizzati come proprietari di oggetto per varie funzioni di sistema. Alcune funzioni di sistema vengono anche eseguite tramite specifici profili utente forniti da IBM.

Controllo parola d'ordine

È possibile utilizzare i meccanismi di controllo della parola d'ordine per controllare la sicurezza del sistema.

- Gli utenti possono modificare le proprie parole d'ordine.

  Consentendo agli utenti di definire le proprie parole d'ordine, non sarà necessario che essi scrivano le relative parole d'ordine. Gli utenti dovrebbero disporre dell'accesso al comando CHGPWD o alla funzione Modifica parola d'ordine dal menu Sicurezza (GO SECURITY).
- Una modifica della parola d'ordine viene richiesta in base alle direttive per la sicurezza dell'organizzazione, ad esempio ogni 30 o 90 giorni.

  Il valore di sistema QPWDEXPITV viene impostato in modo che rispetti le predisposizioni della sicurezza.
- Se un profilo utente dispone di una parola d'ordine con un intervallo di scadenza differente dal valore di sistema, esso rispetta le predisposizioni della sicurezza.

  Riesaminare i profili utente per il valore PWDEXPITV che non sia *SYSVAL.
- È possibile impedire l'accettazione delle parole d'ordine utilizzando i valori di sistema per impostare le regole delle parole d'ordine e utilizzando il programma di approvazione della parola d'ordine.

Utilizzare il comando WRKSYSVAL *SEC e controllare le impostazioni per i valori che iniziano per QPWD.

- I profili di gruppo dispongono della parola d'ordine *NONE.

  Utilizzare il comando DSPAUTUSR per verificare i profili di gruppo che dispongono di parole d'ordine.

Quando il sistema non funziona al livello parola d'ordine 3 e gli utenti modificano le parole d'ordine, il sistema tenta di creare una parola d'ordine equivalente utilizzabile con altri livelli di parola d'ordine. È possibile utilizzare il comando PRTUSRPRF TYPE(*PWDLVL) per verificare quali profili utente dispongano di parole d'ordine che è possibile utilizzare con vari livelli di parola d'ordine.

Nota: la parola d'ordine equivalente è un ottimo metodo per creare una parola d'ordine utilizzabile con altri livelli di parola d'ordine ma è possibile che non abbia passato tutte le regole della parola d'ordine se un altro livello di parola d'ordine era in uso. Ad esempio, se viene specificata la parola d'ordine BbAaA3x al livello di parola d'ordine 2, il sistema creerà una parola d'ordine equivalente corrispondente a BBAAA3X utilizzabile a livello 0 e 1. Questa può essere valida anche se il valore di sistema QPWDLMTCHR include una 'A' come uno dei caratteri limitati (QPWDLMTCHR non viene applicato al livello di parola d'ordine 2) o il se è stato specificato per il valore di sistema QPWDLMTREP che i caratteri consecutivi non possono essere gli stessi (poiché il controllo è sensibile ai caratteri minuscoli e maiuscoli al livello parola d'ordine 2 ma non è sensibile ai caratteri minuscoli e maiuscoli a livello di parola d'ordine 0 e 1).

Profili utente e di gruppo

È possibile convalidare i profili utente e di gruppo e le relative autorizzazioni per controllare l'efficacia della sicurezza sul sistema.

- A ciascun utente viene assegnato un profili utente univoco.

  Impostare il valore di sistema QLMTDEVSSN su 1. Sebbene la limitazione di ciascun utente a una sola sessione unità alla volta non impedisca la condivisione dei profili utente, questa situazione scoraggia l'utente.

- Gli utenti che dispongono dell'autorizzazione speciale *ALLOBJ sono limitati e non vengono utilizzati come profili di gruppo.

  Utilizzare il comando DSPUSRPRF per controllare le autorizzazioni speciali per i profili utente e per determinare quali profili sono profili di gruppo. L'argomento "Stampa profili utente selezionati" a pagina 325 mostra come utilizzare un file di emissione e una query per determinare ciò.

- Il campo *Possibilità limitate* è impostato su *YES nei profili degli utenti che dovrebbero essere limitati per una serie di menu.

  L'argomento "Stampa profili utente selezionati" a pagina 325 fornisce un esempio di come determinare ciò.

- I programmatori dispongono di limiti per le librerie di produzione.

  Utilizzare il comando DSPOBJAUT per determinare le autorizzazioni pubbliche e private per le librerie di produzione e per gli oggetti critici nelle librerie. "Pianificazione della sicurezza per i programmatori" a pagina 259 dispone di ulteriori informazioni sulla sicurezza e sull'ambiente di programmazione.

- L'appartenenza in un profilo di gruppo viene modificata quando si cambiano le responsabilità del lavoro.

  Per verificare l'appartenenza del gruppo, utilizzare uno dei seguenti comandi:

```
DSPAUTUSR SEQ(*GRPPRF)
DSPUSRPRF nome-profilo *GRPMBR
```

- È necessario utilizzare una convenzione di denominazione per i profili di gruppo.

  Quando vengono visualizzate le autorizzazioni, è possibile riconoscere facilmente il profilo di gruppo.
- La gestione dei profili utente è organizzata in maniera adeguata.

  Nessun profilo utente dispone di un numero elevato di autorizzazioni private. L'argomento "Esame dei profili utente di ampie dimensioni" a pagina 325 mostra come rilevare ed esaminare profili utente grandi sul sistema.
- Gli impiegati vengono rimossi immediatamente dal sistema quando vengono trasferiti o rilasciati.

  Rivedere regolarmente l'elenco DSPAUTUSR per assicurarsi che solo impiegati attivi dispongano di accesso al sistema. Per assicurarsi che i profili utente vengano cancellati immediatamente dopo l'uscita degli impiegati, rivedere le voci DO (Cancellazione oggetto) nel giornale di controllo.
- La gestione verifica regolarmente gli utenti autorizzati sul sistema.

  Utilizzare il comando DSPAUTUSR per visualizzare le informazioni sulle autorizzazioni degli utenti.
- La parola d'ordine per un impiegato non attivo è impostata su *NONE.

  Utilizzare il comando DSPAUTUSR per verificare che i profili utente non attivi non dispongano di parole d'ordine.
- La gestione verifica regolarmente gli utenti con autorizzazioni speciali, in particolare le autorizzazioni speciali *ALLOBJ *SAVSYS e *AUDIT.

  L'argomento "Stampa profili utente selezionati" a pagina 325 fornisce un esempio di come determinare ciò.

Controllo autorizzazione

Il controllo dell'autorizzazione consente all'utente di verificare la sicurezza delle informazioni memorizzate sul proprio sistema.

È possibile utilizzare il seguente elenco di controllo per assistere l'utente nella verifica della sicurezza del controllo dell'autorizzazione.

- I proprietari dei dati sono in grado di capire quali utenti autorizzare.
- I proprietari degli oggetti verificano regolarmente l'autorizzazione per utilizzare l'oggetto, inclusa l'autorizzazione pubblica.

  Il comando WRKOBJOWN fornisce un pannello per la gestione delle autorizzazioni per tutti gli oggetti di cui è proprietario un profilo utente.
- I dati sensibili non sono pubblici. Controllare l'autorizzazione per l'utente *PUBLIC per gli oggetti critici utilizzando il comando DSPOBJAUT.
- L'autorizzazione ai profili utente è controllata.

  L'autorizzazione pubblica per i profili utente dovrebbe essere *EXCLUDE. In questo modo gli utenti non possono inoltrare i lavori in esecuzione con un altro profilo utente.
- Le descrizioni lavoro sono controllate:
  - Le descrizioni lavoro con l'autorizzazione pubblica *USE o maggiore vengono specificati come USER(*RQD). Ciò significa che i lavori inoltrati utilizzando la descrizione lavoro devono essere eseguiti utilizzando il profilo dell'utente che li inoltra.

– Le descrizioni lavoro che specificano un utente dispongono dell'autorizzazione pubblica *EXCLUDE. L'autorizzazione per l'utilizzo di tali descrizioni lavoro è controllata. In questo modo gli utenti non autorizzati non potranno inoltrare i lavori in esecuzione con un'autorizzazione di un altro profilo.

Per capire quali descrizioni lavoro sono presenti sul sistema, immettere:

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

Per controllare il parametro *Utente* di una descrizione lavoro, utilizzare il comando DSPJOBD (Visualizzazione descrizione lavoro). Per controllare l'autorizzazione a una descrizione lavoro, utilizzare il comando DSPOBJAUT (Visualizzazione autorizzazione oggetto).

Nota: al livello di sicurezza 40 o 50, un utente che inoltra un lavoro utilizzando una descrizione lavoro che specifica un nome del profilo utente deve disporre dell'autorizzazione *USE per la descrizione lavoro e per il profilo utente. A tutti i livelli di sicurezza, un tentativo di inoltro o di pianificazione di un lavoro senza l'autorizzazione *USE per l'utente specificato nella descrizione lavoro, causa la visualizzazione di una voce AF con il tipo di violazione J nel giornale di controllo.

- Gli utenti non possono collegarsi premendo il tasto Invio sul pannello di collegamento.

  Assicurarsi che nessuna voce della stazione di lavoro nelle descrizioni del sottosistema specifichi una descrizione lavoro con un nome del profilo utente specificato per il parametro USER.

  Il collegamento predefinito non viene consentito al livello di sicurezza 40 o 50, anche se una descrizione del sottosistema lo consente. A tutti i livelli di sicurezza, viene scritta una voce AF con il tipo di violazione S sul giornale di controllo se viene riscontrato il tentativo di un collegamento predefinito e se una descrizione del sottosistema lo consente.
- L'elenco librerie nei programmi dell'applicazione viene controllato per fare in modo che una libreria che contiene un programma simile non venga aggiunta prima delle librerie di produzione.

  L'argomento "Elenchi librerie" a pagina 222 mostra i metodi per controllare l'elenco librerie.
- I programmi che adottano l'autorizzazione vengono utilizzati solo se necessario e vengono controllati attentamente.

  Consultare l'argomento "Analisi dei programmi che adottano l'autorizzazione" a pagina 326 per una spiegazione su come utilizzare la funzione per adottare un programma.
- Le API (Application program interface) sono protette.
- Vengono utilizzate ottime tecniche per la sicurezza dell'oggetto per evitare problemi alle prestazioni.

Accesso non autorizzato

Utilizzare questo elenco di controllo insieme al giornale di controllo per controllare i tentativi non autorizzati di accesso alle informazioni.

- Gli eventi relativi alla sicurezza vengono registrati sul giornale di controllo della sicurezza (QAUDJRN) quando la funzione di controllo è attiva.

  Per controllare gli errori relativi alle autorizzazioni, utilizzare i seguenti valori di sistema e impostazioni:

  – QAUDCTL deve essere impostato su *AUDLVL
  – QAUDLVL deve includere i valori di *PGMFAIL e *AUTFAIL.

  Il metodo migliore per rilevare tentativi di accesso non autorizzati alle informazioni è quello di controllare regolarmente le voci presenti sul giornale di controllo.
- Il valore di sistema QMAXSIGN limita il numero di tentativi di accesso consecutivi non corretti a cinque o a un numero inferiore. Il valore di sistema QMAXSGNACN è impostato su 2 o 3.
- Viene creata e monitorata la coda messaggi QSYSMSG.

- Il giornale di controllo viene controllato per i ripetuti tentativi effettuati dall'utente. (Gli errori di autorizzazione causano la scrittura delle voci di tipo AF sul giornale di controllo).
- I programmi non riescono al accedere agli oggetti utilizzando interfacce non supportate. (Il valore di sistema QSECURITY è impostato su 40 o 50).
- È necessario l'ID utente e la parola d'ordine per collegarsi.

  I livelli di sicurezza 40 e 50 lo richiedono. A livello 20 o 30, è necessario assicurarsi che nessuna descrizione del sottosistema disponga di una voce stazione di lavoro che utilizzi una descrizione lavoro con un nome profilo utente.

Programmi non autorizzati

Il comando CHKOBJITG (Controllo integrità oggetto) consente di controllare le modifiche non autorizzate apportate alle modifiche del programma sul sistema.

- Il valore di sistema QALWOBJRST è impostato su *NONE per impedire a qualsiasi utente di ripristinare i programmi sensibili alla sicurezza sul sistema.
- Il comando CHKOBJITG (Controllo integrità oggetto) viene eseguito periodicamente per rilevare modifiche non autorizzate apportate agli oggetti del programma.

  Questo comando è descritto in "Controllo degli oggetti che sono stati modificati" a pagina 327.

Comunicazioni

È possibile utilizzare questo elenco di controllo per pianificare e per controllare i controlli necessari su vari tipi di comunicazioni sul sistema.

- Utilizzare le procedure call-back per proteggere le comunicazioni telefoniche.
- Utilizzare la codifica per i dati sensibili.
- Controllare l'accesso remoto. Il valore di sistema QRMTSIGN è impostato su *FRCSIGNON o viene utilizzato un programma di convalida pass-through.
- Utilizzare gli attributi di rete JOBACN, PCSACC e DDMACC per controllare l'accesso ai dati da altri sistemi, compresi i personal computer. L'attributo di rete JOBACN dovrebbe essere *FILE.

Utilizzo del giornale di controllo sicurezza

Il giornale di controllo sicurezza è la fonte principale di informazioni sul controllo relative al sistema. Questa sezione descrive come pianificare, impostare e gestire il controllo della sicurezza, quali informazioni sono state registrate e come visualizzare tali informazioni.

Un revisore della sicurezza interno o esterno all'organizzazione può utilizzare la funzione di controllo fornita dal sistema per raccogliere informazioni sugli eventi relativi alla sicurezza che si verificano sul sistema.

È possibile definire il controllo sul sistema in tre livelli differenti:

- Il controllo che viene effettuato sull'intero sistema per tutti gli utenti.
- Il controllo che viene effettuato per oggetti specifici.
- il controllo che viene effettuato per utenti specifici.

È possibile utilizzare i valori di sistema, i parametri del profilo utente e i parametri oggetto per definire il controllo. "Pianificazione del controllo sicurezza" a pagina 282 descrive come effettuare ciò.

Quando si verifica un evento relativo alla sicurezza che potrebbe essere controllato, il sistema verifica se l'utente ha selezionato tale evento per il controllo. Se così fosse, il sistema scrive una voce di giornale sul ricevitore corrente per il giornale di controllo sicurezza (QAUDJRN nella libreria QSYS).

Quando si desidera analizzare le informazioni di controllo raccolte nel giornale QAUDJRN, è possibile utilizzare il comando DSPJRN (Visualizzazione giornale). Tramite questo comando, è possibile scrivere le informazioni dal giornale QAUDJRN al file di database. È possibile utilizzare un programma dell'applicazione o uno strumento query per analizzare i dati.

Riferimenti correlati

Appendice F, "Layout di voci di giornale di controllo", a pagina 595
Questa sezione contiene informazioni sul layout per tutti i tipi di voce con codice giornale T nel giornale di controllo (QAUDJRN). Queste voci sono controllate tramite il controllo operazione e oggetto definito dall'utente.

Appendice E, "Controllo e operazioni oggetto", a pagina 529
Questa raccolta di argomenti elenca le operazioni che possono essere effettuate rispetto ad oggetti sul sistema e se tali operazioni sono sottoposte a controllo.

Pianificazione del controllo sicurezza

La funzione di controllo sicurezza è facoltativa. È necessario eseguire passi specifici per impostare il controllo della sicurezza.

Per pianificare l'utilizzo del controllo sicurezza sul sistema, attenersi a questa procedura:

- Determinare quali eventi rilevanti per la sicurezza si desidera registrare per tutti gli utenti del sistema. Il controllo degli eventi rilevanti per la sicurezza viene denominato *controllo azione*.
- Verificare se è necessario un ulteriore controllo per utenti specifici.
- Stabilire se si desidera controllare l'utilizzo di oggetti specifici sul sistema.
- Stabilire se è necessario utilizzare il controllo oggetto per tutti gli utenti o per utenti specifici.

Pianificazione del controllo delle azioni

I valori di sistema QAUDCTL (controllo), QAUDLVL (livello di controllo), QAUDLVL2 (estensione livello di controllo) e il parametro AUDLVL (controllo azione) nei profili utente collaborano per controllare il controllo azione.

Le funzioni di ogni valore di sistema sono le seguenti:

- Il valore di sistema QAUDLVL indica quali azioni vengono controllate per tutti gli utenti sul sistema.
- Inoltre, il valore di sistema QAUDLVL2 indica quali azioni vengono controllate per tutti gli utenti del sistema e viene utilizzato quando sono necessari più 16 valori di controllo.
- Il parametro AUDLVL nel profilo utente stabilisce quali azioni vengono controllate per un utente specifico. Inoltre, i valori per il parametro AUDLVL *si applicano* ai valori per QAUDLVL e QAUDLVL2.
- Il valore di sistema QAUDCTL avvia e arresta il controllo dell'azione.

La scelta degli eventi da registrare dipende sia dagli obiettivi di sicurezza che dai rischi potenziali. "Controllo azione" a pagina 121 descrive i valori del livello di controllo possibili e come utilizzarli. Mostra se sono disponibili come valori di sistema, come parametro del profilo utente o come entrambi.

Riferimenti correlati

"Livello di controllo (QAUDLVL)" a pagina 73
Il valore di sistema livello di controllo (QAUDLVL) insieme al valore di sistema QAUDLVL2 stabilisce quali eventi relativi alla sicurezza registrare sul giornale di controllo della sicurezza (QAUDJRN) per tutti gli utenti del sistema.

"Estensione livello di controllo (QAUDLVL2)" a pagina 75
Il valore di sistema estensione livello di controllo (QAUDLVL2) è richiesto quando sono necessari più di sedici valori di controllo.

"Controllo azione" a pagina 121
Per un singolo utente, è possibile specificare le azioni relative alla sicurezza da registrare nel giornale di controllo. Le azioni specificate per un singolo utente si applicano in aggiunta alle azioni specificate per tutti gli utenti dai valori di sistema QAUDLVL e QAUDLVL2.

Valori di controllo azione:

Questa tabella elenca i possibili valori disponibili sul sistema di valori QAUDLVL e QAUDLVL2 e il comando CHGUSRAUD durante le azioni di controllo del sistema.

Tabella 131. Valori di controllo azione

Valore possibile	Disponibile sui valori di sistema QAUDLVL e QAUDLVL2	Disponibile sul comando CHGUSRAUD	Descrizione
*NONE	Sì	Sì	Se il valore di sistema QAUDLVL è impostato su *NONE, nessuna azione viene registrata sulle basi dell'intero sistema. Le azioni vengono registrate per singoli utenti in base al valore AUDLVL presente nei relativi profili utente. Se il valore AUDLVL in un profilo utente è impostato su *NONE, non viene effettuato nessun ulteriore controllo dell'azione per questo utente. Tutte le azioni specificate per il valore di sistema QAUDLVL vengono registrate per questo utente.
*ATNEVT	Sì	No	**Eventi di attenzione**: il sistema scrive una voce giornale che richiede un'ulteriore analisi. Con tali informazioni, è possibile determinare il potenziale significato dell'evento di attenzione per il sistema.
*AUTFAIL	Sì	Sì	**Errori autorizzazione**: i tentativi di collegamento al sistema e agli oggetti non riusciti vengono registrati. È possibile utilizzare *AUTFAIL regolarmente per monitorare gli utenti che tentano di di effettuare funzioni non autorizzate sul sistema. È inoltre possibile utilizzare *AUTFAIL come supporto alla migrazione a un livello di sicurezza superiore e per verificare la sicurezza delle risorse per una nuova applicazione.
*CMD	No	Sì	**Comandi**: il sistema registra le stringhe di comando eseguite dall'utente. Se un comando viene eseguito da un programma CL creato con LOG(*NO) e ALWRTVSRC(*NO), solo il nome del comando e della libreria vengono registrati. È possibile utilizzare *CMD per registrare le azioni di un utente particolare, ad esempio il responsabile della riservatezza.
*CREATE	Sì	Sì	**Creazione oggetti**: il sistema scrive una voce giornale quando viene creato o sostituito un nuovo oggetto. È possibile utilizzare *CREATE per verificare quando vengono creati o compilati nuovamente i programmi.
*DELETE	Sì	Sì	**Cancellazione oggetti**: il sistema scrive una voce giornale quando un oggetto viene cancellato.
*JOBBAS	Sì	Sì	**Funzioni di base del lavoro**: vengono registrate azioni che influenzano un lavoro, quale l'avvio o l'arresto di un lavoro, la conservazione, il rilascio, l'annullamento o la modifica del lavoro.

Tabella 131. Valori di controllo azione (Continua)

Valore possibile	Disponibile sui valori di sistema QAUDLVL e QAUDLVL2	Disponibile sul comando CHGUSRAUD	Descrizione
*JOBCHGUSR	Sì	Sì	**Utente modifiche lavoro**: vengono registrate le modifiche al profilo utente attivo di un sottoprocesso o ai relativi profili del gruppo.
*JOBDTA	Sì	Sì	**Attività lavoro**: vengono registrate le azioni che influenzano un lavoro, quale l'avvio o l'arresto di un lavoro, la conservazione, il rilascio, l'annullamento, o la modifica del lavoro, modificando il profilo utente attivo del sottoprocesso o il profilo del gruppo. È possibile utilizzare *JOBDTA per monitorare gli utenti che stanno eseguendo i lavori batch. *JOBDTA è composto da due valori, *JOBBAS e *JOBCHGUSR, in modo da consentire all'utente di personalizzare al meglio il proprio controllo.
*NETBAS	Sì	Sì	**Funzioni di base della rete**: azioni regole IP, connessioni socket, filtro di ricerca indirizzario APPN, filtro endpoint APPN.
*NETCLU	Sì	Sì	**Cluster o operazioni di gruppo risorse cluster**: viene scritta una voce giornale di controllo quando si verifica uno dei seguenti eventi: • Viene aggiunto, creato o cancellato un nodo cluster o un gruppo di risorse cluster. • Viene avviato, arrestato, aggiornato o rimosso un nodo cluster o un gruppo di risorse cluster. • Esito negativo automatico di un sistema che commuta l'accesso a un altro sistema. • L'accesso viene commutato manualmente da un sistema a un altro in un cluster.
*NETCMN	Sì	Sì	**Controllo comunicazioni di rete**: le violazioni rilevate dal supporto filtro APPN vengono registrate sul giornale di controllo di sicurezza quando il filtro di ricerca indirizzario e il filtro endpoint vengono controllati. *NETCMN è composto da diversi valori in modo da consentire all'utente di personalizzare al meglio il proprio controllo. I valori seguenti compongono *NETCMN: *NETBAS *NETCLU *NETFAIL *NETSCK
*NETFAIL	Sì	Sì	**Errori di rete**: viene scritta una voce giornale di controllo quando si tenta di collegarsi a una porta TCP/IP che non esiste o si tenta di inviare informazioni a una porta TCP/IP non aperta o non disponibile.

Tabella 131. Valori di controllo azione (Continua)

Valore possibile	Disponibile sui valori di sistema QAUDLVL e QAUDLVL2	Disponibile sul comando CHGUSRAUD	Descrizione
*NETSCK	Sì	Sì	**Attività socket**: viene scritta una voce giornale di controllo quando si verifica uno dei seguenti eventi: • Viene accettata una connessione socket TCP/IP in entrata. • Viene stabilita una connessione socket TCP/IP in uscita. • Viene assegnato un indirizzo IP mediante il DHCP (Dynamic Host Configuration Protocol). • Un indirizzo IP non può essere assegnato mediante DHCP perché tutti gli indirizzi IP sono stati utilizzati. • La posta viene filtrata o rifiutata.
*OBJMGT	Sì	Sì	**Attività di gestione oggetto**: l'operazione di ridenominazione o di spostamento di un oggetto in una libreria differente viene registrata. È possibile utilizzare *OBJMGT per rilevare la copia di informazioni riservate spostando l'oggetto in una libreria differente.
*OPTICAL	Sì	Sì	**Funzioni dell'unità ottica**: tutte le opzioni dell'unità ottica vengono controllate, incluse le funzioni relative ai file dell'unità ottica, agli indirizzari dell'unità ottica, ai volumi dell'unità ottica e alle cartucce dell'unità ottica. È possibile utilizzare *OPTICAL per rilevare i tentativi effettuati dall'utente di creare o cancellare un indirizzario dell'unità ottica.
*PGMADP	Sì	Sì	**Acquisizione autorizzazione**: il sistema scrive una voce giornale quando l'autorizzazione adottata viene utilizzata per ottenere accesso a un oggetto. È possibile utilizzare *PGMADP per verificare e capire in che modo una nuova applicazione utilizza un'autorizzazione adottata.
*PGMFAIL	Sì	Sì	**Errori programma**: il sistema scrive una voce giornale quando un programma causa un errore di integrità. È possibile utilizzare *PGMFAIL come supporto alla migrazione a un livello di sicurezza superiore o per verificare una nuova applicazione.
*PRTDTA	Sì	Sì	**Funzioni di stampa**: viene registrata la stampa di un file di spool, la stampa direttamente da un programma o l'invio di un file di spool a una stampante remota. È possibile utilizzare *PRTDTA per rilevare informazioni riservate sulla stampa.
*SAVRST	Sì	Sì	**Operazioni di ripristino**: è possibile utilizzare *SAVRST per rilevare i tentativi effettuati dall'utente di ripristinare oggetti non autorizzati.

Tabella 131. Valori di controllo azione (Continua)

Valore possibile	Disponibile sui valori di sistema QAUDLVL e QAUDLVL2	Disponibile sul comando CHGUSRAUD	Descrizione
*SECCFG	Sì	Sì	**Configurazione sicurezza**: viene scritta una voce giornale di controllo quando si verifica uno dei seguenti eventi: • Vengono creati, modificati, cancellati o ripristinati i profili utente. • Vengono apportate delle modifiche ai programmi, ai valori di sistema, all'instradamento del sottosistema o agli attributi di controllo di un oggetto. • La parola d'ordine QSECOFR viene ripristinata al valore originale. • La parola d'ordine del responsabile della riservatezza dei programmi di manutenzione viene impostata su un valore predefinito.
*SECDIRSRV	Sì	Sì	**Funzioni servizio indirizzario**: viene scritta una voce giornale di controllo quando si verifica uno dei seguenti eventi: • Vengono apportate delle modifiche o vengono effettuati degli aggiornamenti per il controllo, l'autorizzazione, le parole d'ordine e la proprietà. • Collegamenti e scollegamenti riusciti. • Le modifiche vengono effettuate alle normative di sicurezza dell'indirizzario (ad esempio, normativa della parola d'ordine)
*SECIPC	Sì	Sì	**IP (Interprocess communications/comunicazioni tra processi)**: viene scritta una voce giornale di controllo quando si verifica uno dei seguenti eventi: • Vengono apportate delle modifiche al proprietario o all'autorizzazione di un oggetto IPC. • Viene creato, cancellato o richiamato un oggetto IPC. • Collegamento memoria condivisa.

Tabella 131. Valori di controllo azione (Continua)

Valore possibile	Disponibile sui valori di sistema QAUDLVL e QAUDLVL2	Disponibile sul comando CHGUSRAUD	Descrizione
*SECNAS	Sì	Sì	**azioni servizio autenticazione di rete**: viene scritta una voce giornale di controllo quando si verifica uno dei seguenti eventi: • Certificato di servizio non valido. • Principal del servizio non corrispondenti. • Principal del client non corrispondenti. • Mancata corrispondenza indirizzo IP certificato. • Decodifica del certificato non riuscita. • Decodifica dell'autenticazione non riuscita. • Il dominio non è contenuto nei domini locali e del client. • Il certificato è un tentativo di ripetizione. • Certificato non ancora valido. • Mancata corrispondenza indirizzo IP locale o remoto. • Decodifica dell'errore di checksum KRB_AP_PRIV o KRB_AP_SAFE. • Per KRB_AP_PRIV o KRB_AP_SAFE: errore registrazione data/ora, errore ripetizione o errore ordine sequenza. • Per accettazione GSS (graphics symbol set/serie di simboli grafici): credenziali scadute, errore di checksum, o collegamenti canali. • Per unwrap GSS o verifica GSS: contesto scaduto, decrittografia/decodifica, errore di checksum o errore sequenza.
*SECRUN	Sì	Sì	**Funzioni di tempo di esecuzione della sicurezza**: le modifiche apportate al proprietario dell'oggetto, all'autorizzazione e al gruppo principale vengono scritte sul giornale di controllo.
*SECSCKD	Sì	Sì	**Descrittori socket**: viene scritta una voce giornale di controllo quando si verifica uno dei seguenti eventi: • Il descrittore socket viene fornito a un altro lavoro. • Viene ricevuto un descrittore socket. • Un descrittore socket non è utilizzabile.

Tabella 131. Valori di controllo azione (Continua)

Valore possibile	Disponibile sui valori di sistema QAUDLVL e QAUDLVL2	Disponibile sul comando CHGUSRAUD	Descrizione
*SECVFY	Sì	Sì	**Funzioni di verifica**: viene scritta una voce giornale di controllo quando si verifica uno dei seguenti eventi: • Viene generata una gestione o token profilo. • Tutti i token del profilo non sono stati convalidati. • È stato creato il numero massimo di token del profilo. • Tutti i token profilo per un utente sono stati eliminati. • Un profilo utente è stato autenticato. • Un profilo di destinazione è stato modificato durante una sessione pass-through.
*SECVLDL	Sì	Sì	**Operazioni elenco di convalida**: viene scritta una voce giornale di controllo quando si verifica uno dei seguenti eventi: • Aggiunta, modifica, rimozione o rilevamento di una voce dell'elenco di convalida. • Verifica riuscita o non di una voce dell'elenco di convalida.
*SECURITY	Sì	Sì	**Attività di sicurezza**: gli eventi rilevanti della sicurezza, quale la modifica di un profilo utente o di un valore di sistema, vengono registrati. È possibile utilizzare *SECURITY per tenere un record di tutte le attività di sicurezza. *SECURITY è composto da diversi valori in modo da consentire all'utente di personalizzare al meglio il proprio controllo. I valori seguenti compongono *SECURITY: *SECCFG *SECDIRSRV *SECIPC *SECNAS *SECRUN *SECSCKD *SECVFY *SECVLDL
*SERVICE	Sì	Sì	**Attività di sicurezza**: l'utilizzo dei programmi di manutenzione, quali DMPOBJ (Dump oggetto) e STRCPYSCN (Avvio copia schermo) viene registrato. È possibile utilizzare *SERVICE per rilevare i tentativi da parte dell'utente di evitare la sicurezza utilizzando i programmi di manutenzione.
*SPLFDTA	Sì	Sì	**Operazioni su file di spool**: le azioni eseguite sui file di spool vengono registrate, inclusa la creazione, la copia e l'invio. È possibile utilizzare *SPLFDTA per rilevare i tentativi da parte dell'utente di stampare o inviare dati riservati.

Tabella 131. Valori di controllo azione (Continua)

Valore possibile	Disponibile sui valori di sistema QAUDLVL e QAUDLVL2	Disponibile sul comando CHGUSRAUD	Descrizione
*SYSMGT	Sì	Sì	**Attività di gestione sistemi**: il sistema scrive una voce di giornale per le attività di gestione sistemi, quali ad esempio la modifica di un elenco di risposte o la pianificazione dell'accensione/spegnimento. È possibile utilizzare *SYSMGT per rilevare i tentativi da parte dell'utente di utilizzare le funzioni di gestione sistemi per evitare i controlli della sicurezza.

Voci di giornale di controllo sicurezza:

Questo argomento fornisce informazioni sulle voci di giornale scritte per i valori di controllo azione specificati sui valori di sistema QAUDLVL e QAUDLVL2 e nel profilo utente.

Mostra:

- Il tipo di voce scritta sul giornale QAUDJRN.
- Il file di emissione database del modello che è possibile utilizzare per definire il record quando si crea un file di emissione con il comando DSPJRN. Completare i layout per i file di emissione database del modello rilevati nell'Appendice F, "Layout di voci di giornale di controllo", a pagina 595.
- Il tipo di voce descritta nei dettagli. Alcuni tipi di voci del giornale vengono utilizzati per registrare più di un tipo di evento. Il campo del tipo di voce descritta nei dettagli nella voce giornale identifica il tipo di evento.
- L'ID del messaggio che può essere utilizzato per definire le informazioni specifiche della voce nella voce giornale.

Tabella 132. Voci di giornale di controllo sicurezza

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
Controllo operazione:				
*ATNEVT	IM	QASYIMJ5	P	È stata rilevata una potenziale intrusione. È richiesta un'ulteriore valutazione per determinare se si tratta di un'intrusione reale o di un'azione prvista e consentita.

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
*AUTFAIL	AF	QASYAFJE/J4/J5	A	Si è tentato di accedere a un oggetto o è stata eseguita un'operazione da parte di un utente non autorizzato.
			B	Istruzione limitata
			C	Errore di convalida
			D	Utilizzo di interfaccia non supportata, errore dominio oggetto
			E	Errore protezione memoria hardware, violazione spazio costante programma
			F	Errore di autorizzazione ICAPI.
			G	Errore di autenticazione ICAPI.
			H	Operazione di scansione programma di uscita.
			I	Eredità sistema Java non consentita
			J	Si è tentato di inoltrare o pianificare un lavoro sotto una descrizione lavoro con un profilo utente specificato. L'utente che ha effettuato l'inoltro non dispone dell'autorizzazione *USE per il profilo utente.
			K	Si è tentato di eseguire un'operazione per cui l'utente non disponeva dell'autorizzazione speciale richiesta.
			N	Il token profilo non era un token profilo rigenerabile.
			O	Errore autorizzazione oggetto unità ottica
			P	Si è tentato di utilizzare una gestione profilo non valida sull'API QWTSETP.
			R	Errore protezione hardware
			S	Tentativo predefinito di accesso.
			T	Non autorizzato per porta TCP/IP.
			U	Richiesta di autorizzazione utente non valida.
			V	Token profilo non valido per la creazione di un nuovo token profilo.
			W	Token profilo non valido per lo scambio.
			X	Violazione di sistema, consultare la descrizione delle voci di giornale AF (Authority Failure) per dettagli

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
			Y	Non autorizzato per il campo JUID corrente un'operazione di ripulitura JUID.
			Z	Non autorizzato per il campo JUID corrente un'operazione di impostazione JUID.
	CV	QASYCVJ4/J5	E	Collegamento terminato in modo anomalo.
			R	Collegamento rifiutato.
	DI	QASYDIJ4/J5	AF	Errore di autorizzazione.
			PW	Errore della parola d'ordine.
	GR	QASYGRJ4/J5	F	Operazioni di registrazione funzione.
	KF	QASYKFJ4/J5	P	Immessa parola d'ordine non corretta.
	IP	QASYIPJE/J4/J5	F	Errore autorizzazione per la richiesta IPC.
	PW	QASYPWJE/J4/J5	A	Errore collegamento APPC.
			C	Errore di CHKPWD.
			D	Immesso ID utente dei programmi di manutenzione non corretto.
			E	Immessa parola d'ordine dei programmi di manutenzione non corretta.
			P	Immessa parola d'ordine non corretta.
			Q	Tentativo di accesso (autenticazione utente) non riuscito a causa della disabilitazione del profilo utente.
			R	Tentativo di accesso (autenticazione utente) non riuscito a causa della scadenza della parola d'ordine.
			S	La decodifica SQL di una parola d'ordine non valida.
			U	Nome utente non valido.
			X	Utente dei programmi di manutenzione disabilitato.
			Y	Utente dei programmi di manutenzione non valido.
			Z	Parola d'ordine dei programmi di manutenzione non valida.
	VC	QASYVCJE/J4/J5	R	Collegamento rifiutato a causa di una parola d'ordine non corretta.
	VO	QASYVOJ4/J5	U	Verifica della voce di un elenco di convalida non riuscita.

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
	VN	QASYVNJE/J4/J5	R	Accesso alla rete rifiutato a causa dell'account scaduto, di ore non corrette, dell'ID utente non corretto o della parola d'ordine non corretta.
	VP	QASYVPJE/J4/J5	P	Utilizzata parola d'ordine non corretta.
	X1	QASYX1J5	F	La delega del token identità ha avuto esito negativo.
			U	Il richiamo dell'utente dal token identità ha avuto esito negativo.
	XD	QASYXDJ5	G	Nomi gruppo (associati alla voce DI)
*CMD [1]	CD	QASYCDJE/J4/J5	C	È stato eseguito un programma.
			L	È stata eseguita un'istruzione S/36E Control Language.
			O	È stato eseguito un comando di controllo operatore S/36E.
			P	È stata eseguita una procedura S/36E.
			S	È stato eseguito un comando dopo la sostituzione del comando.
			U	È stata eseguita un'istruzione S/36E Utility Control.
*CREATE [2]	CO	QASYCOJE/J4/J5	N	Creazione di un nuovo oggetto, ad eccezione della creazione di oggetti nella libreria QTEMP.
			R	Sostituzione di un oggetto esistente.
	DI	QASYDIJ4/J5	CO	Oggetto creato.
	XD	QASYXDJ5	G	Nomi gruppo (associati alla voce DI)
*DELETE [2]	DO	QASYDOJE/J4/J5	A	Oggetto eliminato.
			C	Cancellazione in sospeso sincronizzata.
			D	Creazione in sospeso sottoposta a rollback.
			P	Cancellazione in sospeso.
			R	Cancellazione in sospeso sottoposta a rollback.
	DI	QASYDIJ4/J5	DO	Oggetto eliminato.
	XD	QASYXDJ5	G	Nomi gruppo (associati alla voce DI)
*JOBBAS	JS	QASYJSJ5	A	È stato utilizzato il comando ENDJOBABN.
			B	È stato inoltrato un lavoro.
			C	È stato modificato un lavoro.
			E	È stato terminato un lavoro.
			H	È stato congelato un lavoro.

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
			I	È stato scollegato un lavoro.
			N	È stato utilizzato il comando ENDJOB.
			P	Una richiesta di avvio programma è stata allegata ad un lavoro precedentemente avviato.
			Q	Attributi query modificati.
			R	È stato rilasciato un lavoro congelato.
			S	È stato avviato un lavoro.
			U	Comando CHGUSRTRC.
*JOBCHGUSR	JS	QASYJSJ5	M	Modifica profilo o profilo gruppo.
			T	Modifica profilo o profilo gruppo utilizzando un token profilo.
*JOBDTA	JS	QASYJSJE/J4/J5	A	È stato utilizzato il comando ENDJOBABN.
			B	È stato inoltrato un lavoro.
			C	È stato modificato un lavoro.
			E	È stato terminato un lavoro.
			H	È stato congelato un lavoro.
			I	È stato scollegato un lavoro.
			M	Modifica profilo o profilo gruppo.
			N	È stato utilizzato il comando ENDJOB.
			P	È stata allegata una richiesta di avvio programma a un lavoro precedentemente avviato.
			Q	Attributi query modificati.
			R	È stato rilasciato un lavoro congelato.
			S	È stato avviato un lavoro.
			T	Modifica profilo o profilo gruppo utilizzando un token profilo
			U	Comando CHGUSRTRC.
	SG	QASYSGJE/J4/J5	A	Processo segnale i5/OS asincrono.
			P	Segnale PASE (Private Address Space Environment) (PASE) asincrono elaborato.
	VC	QASYVCJE/J4/J5	S	È stato avviato un collegamento.
			E	È stato terminato un collegamento.
	VN	QASYVNJE/J4/J5	F	Scollegamento richiesto.
			O	Collegamento richiesto.
	VS	QASYVSJE/J4/J5	S	È stata avviata una sessione server.
			E	È stata terminata una sessione server.

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
*NETBAS	CV	QASYCVJE/J4/J5	C	Collegamento stabilito.
			E	Collegamento terminato correttamente.
			R	Collegamento rifiutato.
	IR	QASYIRJ4/J5	L	Regole IP caricate da un file.
			N	Regole IP scaricate per un collegamento Sicurezza IP.
			P	Regole IP caricate per un collegamento Sicurezza IP.
			R	Regole IP lette o copiate su un file.
			U	Regole IP scaricate (rimosse).
	IS	QASYISJ4/J5	1	Negoziazione fase 1.
			2	Negoziazione fase 2.
	ND	QASYNDJE/J4/J5	A	È stata rilevata una violazione dal supporto Filtro APPN quando è stato controllato il Filtro ricerca indirizzario.
	NE	QASYNEJE/J4/J5	A	È stata rilevata una violazione dal supporto Filtro APPN quando è stato controllato il Filtro endpoint.
*NETCLU	CU	QASYCUJE/J4/J5	M	Creazione di un oggetto effettuata dall'operazione di controllo cluster.
			R	Creazione di un oggetto effettuata dall'operazione di gestione Gruppo risorsa cluster (*GRP).
*NETCMN	CU	QASYCUJE/J4/J5	M	Creazione di un oggetto effettuata dall'operazione di controllo cluster.
			R	Creazione di un oggetto effettuata dall'operazione di gestione Gruppo risorsa cluster (*GRP).
	CV	QASYCVJ4/J5	C	Collegamento stabilito.
			E	Collegamento terminato correttamente.
	IR	QASYIRJ4/J5	L	Regole IP caricate da un file.
			N	Regola IP scaricata per un collegamento Sicurezza IP.
			P	Regole IP caricate per un collegamento Sicurezza IP.
			R	Regole IP lette o copiate su un file.
			U	Regole IP scaricate (rimosse).
	IS	QASYISJ4/J5	1	Negoziazione fase 1.
			2	Negoziazione fase 2.

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
	ND	QASYNDJE/J4/J5	A	È stata rilevata una violazione dal supporto Filtro APPN quando è stato controllato il Filtro ricerca indirizzario.
	NE	QASYNEJE/J4/J5	A	È stata rilevata una violazione dal supporto Filtro APPN quando è stato controllato il Filtro endpoint.
	SK	QASYSKJ4/J5	A	Accettare
			C	Collegarsi
			D	Indirizzo DHCP assegnato
			F	Posta filtrata
			P	Porta non disponibile
			R	Respingere posta
			U	Indirizzo DHCP negato
*NETFAIL	SK	QASYSKJ4/J5	P	Porta non disponibile
*NETSCK	SK	QASYSKJ4/J5	A	Accettare
			C	Collegarsi
			D	Indirizzo DHCP assegnato
			F	Posta filtrata
			R	Respingere posta
			U	Indirizzo DHCP negato
*OBJMGT [2]	DI	QASYDIJ4/J5	OM	Ridenominazione oggetto
	OM	QASYOMJE/J4/J5	M	Oggetto spostato su una libreria differente.
			R	Oggetto ridenominato.
*OFCSRV	ML	QASYMLJE/J4/J5	O	È stata aperta una registrazione posta.
	SD	QASYSDJE/J4/J5	S	È stata apportata una modifica all'indirizzario di distribuzione del sistema.
*OPTICAL	O1	QASY01JE/J4/J5	R	Aprire indirizzario o file
			U	Modificare o richiamare gli attributi
			D	Cancellare indirizzario file
			C	Creare indirizzario
			X	Rilasciare il file unità ottica congelato
	O2	QASY02JE/J4/J5	C	Copiare file o indirizzario
			R	Ridenominare il file
			B	Effettuare una copia di riserva del file o dell'indirizzario
			S	Salvare il file unità ottica congelato
			M	Spostare il file

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
	O3	QASY03JE/J4/J5	I	Inizializzare il volume
			B	Effettuare una copia di riserva del volume
			N	Ridenominare il volume
			C	Convertire il volume della copia di riserva in principale
			M	Importare
			E	Esportare
			L	Modificare elenco di autorizzazioni
			A	Modificare attributi volume
			R	Lettura assoluta
*PGMADP	AP	QASYAPJE/J4/J5	S	È stata avviato un programma che adotta l'autorizzazione del proprietario. La voce di avvio viene scritta la prima volta che viene utilizzata l'autorizzazione adottata per ottenere accesso a un oggetto, non quando il programma entra nello stack di chiamata.
			E	È stata terminato un programma che adotta l'autorizzazione del proprietario. La voce di termine viene scritta quando il programma lascia lo stack di chiamata. Se si verifica lo stesso programma più di una volta nello stack di chiamata, la voce di termine viene scritta quando l'ultima ricorrenza del programma lascia lo stack.
			A	È stata utilizzata l'autorizzazione adottata durante l'attivazione del programma.
*PGMFAIL	AF	QASYAFJE/J4/J5	B	È stato eseguito un programma con un'istruzione interfaccia macchina limitata.
			C	È stato ripristinato un programma che ha dato errore durante i controlli di convalida programma di ripristino ora. È possibile trovare informazioni sull'errore nel campo *Tipo di violazione valore di convalida* del record.
			D	Un programma ha avuto accesso a un oggetto mediante un'interfaccia non supportata o il programma richiamabile non è elencato come API richiamabile.
			E	Violazione protezione memoria hardware.

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
			R	Si è tentato di aggiornare un oggetto di sola lettura. (La protezione memoria hardware avanzata viene registrata solo al livello di sicurezza 40 o superiore)
*PRTDTA	PO	QASYPOJE/J4/J5	D	L'emissione di stampa è stata stampata direttamente su una stampante.
			R	Emissione inviata al sistema remoto per la stampa.
			S	L'emissione di stampa è stata sottoposta a spool e stampata.
*SAVRST [2]	OR	QASYORJE/J4/J5	N	È stato ripristinato un nuovo oggetto sul sistema.
			E	È stato ripristinato un oggetto che ha sostituito un oggetto esistente.
	RA	QASYRAJE/J4/J5	A	Il sistema ha modificato l'autorizzazione su un oggetto ripristinato. [3]
	RJ	QASYRJJE/J4/J5	A	Una descrizione lavoro che contiene un nome profilo utente è stata ripristinata.
	RO	QASYROJE/J4/J5	A	Il proprietario oggetto è stato modificato in QDFTOWN durante l'operazione di ripristino.[3]
	RP	QASYRPJE/J4/J5	A	È stato ripristinato un programma che adotta l'autorizzazione del proprietario.
	RQ	QASYRQJE/J4/J5	A	È stato ripristinato un oggetto *CRQD con autorizzazione PROFILE(*OWNER).
	RU	QASYRUJE/J4/J5	A	È stata ripristinata l'autorizzazione per un profilo utente utilizzando il comando RSTAUT.
	RZ	QASYRZJE/J4/J5	A	Il gruppo principale per un oggetto è stato modificato durante un'operazione di ripristino.
			O	È stato modificato il controllo di un oggetto con il comando CHGOBJAUD.
			U	Il controllo per un utente è stato modificato con il comando CHGUSRAUD.
*SECCFG	AD	QASYADJE/J4/J5	D	Il controllo di DLO è stato modificato con il comando CHGDLOAUD.
			O	Il controllo di un oggetto è stato modificato con il comando CHGOBJAUD o CHGAUD.

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
			S	L'attributo scansione è stato modificato utilizzando il comando CHGATR o l'API Qp0lSetAttr, o quando è stato creato l'oggetto.
			U	Il controllo per un utente è stato modificato con il comando CHGUSRAUD.
	AU	QASYAUJ5	E	Modifica configurazione EIM (Enterprise Identity Mapping)
	CP	QASYCPJE/J4/J5	A	Operazione di creazione, modifica o ripristino del profilo utente quando si utilizza l'API QSYSRESPA.
	CQ	QASYCQJE/J4/J5	A	È stato modificato un oggetto *CRQD.
	CY	QASYCYJ4/J5	A	Funzione di controllo accesso
			F	Funzione Facility Control
			M	Funzione tasto principale
	DO	QASYDOJE/J4/J5	A	L'oggetto non è stato cancellato sotto controllo sincronizzazione
			C	Cancellazione oggetto in sospeso sincronizzata
			D	La creazione oggetto in sospeso è stata sottoposta a rollback
			P	La cancellazione oggetto è in sospeso (l'operazione di cancellazione è stata effettuata sotto il controllo sincronizzazione)
			R	La cancellazione oggetto in sospeso è stata sottoposta a rollback
	DS	QASYDSJE/J4/J5	A	Richiesta di ripristino della parola d'ordine QSECOFR DST sul valore predefinito fornito dal sistema.
			C	Profilo DST modificato.
	EV	QASYEVJ4/J5	A	Aggiungere.
			C	Modificare.
			D	Cancellare.
			I	Inizializzare lo spazio della variabile di ambiente.
	GR	QASYGRJ4/J5	A	Aggiunto programma di uscita
			D	Programma di uscita rimosso
			F	Operazione di registrazione funzione
			R	Programma di uscita sostituito
	JD	QASYJDJE/J4/J5	A	Il parametro USER di una descrizione lavoro è stato modificato.
	KF	QASYKFJ4/J5	C	Operazione certificato.

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
			K	Operazione file di chiavi.
			T	Operazione root affidabile.
	NA	QASYNAJE/J4/J5	A	È stato modificato un attributo di rete.
	PA	QASYPAJE/J4/J5	A	È stato modificato un programma in modo tale che adotti l'autorizzazione del proprietario.
	SE	QASYSEJE/J4/J5	A	È stata modificata una voce di instradamento sottosistema.
	SO	QASYSOJ4/J5	A	Aggiungere voce.
			C	Modificare voce.
			R	Rimuovere voce.
	SV	QASYSVJE/J4/J5	A	È stato modificato un valore di sistema.
			B	Gli attributi del servizio sono stati modificati.
			C	Modifica all'orologio del sistema.
			E	Modifica all'opzione
			F	Modifica nell'attributo del giornale dell'intero sistema
	VA	QASYVAJE/J4/J5	S	L'elenco di controllo accessi è stato modificato correttamente.
			F	La modifica dell'elenco di controllo accessi non è riuscita.
			V	Verifica della voce elenco di convalida riuscita.
	VU	QASYVUJE/J4/J5	G	Un record di gruppo è stato modificato.
			M	Informazioni globali del profilo utente modificate.
			U	Record utente modificato.
*SECDIRSRV	DI	QASYDIJE/J4/J5	AD	Controllare modifica.
			BN	Collegamento riuscito
			CA	Modifica autorizzazione
			CP	Modifica parola d'ordine
			OW	Modifica proprietà
			PO	Modifica normative
			UB	Scollegamento riuscito
*SECIPC	IP	QASYIPJE/J4/J5	A	La proprietà o l'autorizzazione di un oggetto IPC sono stati modificati.
			C	Creare un oggetto IPC.
			D	Cancellare un oggetto IPC.

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
			G	Richiamare un oggetto IPC.
*SECNAS	X0	QASYX0J4/J5	1	Certificato di servizio valido.
			2	Principal del servizio non corrispondenti.
			3	Principal del client non corrispondenti.
			4	Mancata corrispondenza indirizzo IP certificato.
			5	Decodifica del certificato non riuscita
			6	Decodifica del programma di autenticazione non riuscita
			7	Il dominio non è contenuto nei domini locali e del client
			8	Il certificato Þ un tentativo di ripetizione
			9	Certificato non ancora valido
			A	Decodifica dell'errore di checksum KRB_AP_PRIV o KRB_AP_SAFE
			B	Mancata corrispondenza indirizzo IP remoto
			C	Mancata corrispondenza indirizzo IP locale
			D	Errore registrazione data/ora KRB_AP_PRIV o KRB_AP_SAFE
			E	Errore ripetizione KRB_AP_PRIV o KRB_AP_SAFE
			F	Errore ordine di sequenza KRB_AP_PRIV o KRB_AP_SAFE
			K	Accettazione GSS - credenziale scaduta
			L	Accettazione GSS - errore di checksum
			M	Accettazione GSS - collegamenti canale
			N	Unwrap GSS o contesto verifica GSS scaduta
			O	Unwrap GSS o decrittografia/ decodifica verifica GSS
			P	Unwrap GSS o errore checksum verifica GSS
			Q	Unwrap GSS o errore di sequenza verifica GSS
*SECRUN	CA	QASYCAJE/J4/J5	A	Modifiche apportate all'elenco di autorizzazioni o all'autorizzazione oggetto.

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
	OW	QASYOWJE/J4/J5	A	Proprietà oggetto modificata.
	PG	QASYPGJE/J4/J5	A	Il gruppo principale di un oggetto è stato modificato.
*SECSCKD	GS	QASYGSJE/J4/J5	G	Il descrittore socket è stato fornito a un altro lavoro. (Viene creato il record di controllo GS se non viene creato per il lavoro corrente).
			R	Ricevere un descrittore.
			U	Impossibile utilizzare il descrittore.
*SECURITY	AD	QASYADJE/J4/J5	D	Il controllo di DLO è stato modificato con il comando CHGDLOAUD.
			O	Il controllo di un oggetto è stato modificato con il comando CHGOBJAUD o CHGAUD.
			S	Attributo di scansione modificato dal comando CHGATR o dall'API Qp01SetAttr
			U	Il controllo per un utente è stato modificato con il comando CHGUSRAUD.
	X1	QASYADJE/J4/J5	D	La delega del token identità ha avuto esito positivo
			G	Il richiamo dell'utente dal token identità ha avuto esito positivo
	AU	QASYAUJ5	E	Modifica configurazione EIM (Enterprise Identity Mapping)
	CA	QASYCAJE/J4/J5	A	Modifiche apportate all'elenco di autorizzazioni o all'autorizzazione oggetto.
	CP	QASYCPJE/J4/J5	A	Operazione di creazione, modifica o ripristino del profilo utente quando si utilizza l'API QSYRESPA.
	CQ	QASYCQJE/J4/J5	A	È stato modificato un oggetto *CRQD.
	CV	QASYCVJ4/J5	C	Collegamento stabilito.
			E	Collegamento terminato correttamente.
			R	Collegamento rifiutato.
	CY	QASYCYJ4/J5	A	Funzione di controllo accesso
			F	Funzione Facility Control
			M	Funzione tasto principale
	DI	QASYDIJ4/J5	AD	Controllare modifica
			BN	Collegamento riuscito
			CA	Modifica autorizzazione
			CP	Modifica parola d'ordine

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
			OW	Modifica proprietà
			PO	Modifica normative
			UB	Scollegamento riuscito
	DO	QASYDOJE/J4/J5	A	L'oggetto non è stato cancellato sotto controllo sincronizzazione
			C	Cancellazione oggetto in sospeso sincronizzata
			D	La creazione oggetto in sospeso è stata sottoposta a rollback
			P	La cancellazione oggetto è in sospeso (l'operazione di cancellazione è stata effettuata sotto il controllo sincronizzazione)
			R	La cancellazione oggetto in sospeso è stata sottoposta a rollback
	DS	QASYDSJE/J4/J5	A	Richiesta di ripristino della parola d'ordine QSECOFR DST sul valore predefinito fornito dal sistema.
			C	Profilo DST modificato.
	EV	QASYEVJ4/J5	A	Aggiungere.
			C	Modificare.
			D	Cancellare.
			I	Inizializzare lo spazio della variabile di ambiente.
	GR	QASYGRJ4/J5	A	Aggiunto programma di uscita
			D	Programma di uscita rimosso
			F	Operazione di registrazione funzione
			R	Programma di uscita sostituito
	GS	QASYGSJE/J4/J5	G	Il descrittore socket è stato fornito a un altro lavoro. (Viene creato il record di controllo GS se non viene creato per il lavoro corrente).
			R	Ricevere un descrittore.
			U	Impossibile utilizzare il descrittore.
	IP	QASYIPJE/J4/J5	A	La proprietà o l'autorizzazione di un oggetto IPC sono stati modificati.
			C	Creare un oggetto IPC.
			D	Cancellare un oggetto IPC.
			G	Richiamare un oggetto IPC.
	JD	QASYJDJE/J4/J5	A	Il parametro USER di una descrizione lavoro è stato modificato.
	KF	QASYKFJ4/J5	C	Operazione certificato.
			K	Operazione file di chiavi.

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
			T	Operazione root affidabile.
	NA	QASYNAJE/J4/J5	A	È stato modificato un attributo di rete.
	OW	QASYOWJE/J4/J5	A	Proprietà oggetto modificata.
	PA	QASYPAJE/J4/J5	A	È stato modificato un programma in modo tale che adotti l'autorizzazione del proprietario.
	PG	QASYPGJE/J4/J5	A	Il gruppo principale di un oggetto è stato modificato.
	PS	QASYPSJE/J4/J5	A	Il profilo utente di destinazione è stato modificato durante una sessione pass-through.
			E	Un utente dell'ufficio ha terminato il lavoro per conto di un altro utente.
			H	La gestione profilo è stata generata mediante l'API QSYGETPH.
			I	Tutti i token del profilo non sono stati convalidati.
			M	È stato creato il numero massimo di token del profilo.
			P	Token profilo generati per l'utente.
			R	Tutti i token profilo per un utente sono stati eliminati.
			S	Un utente dell'ufficio ha avviato il lavoro per conto di un altro utente.
			V	Profilo utente autenticato.
	SE	QASYSEJE/J4/J5	A	È stata modificata una voce di instradamento sottosistema.
	SO	QASYSOJ4/J5	A	Aggiungere voce.
			C	Modificare voce.
			R	Rimuovere voce.
	SV	QASYSVJE/J4/J5	A	È stato modificato un valore di sistema.
			B	Gli attributi del servizio sono stati modificati.
			C	Modifica all'orologio del sistema.
			E	Modifica all'opzione
			F	Modifica nell'attributo del giornale dell'intero sistema
	VA	QASYVAJE/J4/J5	S	L'elenco di controllo accessi è stato modificato correttamente.
			F	La modifica dell'elenco di controllo accessi non è riuscita.

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
	VO		V	Verifica della voce elenco di convalida riuscita.
	VU	QASYVUJE/J4/J5	G	Un record di gruppo è stato modificato.
			M	Informazioni globali del profilo utente modificate.
			U	Record utente modificato.
	X0	QASYX0J4/J5	1	Certificato di servizio valido.
			2	Principal del servizio non corrispondenti
			3	Principal del client non corrispondenti
			4	Mancata corrispondenza indirizzo IP certificato
			5	Decodifica del certificato non riuscita
			6	Decodifica del programma di autenticazione non riuscita
			7	Il dominio non è contenuto nei domini locali e del client
			8	Il certificato Þ un tentativo di ripetizione
			9	Certificato non ancora valido
			A	Decodifica dell'errore di checksum KRB_AP_PRIV o KRB_AP_SAFE
			B	Mancata corrispondenza indirizzo IP remoto
			C	Mancata corrispondenza indirizzo IP locale
			D	Errore registrazione data/ora KRB_AP_PRIV o KRB_AP_SAFE
			E	Errore ripetizione KRB_AP_PRIV o KRB_AP_SAFE
			F	Errore ordine di sequenza KRB_AP_PRIV o KRB_AP_SAFE
			K	Accettazione GSS - credenziale scaduta
			L	Accettazione GSS - errore di checksum
			M	Accettazione GSS - collegamenti canale
			N	Unwrap GSS o contesto verifica GSS scaduta
			O	Unwrap GSS o decrittografia/ decodifica verifica GSS

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
			P	Unwrap GSS o errore checksum verifica GSS
			Q	Unwrap GSS o errore di sequenza verifica GSS
*SECVFY	PS	QASYPSJE/J4/J5	A	Il profilo utente di destinazione è stato modificato durante una sessione pass-through.
	X1	QASYX1J5	D	La delega del token identità ha avuto esito positivo
			G	Il richiamo dell'utente dal token identità ha avuto esito positivo
			E	Un utente dell'ufficio ha terminato il lavoro per conto di un altro utente.
			H	La gestione profilo è stata generata mediante l'API QSYGETPH.
			I	Tutti i token del profilo non sono stati convalidati.
			M	È stato creato il numero massimo di token del profilo.
			P	Token profilo generati per l'utente.
			R	Tutti i token profilo per un utente sono stati eliminati.
			S	Un utente dell'ufficio ha avviato il lavoro per conto di un altro utente.
			V	Profilo utente autenticato.
*SECVLDL	VO		V	Verifica della voce elenco di convalida riuscita.
*SERVICE	ST	QASYSTJE/J4/J5	A	È stato utilizzato un programma di manutenzione.
	VV	QASYVVJE/J4/J5	C	Lo stato del servizio è stato modificato.
			E	Il server è stato arrestato.
			P	Il server è in modalità di pausa.
			R	Il server è stato riavviato.
			S	Il server è stato avviato.
*SPLFDTA	SF	QASYSFJE/J4/J5	A	Il file di spool è stato letto da un utente che non è il proprietario.
			C	È stato creato un file di spool.
			D	È stato cancellato un file di spool.
			H	È stato congelato un file di spool.
			I	È stato creato un file in linea.
			R	È stato rilasciato un file di spool.
			S	È stato salvato un file di spool.

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
			T	È stato ripristinato un file di spool.
			U	È stato modificato un file di spool.
			V	Modificati solo gli attributi dei file di spool non rilevanti per la sicurezza.
*SYSMGT	DI	QASYDIJ4/J5	CF	Modifiche alla configurazione
			CI	Creazione istanza
			DI	Cancellazione istanza
			RM	Gestione replica
	SM	QASYSMJE/J4/J5	B	Opzioni di copia di riserva modificate utilizzando xxxxxxxxxx.
			C	Opzioni di ripulitura automatica modificate utilizzando xxxxxxxxxx.
			D	È stata effettuata una modifica DRDA*.
			F	È stato modificato un file system HFS.
			N	È stata eseguita un'operazione file di rete.
			O	Un elenco di copie di riserva è stato modificato utilizzando xxxxxxxxxx.
			P	La pianificazione per l'accensione/spegnimento è stata modificata utilizzando xxxxxxxxxx.
			S	L'elenco di risposte del sistema è stato modificato.
			T	Ore di ripristino del percorso di accesso modificate.
	VL	QASYVLJE/J4/J5	A	L'account è scaduto.
			D	L'account è disabilitato.
			L	Ore di collegamento superate.
			U	Sconosciuto o non disponibile.
			W	Stazione di lavoro non valida.
Controllo oggetto:				
*CHANGE	DI	QASYDIJ4/J5	IM	Importazione indirizzario LDAP
			ZC	Modifica oggetto
	ZC	QASYZCJ4/J5	C	Modifiche oggetto
			U	Aggiornamento dell'accesso aperto ad un oggetto
	AD	QASYADJEJ4/J5	D	È stato modificato il controllo di un oggetto con il comando CHGOBJAUD.

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
			O	È stato modificato il controllo di un oggetto con il comando CHGOBJAUD.
			S	Attributo di scansione modificato dal comando CHGATR o dall'API Qp01SetAttr
			U	Il controllo per un utente è stato modificato con il comando CHGUSRAUD.
	AU	QASYAUJ5	E	Modifica configurazione EIM (Enterprise Identity Mapping)
	CA	QASYCAJE/J4/J5	A	Modifiche apportate all'elenco di autorizzazioni o all'autorizzazione oggetto.
	OM	QASYOMJE/J4/J5	M	Oggetto spostato su una libreria differente.
			R	Oggetto ridenominato.
	OR	QASYORJE/J4/J5	N	È stato ripristinato un nuovo oggetto sul sistema.
			E	È stato ripristinato un oggetto che ha sostituito un oggetto esistente.
	OW	QASYOWJE/J4/J5	A	Proprietà oggetto modificata.
	PG	QASYPGJE/J4/J5	A	Il gruppo principale di un oggetto è stato modificato.
	RA	QASYRAJE/J4/J5	A	Il sistema ha modificato l'autorizzazione su un oggetto ripristinato.
	RO	QASYROJE/J4/J5	A	Il proprietario oggetto è stato modificato in QDFTOWN durante l'operazione di ripristino.
	RZ	QASYRZJE/J4/J5	A	Il gruppo principale per un oggetto è stato modificato durante un'operazione di ripristino.
	GR	QASYGRJ4/J5	F	Informazione sulla registrazione della funzione[5]
	LD	QASYLDJE/J4/J5	L	Collegare un indirizzario.
			U	Scollegare un indirizzario.
	VF	QASYVFJE/J4/J5	A	Il file è stato chiuso a causa di uno scollegamento di gestione.
			N	Il file è stato chiuso a causa di un normale scollegamento client.
			S	Il file è stato chiuso a causa dello scollegamento della sessione.
	VO	QASYVOJ4/J5	A	Aggiungere voce elenco di convalida.
			C	Modificare voce elenco di convalida.
			F	Trovare voce elenco di convalida.

Tabella 132. Voci di giornale di controllo sicurezza (Continua)

Valore di controllo azione o oggetto	Tipo di voce di giornale	File di emissione database del modello	Voce descritta nei dettagli	Descrizione
			R	Rimuovere voce elenco di convalida.
	VR	QASYVRJE/J4/J5	F	Accesso risorsa non riuscito.
			S	Accesso risorsa riuscito.
	YC	QASYYCJE/J4/J5	C	L'oggetto libreria documento è stato modificato.
	ZC	QASYZCJE/J4/J5	C	Un oggetto è stato modificato.
			U	Aggiornamento dell'accesso aperto ad un oggetto.
*ALL [4]	CD	QASYCDJ4/J5	C	Comando eseguito
	DI	QASYDIJ4/J5	EX	Esportazione indirizzario LDAP
			ZR	Oggetto letto
	GR	QASYGRJ4/J5	F	Informazione sulla registrazione della funzione[5]
	LD	QASYLDJE/J4/J5	K	Ricercare un indirizzario.
	YR	QASYYRJE/J4/J5	R	L'oggetto libreria documento è stato letto.
	ZR	QASYZRJE/J4/J5	R	È stato letto un oggetto.

[1] Questo valore può essere specificato solo per il parametro AUDLVL di un profilo utente. Non è un valore per il valore di sistema QAUDLVL.

[2] Se il controllo oggetto è attivo per un oggetto, viene scritto un record di controllo per un'operazione di creazione, cancellazione, gestione oggetto o ripristino anche se queste azioni non sono incluse nel livello di controllo.

[3] Consultare l'argomento "Ripristino degli oggetti" a pagina 267 per informazioni sulle modifiche autorizzazioni che potrebbero verificarsi dopo il ripristino di un oggetto.

[4] Quando si specifica *ALL, vengono scritte le voci per *CHANGE e *ALL.

[5] Quando l'oggetto QUSRSYS/QUSEXRGOBJ *EXITRG viene controllato.

Pianificazione del controllo dell'accesso agli oggetti

Il sistema operativo i5/OS fornisce un metodo per registrare gli accessi a un oggetto nel giornale di controllo della sicurezza tramite valori di sistema e valori di controllo dell'oggetto per utenti e oggetti. Questa operazione viene denominata *controllo oggetto*.

Il valore di sistema QAUDCTL, il valore OBJAUD per un oggetto e il valore OBJAUD per un profilo utente collaborano per controllare gli accessi all'oggetto. Il valore OBJAUD per l'oggetto e il valore OBJAUD per l'utente che sta utilizzando l'oggetto determinano se è necessario registrare un accesso specifico. Il valore di sistema QAUDCTL avvia e arresta la funzione di controllo dell'oggetto.

La Tabella 133 mostra in che modo i valori OBJAUD per l'oggetto e il profilo utente collaborano.

Tabella 133. Come collaborano il controllo oggetto e utente

Valore OBJAUD per l'oggetto	Valore OBJAUD per l'utente		
	***NONE**	***CHANGE**	***ALL**
*NONE	Nessuna	Nessuna	Nessuna

Tabella 133. Come collaborano il controllo oggetto e utente (Continua)

Valore OBJAUD per l'oggetto	Valore OBJAUD per l'utente		
	***NONE**	***CHANGE**	***ALL**
*USRPRF	Nessuna	Modifica	Modifica e utilizzo
*CHANGE	Modifica	Modifica	Modifica
*ALL	Modifica e utilizzo	Modifica e utilizzo	Modifica e utilizzo

È possibile utilizzare il controllo oggetto per tenere traccia di tutti gli utenti che accedono a un oggetto critico sul sistema. È inoltre possibile utilizzare il controllo oggetto per tenere traccia di tutti gli oggetti cui accede un utente particolare. Il controllo dell'oggetto è uno strumento flessibile che consente di monitorare accessi all'oggetto importanti per l'organizzazione.

Se si desidera trarre vantaggio dalle funzioni del controllo oggetto è necessaria una pianificazione curata. Un controllo progettato in maniera non attenta potrebbe generare molti più record di controllo rispetto a quelli che è possibile analizzare. Ciò potrebbe avere un effetto negativo sulle prestazioni del sistema. Ad esempio, se si imposta il valore OBJAUD su *ALL per una libreria, verrà scritta una voce di controllo ogni volta che il sistema ricerca un oggetto in tale libreria. In una situazione in cui è presente una libreria utilizzata frequentemente su un sistema occupato, si andrà a creare un numero elevato di voci giornale di controllo.

Di seguito sono riportati alcuni esempi di come utilizzare il controllo dell'oggetto.

- Se vengono utilizzati alcuni file critici per tutta l'organizzazione, è possibile verificare periodicamente chi ha accesso a tali file utilizzando la seguente tecnica di esempio:
  1. Impostare il valore OBJAUD per ogni file critico su *USRPRF utilizzando il comando Modifica controllo oggetto:

```
                    Modifica controllo oggetto (CHGOBJAUD)

Immettere le scelte e premere Invio.

Oggetto. . . . . . . . . . . . .   nome-file
  Libreria  . . . . . . . . . . .     nome-libreria
Tipo oggetto  . . . . . . . . . .   *FILE
Unità ASP . . . . . . . . . . . .   *
valore di controllo oggetto . . .   *USRPRF
```

  2. Impostare il valore OBJAUD per ogni utente riportato nell'esempio su *CHANGE o *ALL utilizzando il comando CHGUSRAUD.
  3. Assicurarsi che il valore di sistema QAUDCTL includa *OBJAUD.
  4. Dopo aver creato un esempio dimostrativo, impostare il valore OBJAUD nei profili utente su *NONE o rimuovere *OBJAUD dal valore di sistema QAUDCTL.
  5. Analizzare le voci giornale di controllo utilizzando le tecniche descritte in "Analisi delle voci giornale di controllo con la query o un programma" a pagina 319.
- Se non si è sicuri di chi stia utilizzando un file particolare, è possibile raccogliere informazioni su tutti gli accessi a tale file per un determinato periodo di tempo:
  1. Impostare il controllo oggetto per il file indipendentemente dai valori del profilo utente:

```
CHGOBJAUD OBJECT(nome-libreria/nome-file)
          OBJTYPE(*FILE)  OBJAUD(*CHANGE o *ALL)
```

  2. Assicurarsi che il valore di sistema QAUDCTL includa *OBJAUD.
  3. Dopo aver creato un esempio dimostrativo, impostare il valore OBJAUD nell'oggetto su *NONE.

4. Analizzare le voci giornale di controllo utilizzando le tecniche descritte in “Analisi delle voci giornale di controllo con la query o un programma” a pagina 319.

- Per controllare tutti gli accessi all’oggetto per un utente specifico, effettuare quanto segue:
  1. Impostare il valore OBJAUD per tutti gli oggetti su *USRPRF utilizzando i comandi CHGOBJAUD e CHGAUD:

```
                    Modifica controllo oggetto (CHGOBJAUD)

Immettere le scelte e premere Invio.

Oggetto . . . . . . . . . . . . .   *ALL
  Libreria  . . . . . . . . . . .  *ALLAVL
Tipo oggetto. . . . . . . . . . .   *ALL
Unità ASP . . . . . . . . . . . .   *
Valore di controllo oggetto  . . . . .   *USRPRF
```

     Attenzione: a seconda del numero di oggetti presenti sul sistema, è possibile che questa operazione richieda molte ore per l’esecuzione. Spesso, non è necessario impostare il controllo oggetto per tutti gli oggetti sul sistema, anche perché influirà negativamente sulle prestazioni. Si consiglia di selezionare una sottoserie di tipi di oggetto e librerie per il controllo.
  2. Impostare il valore OBJAUD per un profilo utente specifico su *CHANGE o *ALL utilizzando il comando CHGUSRAUD.
  3. Assicurarsi che il valore di sistema QAUDCTL includa *OBJAUD.
  4. Dopo aver creato un esempio specifico, impostare il valore OBJAUD per il profilo utente su *NONE.

Riferimenti correlati

“Controllo oggetto” a pagina 120
Il valore del controllo dell’oggetto per un profilo utente gestisce il valore di controllo dell’oggetto per un oggetto per stabilire se l’accesso di un oggetto da parte dell’utente viene controllato o meno.

Visualizzazione controllo oggetto:

Utilizzare il comando DSPOBJD per visualizzare il livello di controllo oggetto corrente per un oggetto. Utilizzare il comando DSPDLOAUD per visualizzare il livello di controllo oggetto corrente per un oggetto libreria documento.

Impostazione del controllo predefinito per gli oggetti:

È possibile utilizzare il valore di sistema QCRTOBJAUD e il valore CRTOBJAUD per librerie e indirizzari per impostare il controllo oggetto per gli oggetti appena creati.

Ad esempio, se si desidera che tutti i nuovi oggetti nella libreria INVLIB dispongano di un valore di controllo corrispondente a *USRPRF, utilizzare il seguente comando:

```
CHGLIB LIB(INVLIB) CRTOBJAUD(*USRPRF)
```

Questo comando influenza solo il valore di controllo dei nuovi oggetti. Non modifica il valore di controllo degli oggetti che esistono già nella libreria.

Utilizzare con cautela i valori di controllo predefiniti. Un utilizzo non corretto potrebbe risultare nella creazione di voci non desiderate sul giornale di controllo della sicurezza. Per un utilizzo corretto delle funzioni di controllo oggetto del sistema è necessaria una pianificazione curata.

Come evitare la perdita di informazioni sul controllo

Sono disponibili due valori di sistema che controllano le reazioni del sistema quando condizioni di errore potrebbero causare la perdita di voci giornale di controllo.

Livello forzatura controllo

Il valore di sistema QAUDFRCLVL determina la frequenza con la quale il sistema scrive le voci giornale di controllo dalla memoria alla memoria ausiliaria.

Il valore di sistema QAUDFRCLVL funziona come livello di forzatura per i file di database. È necessario seguire istruzioni simili per determinare il livello di forzatura corretto per l'installazione.

Se si consente al sistema di stabilire quando scrivere le voci nella memoria ausiliaria, esso bilancia l'effetto sulle prestazioni rispetto alla potenziale perdita di informazioni dovuta all'interruzione dell'alimentazione. *SYS è la scelta predefinita.

Se il livello di forzatura viene impostato su un numero basso, si riducono al minimo le possibilità di perdita dei record di controllo ma si potrebbe notare un effetto negativo sulle prestazioni. Se l'installazione non accetta la perdita di record di controllo nel caso di un'interruzione anomala del sistema, è necessario impostare QAUDFRCLVL su 1.

Azione fine controllo

Il valore di sistema QAUDENDACN (Azione fine controllo) determina l'azione che il sistema deve eseguire nel caso in cui non fosse in grado di scrivere le voci sul giornale di controllo.

Il valore predefinito è *NOTIFY. Il sistema effettua le seguenti attività nel caso in cui non sia in grado di scrivere le voci giornale di controllo e QAUDENDACN è *NOTIFY:

1. Il valore di sistema QAUDCTL è impostato su *NONE per impedire ulteriori tentativi di scrittura delle voci.
2. Il messaggio CPI2283 viene inviato alle code messaggi QSYSOPR e QSYSMSG (qualora esistano) ogni ora fino a quando il controllo non viene riavviato con esito positivo.
3. L'elaborazione prosegue normalmente.
4. Se viene eseguito un IPL sul sistema, viene inviato il messaggio CPI2284 alle code messaggi QSYSOPR e QSYSMSG durante l'IPL.

Nota: nella maggior parte dei casi, l'esecuzione di un IPL risolve i problemi che hanno causato l'esito negativo del controllo. Dopo aver riavviato il sistema, impostare il valore di sistema QAUDCTL sul valore corretto. Il sistema tenta di scrivere un record del giornale di controllo ogni volta che viene modificato questo valore di sistema.

È possibile impostare il valore di sistema QAUDENDACN in modo tale che disattivi il sistema dopo un esito negativo del controllo (*PWRDWNSYS). Utilizzare questo valore solo se l'installazione richiede che il controllo sia attivo per l'esecuzione del sistema. Se il sistema non è in grado di scrivere una voce giornale di controllo e il valore di sistema QAUDENDACN è *PWRDWNSYS, si verifica quanto segue:

1. Il sistema si arresta immediatamente (equivale all'immissione del comando PWRDWNSYS *IMMED).
2. Viene visualizzato il codice B900 3D10 di SRC.

Successivamente, è necessario effettuare quanto segue:

1. Avviare un IPL dall'unità di sistema. Assicurarsi che l'unità specificata nel valore di sistema della console (QCONSOLE) sia disattivata.
2. Per completare un IPL, collegarsi alla console utilizzando un utente che dispone dell'autorizzazione speciale *ALLOBJ e *AUDIT.

Il sistema viene avviato in uno stato limitato e visualizza un messaggio che indica che un errore del controllo ha causato l'arresto del sistema.

3. Il valore di sistema QAUDCTL è impostato su *NONE.
4. Per ripristinare il sistema alla modalità normale, impostare il valore di sistema QAUDCTL su un valore diverso da *NONE. Quando si modifica il valore di sistema QAUDCTL, il sistema tenta di scrivere una voce giornale di controllo. Se questa operazione riesce, il sistema ritorna allo stato normale.

   Se il sistema non riesce a ritornare allo stato normale, utilizzare la registrazione lavori per determinare le cause che hanno provocato l'errore del controllo. Correggere il problema e reimpostare il valore QAUDCTL.

Come scegliere di non controllare gli oggetti QTEMP

È possibile scegliere di non controllare gli oggetti QTEMP specificando *NOQTEMP.

È possibile specificare il valore *NOQTEMP come valore per il valore di sistema QAUDCTL. Se si utilizza il valore *NOQTEMP, è inoltre necessario specificare *OBJAUD o *AUDLVL per QAUDCTL. Quando il controllo è attivo ed è stato specificato il valore *NOQTEMP, le seguenti azioni sugli oggetti nella libreria QTEMP NON verranno controllate.

- Modifica o lettura degli oggetti in QTEMP (tipi di voce giornale ZC, ZR).
- Modifica dell'autorizzazione, del proprietario o del gruppo principale degli oggetti in QTEMP (tipi di voce giornale CA, OW, PG).

Utilizzo di CHGSECAUD per impostare il controllo sicurezza

Panoramica:

Utilizzando il comando CHGSECAUD, è possibile attivare il controllo di sicurezza del sistema per le azioni, accertandosi che esista il giornale di sicurezza, impostando il valore di sistema QAUDCTL su *AUDLVL e il valore di sistema QAUDLVL sulla serie predefinita dei valori. La serie predefinita include i controlli di azione *AUTFAIL, *CREATE, *DELETE, *SECURITY e *SAVRST.

```
CHGSECAUD QAUDCTL(*AUDLVL) QAUDLVL(*DFTSET)
```

Scopo: impostare il sistema in modo tale che raccolga gli eventi di sicurezza nel giornale QAUDJRN.

Modalità:

CHGSECAUD
DSPSECAUD

Autorizzazione:

l'utente deve disporre dell'autorizzazione speciale *ALLOBJ e *AUDIT.

Voce di giornale:

CO (creazione oggetto)
SV (modifica valore di sistema)
AD (modifiche controllo utente e oggetto)

Nota: il comando CHGSECAUD crea il giornale e il ricevitore del giornale se non esistenti. Il comando CHGSECAUD successivamente imposta i valori di sistema QAUDCTL, QAUDLVL e QAUDLVL2.

Riferimenti correlati

"Opzioni sul menu Strumenti di sicurezza" a pagina 751
È possibile utilizzare il menu SECTOOLS (Strumenti di sicurezza) per semplificare la gestione e il controllo della sicurezza sul sistema con numerose opzioni e comandi da esso forniti.

Impostazione del controllo della sicurezza

Con il controllo della sicurezza, è possibile raccogliere informazioni sugli eventi di sicurezza nel giornale QAUDJRN.

Panoramica:

Scopo: impostare il sistema in modo tale che raccolga gli eventi di sicurezza nel giornale QAUDJRN.

Modalità:

CRTJRNRCV
CRTJRN QSYS/QAUDJRN
WRKSYSVAL *SEC
CHGOBJAUD
CHGDLOAUD
CHGUSRAUD

Autorizzazione:

Autorizzazione *ADD su QSYS e sulla libreria del ricevitore giornale
Autorizzazione speciale *AUDIT

Voce di giornale:

CO (creazione oggetto)
SV (modifica valore di sistema)
AD (modifiche controllo utente e oggetto)

Nota: è necessario che QSYS/QAUDJRN sia presente prima di poter modificare QAUDCTL, altrimenti la funzione di controllo del sistema non riconosce il nome del giornale e non lo trova.

Per impostare il controllo della sicurezza, effettuare quanto segue. È necessaria l'autorizzazione speciale *AUDIT per completare questa procedura.

1. Creare un ricevitore di giornale in una libreria desiderata utilizzando il comando CRTJRNRCV (Creazione ricevitore di giornale). In questo esempio viene utilizzata la libreria denominata JRNLIB per i ricevitori del giornale.

   ```
   CRTJRNRCV  JRNRCV(JRNLIB/AUDRCV0001) +
              THRESHOLD(100000) AUT(*EXCLUDE)   +
              TEXT('Auditing Journal Receiver')
   ```

   a. Posizionare il ricevitore giornale in una libreria salvata regolarmente. **Non** posizionare il ricevitore giornale nella libreria QSYS, anche se quella sarebbe la posizione del giornale.
   b. Selezionare un nome del ricevitore del giornale che è possibile utilizzare per creare una convenzione di denominazione per un futuro ricevitore del giornale, quale AUDRCV0001. È possibile utilizzare l'opzione *GEN quando si modificano i ricevitori del giornale per continuare la convenzione di denominazione.

      È molto utile utilizzare questo tipo di convenzione di denominazione se si desidera che il sistema gestisca le modifiche dei ricevitori del giornale.
   c. Specificare una soglia del ricevitore appropriata per l'attività e la dimensione del sistema. La dimensione scelta deve basarsi sul numero di transazioni sul sistema e sul numero di azioni che si è scelto di controllare. Se si utilizza il supporto di gestione modifica del giornale del sistema, le soglie del ricevitore del giornale devono avere un valore almeno di 100.000 KB. Per ulteriori informazioni sulla soglia del ricevitore del giornale, fare riferimento a Gestione giornale.
   d. Specificare *EXCLUDE sul parametro AUT per limitare l'accesso alle informazioni memorizzate nel giornale.
2. Creare il giornale QSYS/QAUDJRN utilizzando il comando CRTJRN (Creazione giornale):

```
CRTJRN  JRN(QSYS/QAUDJRN) +
        JRNRCV(JRNLIB/AUDRCV0001) +
        MNGRCV(*SYSTEM) DLTRCV(*NO) +
        AUT(*EXCLUDE) TEXT('Auditing Journal')
```

- Deve essere utilizzato il nome QSYS/QAUDJRN.
- Specificare il nome del ricevitore del giornale creato nel passo precedente.
- Specificare *EXCLUDE sul parametro AUT per limitare l'accesso alle informazioni memorizzate nel giornale. È necessario disporre dell'autorizzazione per aggiungere gli oggetti a QSYS per creare il giornale.
- Utilizzare il parametro *Gestione ricevitore* (MNGRCV) per consentire al sistema di modificare il ricevitore del giornale e collegarne uno nuovo quando il ricevitore collegato supera la soglia specificata nella creazione del ricevitore del giornale. Se si seleziona questa opzione, non è necessario utilizzare il comando CHGJRN per scollegare i ricevitori e creare e collegare nuovi ricevitori manualmente.
- Non consentire al sistema di cancellare ricevitori scollegati. Specificare DLTRCV(*NO), che corrisponde a un valore predefinito. I ricevitori QAUDJRN sono la traccia del controllo sicurezza. Assicurarsi di averli salvati correttamente prima di cancellarli dal sistema.

L'argomento Gestione giornale fornisce ulteriori informazioni sulla gestione dei giornali e sui ricevitori del giornale.

3. Impostare il valore di sistema (QAUDLVL) del livello di controllo o il valore di sistema dell'estensione del livello di controllo (QAUDLVL2) utilizzando il comando WRKSYSVAL. I valori di sistema QAUDLVL e QAUDLVL2 stabiliscono quali azioni vengono registrate sul giornale di controllo per tutti gli utenti sul sistema. Consultare "Pianificazione del controllo delle azioni" a pagina 282.
4. Se necessario, impostare il controllo dell'azione per singoli utenti utilizzando il comando CHGUSRAUD. Consultare "Pianificazione del controllo delle azioni" a pagina 282.
5. Se necessario, impostare il controllo dell'oggetto per oggetti specifici utilizzando i comandi CHGOBJAUD, CHGAUD e CHGDLOAUD. Consultare "Pianificazione del controllo dell'accesso agli oggetti" a pagina 308.
6. Se necessario, impostare il controllo dell'oggetto per utenti specifici utilizzando il comando CHGUSRAUD.
7. Impostare il valore di sistema QAUDENDACN per controllare la reazione del sistema quando non è in grado di accedere al giornale di controllo. Consultare "Azione fine controllo" a pagina 311.
8. Impostare il valore di sistema QAUDFRCLVL per controllare la frequenza con la quale i record di controllo vengono scritti sulla memoria ausiliaria. Consultare "Come evitare la perdita di informazioni sul controllo" a pagina 311.
9. Iniziare il controllo impostando il valore di sistema QAUDCTL su un valore diverso da *NONE.

   È necessario che il giornale QSYS/QAUDJRN sia presente prima di poter modificare il valore di sistema QAUDCTL in un valore diverso da *NONE. Quando si avvia il controllo, il sistema tenta di scrivere un record sul giornale di controllo. Se il tentativo di scrittura non riesce, viene visualizzato un messaggio e il controllo non si avvia.

Gestione del giornale di controllo e dei ricevitori del giornale

Il sistema fornisce un meccanismo per la gestione del giornale di controllo e dei ricevitori del giornale. È possibile utilizzare i metodi descritti in questo argomento per controllare la sicurezza sul sistema.

Il giornale di controllo QSYS/QAUDJRN è destinato solo al 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 SNDJRNE (Invio voce di giornale) o l'API Invio voce di giornale (QJOSJRNE).

Il sistema utilizza una speciale protezione vincoli per essere certo di poter 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
- Spostamento del giornale
- Ripristino del giornale
- Comando WRKJRN

Le informazioni registrate nelle voci del giornale di sicurezza sono descritte nell'Appendice F, "Layout di voci di giornale di controllo", a pagina 595. 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.

È 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 giornale*.

Se si specifica MNGRCV(*USER) per QAUDJRN, viene inviato un messaggio alla coda messaggi della soglia specificata per il giornale quando il ricevitore del giornale raggiunge una soglia della memoria. Il messaggio indica che il ricevitore ha raggiunto la relativa soglia. Utilizzare il comando CHGJRN per scollegare il ricevitore e collegare un nuovo ricevitore del giornale. In questo modo si evitano le condizioni di errore del tipo *Voce non registrata su giornale*. Se si riceve un messaggio, è necessario utilizzare il comando CHGJRN per far continuare il controllo della sicurezza.

La coda messaggi predefinita per un giornale è QSYSOPR. Se l'installazione dispone di un volume elevato di messaggi nella coda messaggi QSYSOPR, è possibile associare una coda messaggi differente, quale AUDMSG, con il giornale QAUDJRN. È possibile utilizzare un programma di gestione messaggi per monitorare la coda messaggi AUDMSG. Quando si riceve un'avvertenza della soglia giornale (CPF7099), è possibile collegare automaticamente un nuovo ricevitore. Se si utilizza modifica di sistema-gestione giornale, viene inviato il messaggio CPF7020 alla coda messaggi del giornale quando l'operazione di modifica giornale del sistema viene completata. È possibile monitorare questo messaggio per capire quando effettuare un salvataggio dei ricevitori di giornale scollegati.

Attenzione: la funzione di ripulitura automatica fornita mediante l'utilizzo dei menu di Operational Assistant non ripulisce i ricevitori QAUDJRN. Per evitare problemi con lo spazio su disco, scollegare, salvare e cancellare regolarmente i ricevitori QAUDJRN.

Consultare l'argomento Gestione giornale per ulteriori informazioni sulla gestione dei giornali e sui ricevitori del giornale.

il giornale QAUDJRN viene creato durante un IPL se non è presente e il valore di sistema QAUDCTL viene impostato su un valore diverso da *NONE. Ciò si verifica solo se si presenta una situazione anomala, quale la sostituzione di un'unità disco o la ripulitura di un lotto di memorie ausiliari.

Informazioni correlate

Gestione giornale

Salvataggio e cancellazione dei ricevitori del giornale di controllo

È necessario scollegare regolarmente il ricevitore del giornale di controllo corrente e collegarne uno nuovo.

Panoramica:

Scopo: collegare un nuovo ricevitore del giornale di controllo; per salvare e cancellare il vecchio ricevitore

Modalità:

- CHGJRN QSYS/QAUDJRN JRNRCV(*GEN)
- JRNRCV(*GEN) SAVOBJ (per salvare il vecchio ricevitore)
- DLTJRNRCV (per cancellare il vecchio ricevitore)

Autorizzazione:
autorizzazione *ALL per il ricevitore del giornale, autorizzazione *USE per il giornale

Voce di giornale:
J (voce di sistema su QAUDJRN)

Nota: selezionare un'ora in cui il sistema non è occupato.

È necessario scollegare regolarmente il ricevitore del giornale di controllo corrente e collegarne uno nuovo per due motivi:

- L'analisi delle voci di giornale risulta più semplice se ciascun ricevitore del giornale contiene le voci per un periodo di tempo gestibile, specifico.
- I ricevitori di giornale grandi possono influenzare le prestazioni del sistema e occupare uno spazio notevole della memoria ausiliaria.

Si consiglia di fare in modo che il sistema gestisca i ricevitori automaticamente. È possibile specificare ciò utilizzando il parametro *Gestione ricevitore* quando si crea il giornale.

Se il controllo azione e il controllo oggetto sono stati impostati per registrare differenti eventi, è necessario specificare un valore soglia grande per il ricevitore del giornale. Se i ricevitori sono gestiti manualmente, è necessario modificare i ricevitori del giornale più volte al giorno. Se si registrano solo pochi eventi, è possibile modificare i ricevitori in modo tale che corrispondano alla pianificazione salvata per la libreria che contiene il ricevitore del giornale.

Il comando CHGJRN viene utilizzato per scollegare un ricevitore e collegarne uno nuovo.

Ricevitori di giornale gestiti dal sistema:

È possibile attenersi alla procedura descritta in questo argomento per salvare o cancellare i ricevitori di giornale.

Se il sistema gestisce i ricevitori, utilizzare la seguente procedura per salvare e cancellare tutti i ricevitori QAUDJRN scollegati:

1. Immettere WRKJRNA QAUDJRN. Il pannello mostra il ricevitore attualmente collegato. Non salvare o cancellare questo ricevitore.
2. Utilizzare F15 per gestire l'indirizzario del ricevitore. L'indirizzario mostra tutti i ricevitori associati al giornale e lo stato corrispondente.
3. Utilizzare il comando SAVOBJ per salvare ogni ricevitore. Non ricevere il ricevitori correntemente collegato.
4. Utilizzare il comando DLTJRNRCV per cancellare ciascun ricevitore dopo il relativo salvataggio.

Un'alternativa alla procedura sopra indicata è quella di utilizzare la coda messaggi del giornale e monitorare il messaggio CPF7020 che indica che il giornale di modifica sistema è stato completato con esito positivo.

Informazioni correlate

 Copia di riserva e ripristino

Ricevitori di giornale gestiti dall'utente:

È possibile attenersi alla procedura qui descritta per scollegare, salvare o cancellare manualmente ricevitori di giornale.

Se si sceglie di gestire i ricevitori del giornale manualmente, utilizzare la seguente procedura per scollegare, salvare e cancellare il ricevitore del giornale:

1. Immettere `CHGJRN JRN(QAUDJRN) JRNRCV(*GEN)`. Questo comando:
   a. Scollega il ricevitore attualmente collegato.
   b. Crea un nuovo ricevitore con il successivo numero in sequenza.
   c. Collega il nuovo ricevitore al giornale.

   Ad esempio, se il ricevitore corrente è AUDRCV0003, il sistema crea e collega un nuovo ricevitore denominato AUDRCV0004.

   Il comando WRKJRNA (Gestione attributi giornale) indica quale ricevitore è attualmente collegato: `WRKJRNA QAUDJRN`.
2. Utilizzare il comando SAVOBJ (Salvataggio oggetto) per salvare il ricevitore del giornale scollegato. Specificare il tipo di oggetto *JRNRCV.
3. Utilizzare il comando DLTJRNRCV (Cancellazione ricevitore giornale) per cancellare il ricevitore. Se si tenta di cancellare il ricevitore senza salvarlo, viene visualizzato in messaggio di avviso.

Arresto della funzione di controllo

È possibile utilizzare periodicamente la funzione di controllo, piuttosto che utilizzarla sempre. Ad esempio, è possibile utilizzarla quando si effettua una verifica di una nuova applicazione. Altrimenti, è possibile utilizzarla per eseguire un controllo sicurezza trimestrale.

Per arrestare la funzione di controllo, effettuare quanto segue:

1. Utilizzare il comando WRKSYSVAL per modificare il valore di sistema QAUDCTL in *NONE. In questo modo il sistema non registra più ulteriori eventi sulla sicurezza.
2. Scollegare il ricevitore giornale corrente utilizzando il comando CHGJRN.
3. Salvare e cancellare il ricevitore scollegato, utilizzando i comandi SAVOBJ e DLTJRNRCV.
4. È possibile cancellare il giornale QAUDJRN dopo aver modificato QAUDCTL in *NONE. Se si desidera ripristinare il controllo sicurezza in futuro, è opportuno lasciare il giornale QAUDJRN sul sistema.

   > Se il giornale QAUDJRN viene impostato con MNGRCV(*SYSTEM), il sistema scollega il ricevitore e ne collega uno quando si esegue un IPL, se il controllo sicurezza è attivo. È necessario cancellare tali ricevitori giornale. Non è necessario salvarli prima di cancellarli poiché non contengono voci di controllo.

Analisi voci giornale di controllo

Una volta impostata la funzione di controllo sicurezza, è possibile utilizzare una serie di metodi differenti per analizzare gli eventi registrati.

- Visualizzare le voci selezionate nella stazione di lavoro tramite il comando DSPJRN (Visualizzazione giornale).

- Copiare le voci selezionate nei file di emissione tramite il comando DSPJRN o CPYAUDJRN (Copia voci giornale di controllo, e quindi utilizzando un programma o uno strumento di interrogazione per analizzare le voci.
- Utilizzare il comando DSPAUDJRNE (Visualizzazione voci giornale di controllo).

  Nota: l'IBM non fornisce più aggiornamenti per il comando DSPAUDJRNE. Il comando non supporta tutti i tipi di record di controllo sicurezza e non fornisce un elenco di tutti i campi per i record da esso supportati.
- Utilizzare il comando RCVJRNE (Ricezione voce di giornale) sul giornale QAUDJRN per ricevere le voci non appena vengono scritte sul giornale QAUDJRN.

Visualizzazione voci giornale di controllo

Panoramica:

Scopo: visualizzare le voci QAUDJRN

Modalità:
comando DSPJRN (Visualizzazione giornale)

Autorizzazione:
autorizzazione *USE per QSYS/QAUDJRN, autorizzazione *USE per il ricevitore del giornale

Il comando DSPJRN (Visualizzazione giornale) consente di visualizzare le voci di giornale selezionate sulla stazione di lavoro. Per visualizzare tali voci, effettuare quanto segue:

1. Immettere `DSPJRN QAUDJRN` e premere F4. Sul pannello di richiesta, è possibile immettere le informazioni per selezionare l'intervallo di voci visualizzato. Ad esempio, è possibile selezionare tutte le voci in un intervallo di date specifico oppure è possibile selezionare solo alcuni tipi di voci, quale un tentativo di accesso non corretto (tipo di voce giornale PW).

   Per impostazione predefinita, vengono visualizzate le voci solo dal ricevitore collegato. È possibile utilizzare RCVRNG(*CURCHAIN) per visualizzare le voci da tutti i ricevitori presenti sul concatenamento di ricevitori per il giornale QAUDJRN, fino a e includendo il ricevitore attualmente collegato.
2. Quando si preme il tasto Invio, viene visualizzato il pannello Visualizzazione voci di giornale:

```
                        Visualizzazione voci di giornale

Giornale  . . . . . :   QAUDJRN        Libreria  . . . . . :   QSYS
Numero sequenza più grande su questo pannello  . . :00000000000000000012
Immettere le opzioni e premere Invio.
  5=Visualizzazione voce completa


Opz    Sequenza  Codice Tipo  Oggetto    Libreria    Lavoro    Ora
              1   J     PR                          SCPF      10:24:55
              2   T     CA                          SCPF      10:24:55
              3   T     CO                          SCPF      10:24:55
              4   T     CA                          SCPF      10:24:55
              5   T     CO                          SCPF      10:24:55
              6   T     CA                          SCPF      10:24:55
              7   T     CO                          SCPF      10:24:55
              8   T     CA                          SCPF      10:24:56
              9   T     CO                          SCPF      10:24:56
             10   T     CA                          SCPF      10:24:57
             11   T     CO                          SCPF      10:24:57
             12   T     CA                          SCPF      10:24:57
                                                                Segue..
F3=Fine   F12=Annullamento
```

3. Utilizzare l'opzione 5 (Visualizzazione voce completa) per visualizzare informazioni su una voce specifica:

```
                          Visualizzazione voci di giornale

Oggetto . . . . . :                  Libreria  . . . . . :
Membro . . . . . :
Dati non completi  . :   No              Dati voci ridotti : *None
Sequenza . . . . . :   1198
Codice . . . . . :   T  - Voce traccia di controllo
Tipo  . . . . . :   CO - Creazione oggetto

            Dati specifici della voce
Colonna     *...+....1....+....2....+....3....+....4....+....5
00001      'NISAVLDCK  QSYS      *PGM    CLE                  '
00051      '                                                  '
00101      '                                                  '
00151      '                                                  '
00201      '                                                  '
00251      '                                                  '
00301      '                                                  '

                                                                  Segue..
Premere Invio per continuare.

F3=Fine   F6=Visualizzazione solo dati specifici della voce
F10=Visualizz. solo dettagli voce    F12=Annullamento    F24=Altri tasti
```

4. È possibile utilizzare F6 (Visualizzazione solo dati specifici della voce) per le voci con un numero notevole di dati specifici della voce. È inoltre possibile selezionare una versione esadecimale di tale pannello. È possibile utilizzare F10 per visualizzare i dettagli relativi alla voce di giornale senza le informazioni specifiche della voce.

   L'Appendice F, "Layout di voci di giornale di controllo", a pagina 595 contiene il layout per ogni tipo di voce di giornale QAUDJRN.

Analisi delle voci giornale di controllo con la query o un programma

Panoramica:

Scopo: visualizzare o stampare le informazioni selezionate dalle voci di giornale.

Modalità:
DSPJRN OUTPUT(*OUTFILE), creare una query o un programma o eseguire una query o un programma

Autorizzazione:
autorizzazione *USE per QSYS/QAUDJRN, autorizzazione *USE per il ricevitore del giornale e autorizzazione *ADD per la libreria del file di emissione

È possibile utilizzare il comando DSPJRN (Visualizzazione giornale) per scrivere le voci selezionate dai ricevitori del giornale di controllo a un file di emissione. È possibile utilizzare un programma o una query per visualizzare le informazioni contenute nel file di emissione.

Per il parametro di emissione del comando DSPJRN, specificare *OUTFILE. Vengono visualizzati ulteriori parametri che richiedono le informazioni sul file di emissione:

```
                        DSPJRN (Visualizzazione giornale)

Immettere le scelte e premere Invio.
:
Emissione. . . . . . . . . . . . . > *OUTFILE
Formato file di emissione . . . . .   *TYPE5
File ricezione emissione . . . .   dspjrnout
  Libreria  . . . . . . . . . . .     mylib
Opzioni membro di emissione:
  Membro ricezione emissione . . .   *FIRST
  Sostituzione o aggiunta record . . . .   *REPLACE
Lunghezza dati voce:
  Formato dati campo  . . . . . .   *OUTFILFMT
  Lunghezza campo lunghezza variabile
  Lunghezza assegnata . . . . . .
```

Tutte le voci relative alla sicurezza nel giornale di controllo contengono le stesse informazioni di intestazione, quali il tipo di voce, la data della voce e il lavoro che ha causato la creazione della voce. Viene fornito QADSPJR5 (con il formato record QJORDJE5) per definire questi campi quando si specifica *TYPE5 come parametro formato del file di emissione. Consultare “Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)” a pagina 596 per ulteriori informazioni.

Per ulteriori informazioni su altri record e sui relativi formati del file di emissione, consultare Appendice F, “Layout di voci di giornale di controllo”, a pagina 595.

Se si desidera eseguire un’analisi dettagliata di un tipo di voce particolare, utilizzare uno dei file di emissione di database del modello forniti. La Tabella 132 a pagina 289 mostra il nome del file di emissione di database del modello per ogni tipo di voce. Appendice F, “Layout di voci di giornale di controllo”, a pagina 595 mostra i layout del file per ogni file di emissione database modello.

Ad esempio, per creare un file di emissione denominato AUDJRNAF5 in QGPL che includa solo voci di errore autorizzazione:

1. Creare un file di emissione vuoto con il formato definito per le voci di giornale AF:
   ```
   CRTDUPOBJ OBJ(QASYAFJ5) FROMLIB(QSYS) +
     OBJTYPE(*FILE) TOLIB(QGPL) NEWOBJ(AUDJRNAF5)
   ```
2. Utilizzare il comando DSPJRN per scrivere le voci di giornale selezionate sul file di emissione:
   ```
   DSPJRN JRN(QAUDJRN) ... +
      JRNCDE(T) ENTTYP(AF) OUTPUT(*OUTFILE) +
      OUTFILFMT(*TYPE5) OUTFILE(QGPL/AUDJRNAF5)
   ```
3. Utilizzare una query o un programma per analizzare le informazioni nel file AUDJRNAF5.

Seguono alcuni esempi su come utilizzare le informazioni QAUDJRN:

- Se si sospetta che un estraneo stia cercando di entrare nel sistema:
  1. Assicurarsi che il valore di sistema QAUDLVL includa *AUTFAIL.
  2. Utilizzare il comando dell’oggetto CRTDUPOBJ per creare un file di emissione vuoto con il formato QASYPWJ5.
  3. La voce di giornale di tipo PW viene registrata quando un utente immette un ID utente e una parola d’ordine non corretti sul pannello di collegamento. Utilizzare il comando DSPJRN per scrivere le voci di giornale di tipo PW sul file di emissione.
  4. Creare un programma query che visualizzi o stampi la data, l’ora e la stazione di lavoro per ogni voce di giornale. Queste informazioni sono utili per determinare quando e come si verificano i tentativi.
- Se si desidera verificare la sicurezza delle risorse definita per una nuova applicazione:
  1. Assicurarsi che il valore di sistema QAUDLVL includa *AUTFAIL.

2. Eseguire delle verifiche dell'applicazione con ID utente differente.
3. Utilizzare il comando dell'oggetto CRTDUPOBJ per creare un file di emissione vuoto con il formato QASYAFJ5.
4. Utilizzare il comando DSPJRN per scrivere voci di giornale di tipo AF sul file di emissione.
5. Creare un programma query che visualizzi o stampi le informazioni sull'oggetto, sul lavoro e sull'utente. Queste informazioni sono utili per determinare quali utenti e funzioni dell'applicazione stanno causando errori di autorizzazione.

- Se si sta pianificando una migrazione al livello di sicurezza 40:
  1. Assicurarsi che il valore di sistema QAUDLVL includa *PGMFAIL e *AUTFAIL.
  2. Utilizzare il comando dell'oggetto CRTDUPOBJ per creare un file di emissione vuoto con il formato QASYAFJ5.
  3. Utilizzare il comando DSPJRN per scrivere voci di giornale di tipo AF sul file di emissione.
  4. Creare un programma query che selezioni il tipo di violazioni che si stanno riscontrando durante il processo di verifica e che stampi le informazioni sul lavoro e sul programma che ha causato la creazione di ogni voce.

     Nota: la Tabella 132 a pagina 289 mostra quale voce di giornale viene scritta per ciascun messaggio di violazione di autorizzazione.

Relazioni tra data/ora di modifica di un oggetto e record del controllo

I prospetti scritti per rilevare le modifiche al programma o ad altri oggetti si basano, talvolta, sul campo Data/Ora di modifica dell'oggetto anziché sulle informazioni nel giornale di controllo sicurezza. Il seguente elenco descrive i motivi per cui potrebbe esserci una differenza tra la data sull'oggetto e la data sull'origine dell'oggetto.

- Il comando CHGPGM viene utilizzato per forzare la nuova creazione del programma ad aggiornare il campo Data/Ora di modifica del programma. Questa operazione scrive un record di controllo ZC (Modifica in oggetto).
- L'API firma oggetto (QYDOSGNO) viene utilizzata per apporre una firma digitale ad un programma o un comando per aggiornare il campo Data/Ora di modifica per il programma o il comando. Tale operazione scrive un record di controllo ZC.

Il sistema operativo può anche aggiornare automaticamente il campo Data/Ora di modifica di un oggetto nelle seguenti situazioni:

- Quando un profilo utente dispone dell'autorizzazione privata a un oggetto e tale oggetto viene eliminato, il sistema aggiorna il campo Data/Ora di modifica di tale profilo utente mente rimuove tale autorizzazione privata.
- Se il controllo di sicurezza è attivo quando si elimina l'oggetto, un record di controllo DO (Delete Operation) viene scritto per l'oggetto eliminato.
- Dal momento che il sistema aggiorna automaticamente ogni profilo utente con autorizzazione privata all'oggetto eliminato, non viene scritto alcun record di controllo per tali profili utente, anche se i relativi campi Data/Ora di modifica vengono aggiornati.

Per tenere traccia del momento in cui gli utenti hanno utilizzato normali interfacce di sistema per modificare gli oggetti, utilizzare il giornale di controllo sicurezza. I prospetti di rilevazione modifiche agli oggetti basate esclusivamente sul campo Data/Ora di modifica possono produrre solo risultati parziali.

Motivi per cui è consigliabile non utilizzare il campo Data/Ora per il controllo sicurezza generale.

La linea guida principale utilizzata per decidere quali elementi controllare per i5/OS è controllare le azioni dell'utente rilevanti per la sicurezza. La seconda linea guida è non scrivere i record di controllo per

operazioni eseguite automaticamente dal sistema operativo. In alcuni casi, è possibile controllare tali operazioni automatiche se il sistema operativo esegue l'operazione tramite una funzione pensata per essere utilizzata dagli utenti.

Gli obiettivi per la manutenzione del campo Data/Ora di modifica di un oggetto sono differenti dagli obiettivi di controllo. Lo scopo principale del campo Data/Ora di modifica è indicare quando è stato modificato un oggetto. Un campo Data/Ora di modifica non indica quali modifiche sono state apportate per l'oggetto e chi ha effettuato la modifica. Uno degli utilizzi principali di questo campo è indicare che occorre salvare l'oggetto tramite il comando SAVCHGOBJ (Salvataggio oggetti modificati). Per eseguire il comando SAVCHGOBJ, non è necessario sapere quando è stata effettuata l'ultima modifica, ma solo che l'oggetto è stato modificato dall'ultimo salvataggio. Questa funzione consente l'ottimizzazione delle prestazioni per i file di database. Il campo Data/Ora di modifica viene aggiornato solo dopo la prima modifica del file in seguito al salvataggio. Le prestazioni possono essere interessate se il campo Data/Ora di modifica è stato aggiornato ad ogni aggiornamento, aggiunta o eliminazione di un record nel file.

Altre tecniche per il monitoraggio della sicurezza

Il giornale di controllo sicurezza (QAUDJRN) è la fonte principale di informazioni sugli eventi relativi alla sicurezza sul sistema. Le seguenti sezioni mostrano altri metodi per osservare gli eventi relativi alla sicurezza e i valori di sicurezza sul sistema.

È possibile trovare ulteriori informazioni nell'Appendice G, "Comandi e menu per i comandi di sicurezza", a pagina 751. Questa sezione include esempi su come utilizzare i comandi e le informazioni sui menu per gli strumenti di sicurezza.

Monitoraggio messaggi sulla sicurezza

Alcuni eventi rilevanti della sicurezza, quali i tentativi di accesso non corretti, danno vita a un messaggio nella coda messaggi QSYSOPR. È inoltre possibile creare una coda messaggi separata denominata QSYSMSG nella libreria QSYS.

Se si crea la coda messaggi QSYSMSG nella libreria QSYS, i messaggi sugli eventi di sistema critici vengono inviati a quella coda messaggi e alla coda QSYSOPR. La coda messaggi QSYSMSG può essere controllata separatamente da un programma o da un operatore di sistema. Ciò fornisce una protezione ulteriore delle risorse di sistema. I messaggi critici del sistema in QSYSOPR vengono alcune volte saltati a causa del volume dei messaggi inviati a quella coda messaggi.

Utilizzo della registrazione cronologica

Non tutti i messaggi di errore di autorizzazione e di violazione dell'integrità vengono trovati nella registrazione QHST. Tali messaggi vengono elencati qui.

Alcuni eventi rilevanti della sicurezza, quali il superamento del numero di tentativi di accesso non riusciti specificati nel valore di sistema QMAXSIGN, causano l'invio di un messaggio alla registrazione lavori QHST. I messaggi di sicurezza sono compresi nell'intervallo tra 2200 e 22FF. Come prefisso hanno CPI, CPF, CPC, CPD e CPA.

A partire dalla Versione 2 Release 3 del programma sul licenza i5/OS, alcuni messaggi di errore di autorizzazione e di violazione dell'integrità non vengono più inviati alla registrazione QHST (cronologia). È possibile ottenere tutte le informazioni disponibili nella registrazione QHST dal giornale di controllo sicurezza. La registrazione di informazioni sul giornale di controllo fornisce prestazioni di sistema migliori e informazioni più complete su tali eventi relativi alla sicurezza rispetto alla registrazione QHST. La registrazione QHST non deve essere considerata come un'origine completa di violazioni di sicurezza. Al contrario, utilizzare le funzioni di controllo sicurezza.

Questi messaggi non vengono più scritti sulla registrazione QHST:

- CPF2218. È possibile rilevare questi eventi nel giornale di controllo specificando *AUTFAIL per il valore di sistema QAUDLVL.
- CPF2240. È possibile rilevare questi eventi nel giornale di controllo specificando *AUTFAIL per il valore di sistema QAUDLVL.
- CPF2220. È possibile rilevare questi eventi nel giornale di controllo specificando *AUTFAIL per il valore di sistema QAUDLVL.
- CPF4AAE. È possibile rilevare questi eventi nel giornale di controllo specificando *AUTFAIL per il valore di sistema QAUDLVL.
- CPF2246. È possibile rilevare questi eventi nel giornale di controllo specificando *AUTFAIL per il valore di sistema QAUDLVL.

Utilizzo dei giornali per monitorare l'attività dell'oggetto

Se si include il valore *AUTFAIL per il controllo dell'azione di sistema (il valore di sistema QAUDLVL), il sistema scrive una voce di giornale di controllo per ogni tentativo di accesso alla risorsa non riuscito. Per gli oggetti critici, è inoltre possibile impostare il controllo oggetto in modo tale che il sistema scrivi una voce di giornale di controllo per ogni accesso riuscito.

Il giornale di controllo registra solo l'accesso all'oggetto. Non registra tutte le transazioni sull'oggetto. Per gli oggetti critici sul sistema, è necessario ricevere informazioni più dettagliate sui dati specifici a cui si è avuto accesso o che sono stati modificati. la registrazione su giornale dell'oggetto è in grado di fornire questi dettagli. La registrazione su giornale dell'oggetto viene utilizzata principalmente per il ripristino e l'integrità dell'oggetto. Fare riferimento all'argomento Journal management per un elenco dei tipi di oggetto che possono essere registrati su giornale e per un elenco di cosa viene registrato su giornale per ciascun tipo di oggetto. Un responsabile della riservatezza può inoltre utilizzare queste voci di giornale per riesaminare le modifiche apportate all'oggetto. Non registrare su giornale gli oggetti presenti sul giornale QAUDJRN.

Le voci di giornale possono includere:

- Identificazione del lavoro, dell'utente e del momento di accesso
- Immagini precedenti o successive di tutte le modifiche apportate all'oggetto
- Record che mostrano quando un oggetto è stato aperto, chiuso, modificato, salvato, creato, eliminato, ecc.

Una voce di giornale non può essere modificata da nessun utente, neanche da un responsabile della riservatezza. È possibile cancellare un intero giornale e un ricevitore del giornale ma questa operazione è facilmente rilevabile.

Se si sta registrando su giornale un file di database, un'area di dati, una coda dati, una libreria o un oggetto IFS, è possibile utilizzare il comando DSPJRN per stampare tutte le modifiche per tale oggetto specifico. Di seguito vengono riportati alcuni esempi:

```
| Immettere il seguente comando per uno specifico file di database.
| DSPJRN JRN(library/journal) +
|        FILE(library/file) OUTPUT(*PRINT)
|
| Immettere il seguente comando per una particolare area di dati.
| DSPJRN JRN(library/journal) +
|        OBJ((library/object name *DTAARA))  OUTPUT(*PRINT)
|
| Immettere il seguente comando per una particolare coda di dati.
| DSPJRN JRN(library/journal) +
|        OBJ((library/object name *DTAQ)  OUTPUT(*PRINT)
|
| Immettere il seguente comando per uno specifico oggetto IFS.
| DSPJRN JRN(library/journal) +
|        OBJPATH(('path name')) OUTPUT(*PRINT)
```

| Immettere il seguente comando per una libreria particolare.
| DSPJRN JRN(library/journal) +
| OBJ(*LIBL/library-name *LIB) OUTPUT(*PRINT)

Ad esempio, se il giornale JRNCUST nella libreria CUSTLIB viene utilizzato per registrare le informazioni su un file CUSTFILE (anche nella libreria CUSTLIB), il comando può essere il seguente:

```
DSPJRN JRN(CUSTLIB/JRNCUST) +
       FILE(CUSTLIB/CUSTFILE) OUTPUT(*PRINT)
```

È anche possibile creare un file di emissione ed effettuare una query o utilizzare SQL per selezionare tutti i record dal file di emissione per un'emissione specifica.

Immettere il seguente comando per creare un file di emissione per un file database specifico.

```
DSPJRN JRN(library/journal) +
                   FILE(library/file name) +
               OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(library/outfile) ENTDTALEN(*CALC)
```

Immettere il seguente comando per creare un file di emissione per un'area dati specifica.

```
DSPJRN JRN(library/journal) +
                   OBJ((library/object name *DTAARA)) +
               OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(library/outfile) ENTDTALEN(*CALC)
```

Immettere il seguente comando per creare un file di emissione per una specifica coda di dati.

```
DSPJRN JRN(library/journal) +
                   OBJ((library/object name *DTAQ)) +
               OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(library/outfile) ENTDTALEN(*CALC)
```

Immettere il seguente comando per creare un file di emissione per un oggetto IFS specifico.

```
DSPJRN JRN(library/journal) +
                   OBJPATH(('path name')) +
               OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(library/outfile) ENTDTALEN(*CALC)
```

Immettere il seguente comando per creare un file di emissione per una libreria specifica.

```
| DSPJRN JRN(library/journal) +
|                   OBJ((*LIBL/library-name *LIB)) +
|               OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(library/outfile) ENTDTALEN(*CALC)
```

Per sapere quali giornali sono presenti sul sistema, utilizzare il comando WRKJRN (Gestione giornali). Per sapere quali oggetti sono registrati su giornale da un giornale particolare, utilizzare il comando WRKJRNA (Gestione attributi giornale).

Informazioni correlate

Gestione giornale

Analisi profili utente

È possibile visualizzare o stampare un elenco completo di tutti gli utenti sul sistema utilizzando il comando DSPAUTUSR (Visualizzazione utenti autorizzati).

È possibile ordinare in sequenza l'elenco per nome profilo o nome profilo gruppo. Di seguito viene riportato un esempio della sequenza del profilo del gruppo.

```
                          Visualizzazione utenti autorizzati

                       Ultima
Profilo     Profilo    modifica  Nessuna
gruppo      utente     par. ord. par. ord. 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 profili utente selezionati

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

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

È 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.

È 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 accesso.
- Elencare tutti gli utenti che non dispongono di una parola d'ordine da utilizzare a livello 0 e 1 selezionando i record in cui il campo Parola d'ordine presente per il livello 0 o 1 (denominato UPENPW nel file di emissione modello) ha il valore N.
- Elencare tutti gli utenti che dispongono di una parola d'ordine che possono utilizzare ai livelli 2 e 3 selezionando i record in cui il campo Parola d'ordine presente per il livello 2 o 3 (denominato UPENPH nel file di emissione del modello) ha il valore Y.

Esame dei profili utente di ampie dimensioni

È possibile valutare l'efficacia della sicurezza di profili utente di ampie dimensioni sul sistema. 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)
   ```

   Nota: Gli oggetti indirizzario e basati sull'indirizzario non vengono stampati. I comandi WRKOBJOWN e WRKOBJPVT possono essere utilizzati per visualizzare oggetti basati sull'indirizzario e oggetti basati sulla libreria, ma non esiste alcuna funzione di stampa associata a tali comandi.

   Alcuni profili utente forniti da IBM sono di dimensioni molto ampie a causa del numero di oggetti che possiedono. 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. Consultare "Analisi dei programmi che adottano l'autorizzazione".

   Riferimenti correlati

   Appendice B, "Profili utente forniti da IBM", a pagina 341
   Questa sezione contiene informazioni sui profili utente forniti con il sistema. Questi profili sono utilizzati come proprietari di oggetto per varie funzioni di sistema. Alcune funzioni di sistema vengono anche eseguite tramite specifici profili utente forniti da IBM.

Analisi delle autorizzazioni oggetto e libreria

È possibile controllare le autorizzazioni oggetto e libreria sul proprio sistema.

È 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)
   ```
2. Utilizzare il comando Visualizzazione autorizzazione oggetto (DSPOBJAUT) per elencare le autorizzazioni a una libreria specifica:
   ```
   DSPOBJAUT OBJ(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(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.

Analisi dei programmi che adottano l'autorizzazione

I programmi che adottano l'autorizzazione di un utente con autorizzazione speciale *ALLOBJ rappresentano un rischio per la sicurezza. È possibile analizzare questi programmi per controllare la sicurezza del sistema.

È possibile utilizzare il seguente metodo per trovare ed esaminare i programmi che adottano l'autorizzazione:

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 profili utente selezionati" a pagina 325 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-unità-asp) OUTPUT(*PRINT)
   ```

   Nota: è possibile che il parametro del tipo di oggetto debba essere *PGM, *SQLPKG o *SRVPGM come indicato dal prospetto DSPPGMADP.
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'autorizzazione adottata di 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-unità-asp) DETAIL(*FULL)
   ```

   Nota: è possibile che il parametro del tipo di oggetto debba essere *PGM, *SQLPKG o *SRVPGM come indicato dal prospetto DSPPGMADP.

Controllo degli oggetti che sono stati modificati

Un oggetto modificato rappresenta spesso un'indicazione che qualcuno sta tentando di manomettere il sistema. È possibile utilizzare il comando CHKOBJITG (Controllo integrità oggetto) per controllare gli oggetti che sono stati modificati.

È 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. È possibile controllare gli oggetti di proprietà di uno o più profili, gli oggetti che corrispondono a un nome percorso o tutti gli oggetti sul sistema. È possibile ricercare gli oggetti di cui è stato modificato il dominio e gli oggetti che sono stati manomessi. È possibile calcolare nuovamente i valori di convalida programma per ricercare gli oggetti di tipo *PGM, *SRVPGM, *MODULE e *SQLPKG che sono stati modificati. È possibile controllare la firma degli oggetti che possono contenere una firma digitale. È possibile controllare se le librerie e i comandi sono stati manomessi. È inoltre possibile avviare una scansione dell'IFS (integrated file system) o controllare se gli oggetti hanno avuto esito negativo in una precedente scansione dell'integrated file system.

L'esecuzione del comando CHKOBJITG richiede l'autorizzazione speciale *AUDIT. È 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. La maggior parte dei comandi IBM duplicati da

un release precedente alla V5R2 verranno registrati come violazioni. È necessario cancellare e creare nuovamente tali comandi utilizzando il comando CRTDUPOBJ (Creazione oggetto duplicato) ogni volta che viene caricato un nuovo release.

Informazioni correlate

Scanning support

Controllo del sistema operativo

È possibile utilizzare l'API QYDOCHKS (Controllo sistema) per controllare se un oggetto del sistema operativo con chiave è stato modificato dal momento in cui è stato firmato.

Gli oggetti non firmati o che sono stati modificati dopo la firma verranno riportati come errori. Solo le firme provenienti da un'origine protetta del sistema sono valide.

Per eseguire le API QYDOCHKS è necessario disporre dell'autorizzazione speciale *AUDIT. È possibile che l'API impieghi del tempo per eseguire, poiché deve effettuare dei calcoli. Sarebbe opportuno eseguirlo quando il sistema non è occupato.

Riferimenti correlati

Check System (QYDOCHKS) API

Controllo delle azioni del responsabile della riservatezza

È possibile tenere traccia di tutte le azioni eseguite dagli utenti con autorizzazione speciale *ALLOBJ e *SECADM.

Per effettuare ciò, è possibile utilizzare il valore di controllo azione nel profilo utente:

1. Per ogni utente con autorizzazione speciale *ALLOBJ e *SECADM, utilizzare il comando CHGUSRAUD per impostare AUDLVL in modo che disponga di tutti i valori non inclusi nei valori di sistema QAUDLVL o QAUDLVL2 sul sistema. Ad esempio, se il valore di sistema QAUDLVL è impostato su *AUTFAIL, *PGMFAIL, *PRTDTA e *SECURITY, utilizzare questo comando per impostare AUDLVL per un profilo utente di responsabile della riservatezza:

   ```
   CHGUSRAUD USER(SECUSER) +
             AUDLVL(*CMD *CREATE *DELETE +
                    *OBJMGT *OFCSRV *PGMADP +
                    *SAVRST *SERVICE, +
                    *SPLFDTA *SYSMGT)
   ```

   la "Controllo azione" a pagina 121 mostra tutti i valori possibili per il controllo dell'azione.
2. Rimuovere l'autorizzazione speciale *AUDIT dai profili utente con autorizzazione speciale *ALLOBJ e *SECADM. In questo modo, si impedisce agli utenti di modificare le caratteristiche di controllo dei relativi profili.

   non è possibile rimuovere autorizzazioni speciali dal profilo QSECOFR. Pertanto, non è possibile impedire a un utente collegato come QSECOFR di modificare le caratteristiche di controllo di tale profilo. Tuttavia, se un utente collegato come QSECOFR utilizza il comando CHGUSRAUD per modificare le caratteristiche di controllo, viene scritta una voce di tipo AD sul giornale di controllo.

   È preferibile che i responsabili della riservatezza (utenti con autorizzazione speciale *ALLOBJ o *SECADM) utilizzino i propri profili per un controllo migliore. La parola d'ordine per il profilo QSECOFR non deve essere distribuita.
3. Assicurarsi che il valore di sistema QAUDCTL includa *AUDLVL.
4. Utilizzare il comando DSPJRN per rivedere le voci nel giornale di controllo utilizzando le tecniche descritte in "Analisi delle voci giornale di controllo con la query o un programma" a pagina 319.

Capitolo 10. Informazioni sull'esonero di responsabilità e licenza codice

IBM fornisce una licenza non esclusiva per utilizzare tutti gli esempi del codice di programmazione da cui creare funzioni simili personalizzate, in base a richieste specifiche.

IN BASE ALLE GARANZIE INDEROGABILMENTE PREVISTE DALLA LEGGE, IBM NON RILASCIA ALCUNA GARANZIA O CONDIZIONE, ESPRESSA O IMPLICITA, INCLUSA SENZA LIMITAZIONE, LA GARANZIA DI FUNZIONAMENTO ININTERROTTO E LE GARANZIE IMPLICITE DI COMMERCIABILITA' ED IDONEITA' AD UNO SCOPO SPECIFICO, RELATIVE AI PROGRAMMI O A QUALSIASI SUPPORTO TECNICO.

IN NESSUN CASO IBM SARA' RESPONSABILE PER QUALSIASI DANNO DIRETTO O INDIRETTO, ANCHE QUALORA IBM FOSSE A CONOSCENZA DEL POSSIBILE VERIFICARSI DI TALI DANNI:

1. PERDITE O DANNEGGIAMENTI DI DATI;
2. DANNO SPECIALE, INCIDENTALE, DIRETTO O INDIRETTO O QUALSIASI DANNO ECONOMICO CONSEGUENTE O
3. MANCATI GUADAGNI, PERDITE DI REDDITI, DI BENEFICI O DI RISPARMI ANTICIPATI.

LA LEGISLAZIONE DI ALCUNI PAESI NON CONSENTE L'ESCLUSIONE O LA LIMITAZIONE DI DANNI INCIDENTALI, DIRETTI O CONSEQUENZIALI, PERTANTO LE SUDDETTE ESCLUSIONI O LIMITAZIONI POTREBBERO NON ESSERE APPLICABILI.

Appendice A. Comandi di sicurezza

Questa sezione contiene i comandi di sistema relativi alla sicurezza. È possibile utilizzare questi comandi al posto dei menu di sistema, immettendoli in una riga comandi. I comandi sono suddivisi in gruppi orientati sull'attività.

L'argomento CL (Control language) contiene informazioni più dettagliate su questi comandi. Le tabelle nell'Appendice D, "Autorizzazione richiesta per gli oggetti utilizzati dai comandi", a pagina 361 indicano quali autorizzazioni oggetto sono necessarie per utilizzare questi comandi.

Per ulteriori informazioni sugli strumenti e suggerimenti su come utilizzare gli strumenti della sicurezza, consultare Configuring the system to use security tools topic.

Comandi archivi autorizzazioni

Questa tabella fornisce un elenco dei comandi che consentono all'utente di gestire gli archivi autorizzazioni.

Tabella 134. Comandi archivi autorizzazioni

Nome comando	Nome descrittivo	Funzione
CRTAUTHLR	Creazione archivio autorizzazione	proteggere un file prima ancora che il file esista. Gli archivi autorizzazioni sono validi solo per file di database descritti dal programma.
DLTAUTHLR	Cancellazione archivio autorizzazione	Cancellare un archivio autorizzazioni. Se il file associato esiste, le informazioni sull'archivio autorizzazioni vengono copiate nel file.
DSPAUTHLR	Visualizzazione archivio autorizzazioni	Visualizzare tutti gli archivi autorizzazioni sul sistema.

Comandi elenchi autorizzazioni

È possibile utilizzare questi comandi per eseguire attività differenti sugli elenchi autorizzazioni.

Tabella 135. Comandi elenchi autorizzazioni

Nome comando	Nome descrittivo	Funzione
ADDAUTLE	Aggiunta voce elenco autorizzazioni	Aggiungere un utente a un elenco autorizzazioni. Si specifica di quale autorizzazione l'utente dispone per tutti gli oggetti nell'elenco.
CHGAUTLE	Modifica voce elenco autorizzazioni	Modificare le autorizzazioni degli utenti agli oggetti sull'elenco autorizzazioni.
CRTAUTL	Creazione elenco autorizzazioni	Creare un elenco autorizzazioni.
DLTAUTL	Cancellazione elenco autorizzazioni	Cancellare un elenco autorizzazioni completo.
DSPAUTL	Visualizzazione elenco autorizzazioni	Visualizzare un elenco di utenti e rispettive autorizzazioni in un elenco di autorizzazioni.
DSPAUTLOBJ	Visualizzazione oggetti elenco autorizzazioni	Visualizzare un elenco di oggetti protetti da un elenco autorizzazioni.
EDTAUTL	Editazione elenco autorizzazioni	Aggiungere, modificare e rimuovere utenti e relative autorizzazioni in un elenco di autorizzazioni.

Tabella 135. Comandi elenchi autorizzazioni (Continua)

Nome comando	Nome descrittivo	Funzione
RMVAUTLE	Eliminazione voce elenco autorizzazioni	Rimuovere un utente da un elenco di autorizzazioni.
RTVAUTLE	Richiamo voce elenco autorizzazioni	Utilizzato in un programma CL (control language) per richiamare uno o più valori associati ad un utente nell'elenco di autorizzazioni. Il comando può essere utilizzato insieme al comando CHGAUTLE per fornire ad un utente nuove autorizzazioni in aggiunta a quelle esistenti di cui l'utente già dispone.
WRKAUTL	Gestione elenchi di autorizzazioni	Gestire elenchi di autorizzazioni da un pannello di elenco.

Comandi controllo e autorizzazione oggetto

È possibile fare riferimento a questa tabella per i comandi che l'utente può utilizzare per gestire il controllo e l'autorizzazione oggetto.

Tabella 136. Comandi controllo e autorizzazione oggetto

Nome comando	Nome descrittivo	Funzione
CHGAUD	Modifica controllo	Modificare il valore di controllo di un oggetto.
CHGAUT	Modifica autorizzazione	Modificare l'autorizzazione degli utenti agli oggetti.
CHGOBJAUD	Modifica controllo oggetto	Specificare se l'accesso a un oggetto è controllato.
CHGOBJOWN	Modifica proprietario oggetto	Modificare la proprietà di un oggetto da un utente ad un altro.
CHGOBJPGP	Modifica gruppo principale oggetto	Modificare il gruppo principale di un oggetto in un altro utente o in nessun gruppo principale.
CHGOWN	Modifica proprietario	Modificare la proprietà di un oggetto da un utente ad un altro.
CHGPGP	Modifica gruppo principale	Modificare il gruppo principale di un oggetto in un altro utente o in nessun gruppo principale.
DSPAUT	Visualizzazione autorizzazione	Visualizzare l'autorizzazione degli utenti a un oggetto.
DSPLNK	Visualizzazione collegamenti	Visualizzare un elenco di nomi di oggetti specificati in indirizzari e opzioni per visualizzare informazioni sugli oggetti.
DSPOBJAUT	Visualizzazione autorizzazione oggetto	Visualizza il proprietario dell'oggetto, l'autorizzazione pubblica per l'oggetto, qualsiasi autorizzazione privata ad esso relativa ed il nome dell'elenco di autorizzazioni utilizzato per proteggere l'oggetto.
DSPOBJD	Visualizzazione descrizione oggetto	Visualizza il livello di controllo oggetto relativo all'oggetto.
EDTOBJAUT	Editazione autorizzazione oggetto	Aggiungere, modificare o rimuovere l'autorizzazione utente per l'oggetto.
GRTOBJAUT	Concessione autorizzazione oggetto	concedere in modo specifico l'autorizzazione ad utenti denominati, a tutti gli utenti (*PUBLIC) o ad utenti dell'oggetto a cui si fa riferimento per gli oggetti denominati in questo comando.
RVKOBJAUT	Revoca autorizzazione oggetto	Rimuovere una o più (anche tutte) le autorizzazioni concesse in modo specifico ad un utente per gli oggetti denominati.

Tabella 136. Comandi controllo e autorizzazione oggetto (Continua)

Nome comando	Nome descrittivo	Funzione
WRKAUT	Gestione autorizzazione	Gestire l'autorizzazione per l'oggetto selezionando opzioni in un pannello di elenco.
WRKLNK	Gestione collegamenti	Visualizzare un elenco di nomi di oggetti specificati in indirizzari e opzioni per gestire gli oggetti.
WRKOBJ	Gestione oggetti	Gestire l'autorizzazione per l'oggetto selezionando opzioni in un pannello di elenco.
WRKOBJOWN	Gestione oggetti per proprietario	Gestire gli oggetti posseduti da un profilo utente.
WRKOBJPGP	Gestione oggetti per gruppo principale	Gestire gli oggetti per cui un profilo è il gruppo principale utilizzando opzioni da un pannello di elenco.
WRKOBJPVT	Gestione oggetti per autorizzazioni private	Gestire gli oggetti per cui un profilo viene autorizzato privatamente, utilizzando opzioni da un pannello di elenco.

Comandi parole d'ordine

Questi comandi consentono all'amministratore della riservatezza di assegnare, modificare, verificare o reimpostare la parola d'ordine associata ad un profilo utente.

Tabella 137. Comandi parole d'ordine

Nome comando	Nome descrittivo	Funzione
CHGDSTPWD	Modifica parola d'ordine DST	Reimpostare il profilo delle funzioni della sicurezza DST sulla parola d'ordine predefinita fornita con il sistema.
CHGPWD	Modifica parola d'ordine	Modificare la parola d'ordine dell'utente.
CHGUSRPRF	Modifica profilo utente	Modificare i valori specificati nel profilo di un utente, inclusa la parola d'ordine dell'utente.
CHKPWD	Controllo parola d'ordine	Verificare una parola d'ordine dell'utente. Ad esempio, se si desidera che l'utente immetta di nuovo la parola d'ordine per eseguire una particolare applicazione, è possibile utilizzare CHKPWD nel proprio programma CL per verificare la parola d'ordine.
CRTUSRPRF[1]	Creazione profilo utente	Quando si aggiunge un utente al sistema, si assegna ad esso una parola d'ordine.

[1] Quando si esegue CRTUSRPRF, non è possibile specificare la creazione di *USRPRF in un ASP (auxiliary storage pool) indipendente. Tuttavia, quando un utente dispone di un'autorizzazione privata per un oggetto in un ASP indipendente, è il proprietario di un oggetto in un ASP indipendente o è il gruppo principale di un oggetto in un ASP indipendente, il nome del profilo viene memorizzato nell'ASP indipendente. Se l'ASP indipendente viene spostato in un altro sistema, le voci autorizzazione privata, proprietà dell'oggetto e gruppo principale verranno associate al profilo con lo stesso nome sul sistema di destinazione. Se un profilo non esiste sul sistema di destinazione, verrà creato un profilo. L'utente non disporrà di alcuna autorizzazione speciale e la parola d'ordine verrà impostata su *NONE.

Comandi profili utente

Come amministratore della riservatezza, è necessario utilizzare questi comandi per gestire i profili utente.

Tabella 138. Comandi profili utente

Nome comando	Nome descrittivo	Funzione
CHGPRF	Modifica profilo	Modificare alcuni attributi del profilo dell'utente.

Tabella 138. Comandi profili utente (Continua)

Nome comando	Nome descrittivo	Funzione
CHGUSRAUD	Modifica controllo utente	Specificare il controllo dell'operazione e del controllo oggetto per un profilo utente.
CHGUSRPRF	Modifica profilo utente	Modificare i valori specificati nel profilo di un utente come ad esempio la parola d''ordine dell'utente, le autorizzazioni speciali, il menu iniziale, il programma iniziale, la libreria corrente ed il limite di priorità.
CHKOBJITG	Controllo integrità oggetto	Controllare gli oggetti di proprietà di uno o più profili utente o controllare gli oggetti che corrispondono al nome percorso per garantire che gli oggetti non siano stati manomessi.
CRTUSRPRF	Creazione profilo utente	Aggiungere un utente al sistema e specificare valori come ad esempio la parola d'ordine dell'utente, le autorizzazioni speciali, il menu iniziale, il programma iniziale, la libreria corrente ed il limite di priorità.
DLTUSRPRF	Cancellazione profilo utente	Cancellare un profilo utente dal sistema. Questo comando fornisce un'opzione per cancellare o modificare la proprietà di oggetti posseduti da un profilo utente.
DMPUSRPRF	Profilo utente dump	Consente di eseguire il dump del profilo utente e delle informazioni correlate.
DSPAUTUSR	Visualizzazione utenti autorizzati	Consente di visualizzare o stampare quanto segue per tutti i profili utente sul sistema: profilo gruppo associato (se esistente), se il profilo utente ha una parola d'ordine utilizzabile a qualsiasi livello di parola d'ordine, se il profilo utente ha una parola d'ordine utilizzabile ai vari livelli della parola d'ordine, se il profilo utente ha una parola d'ordine utilizzabile con NetServer, la data dell'ultima modifica della parola d'ordine ed il testo del profilo utente.
DSPSSTUSR	Visualizzazione ID utente programmi di manutenzione	Visualizza un elenco di ID utente dei programmi di manutenzione. Esso può anche essere utilizzato per visualizzare informazioni dettagliate relative a uno specifico ID utente dei programmi di manutenzione, includendo lo stato ed i privilegi di tale utente.
DSPUSRPRF	Comando Visualizzazione profilo utente	Visualizzare un profilo utente in diversi formati.
GRTUSRAUT	Concessione autorizzazione utente	Copiare le autorizzazioni private da un profilo utente ad un altro profilo utente.
PRTPRFINT	Stampa valori interni profilo	Stampare un prospetto di informazioni contenente informazioni relative ai valori interni sul numero di voci.
PRTUSRPRF	Stampa profilo utente	Analizzare i profili utente che soddisfano i criteri specificati.
RTVUSRPRF	Richiamo profilo utente	Utilizzato in un programma CL(control language) per richiamare ed utilizzare uno o più valori memorizzati e associati ad un profilo utente.
WRKUSRPRF	Gestione profili utente	Gestire i profili utente immettendo opzioni su un pannello di elenco.

Comandi profilo utente correlati

Questa tabella elenca altri comandi correlati ai profili utente. Questi comandi consentono di ripristinare o salvare i profili utente ed i relativi attributi.

Tabella 139. Comandi profilo utente correlati

Nome comando	Nome descrittivo	Funzione
DSPPGMADP	Visualizzazione programmi di adozione	Visualizza un elenco di programmi e pacchetti SQL che adottano un profilo utente specificato.
RSTAUT	Ripristino autorizzazione	Ripristina le autorizzazioni per oggetti congelati da un profilo utente quando il profilo utente è stato salvato. Queste autorizzazioni possono essere ripristinate solo dopo il ripristino di un profilo utente con il comando RSTUSRPRF (Ripristino profilo utente).
RSTUSRPRF	Ripristino profilo utente	Ripristina un profilo utente ed i relativi attributi. Il ripristino dell'autorizzazione specifica per gli oggetti viene eseguito tramite il comando RSTAUT dopo il ripristino del profilo utente. Il comando RSTUSRPRF ripristina anche tutti gli elenchi di autorizzazioni ed gli archivi autorizzazioni se viene specificato RSTUSRPRF(*ALL).
SAVSECDTA	Salvataggio dati di sicurezza	Salva tutti i profili utente, gli elenchi di autorizzazioni e gli archivi autorizzazioni senza utilizzare un sistema che si trova in stato limitato.
SAVSYS	Salvataggio sistema	Salva tutti i profili utente, gli elenchi di autorizzazioni e gli archivi autorizzazioni nel sistema. È necessario un sistema dedicato per utilizzare questa funzione.

Comandi controllo

È possibile utilizzare questi comandi per gestire il controllo su un oggetto.

Tabella 140. Comandi controllo

Nome comando	Nome descrittivo	Funzione
CHGAUD	Modifica controllo	Specificare il controllo per un oggetto.
CHGDLOAUD	Modifica controllo DLO	Specificare se l'accesso è controllato per un DLO (document library object).
CHGOBJAUD	Modifica controllo oggetto	Specificare il controllo per un oggetto.
CHGUSRAUD	Modifica controllo utente	Specificare il controllo dell'operazione e del controllo oggetto per un profilo utente.

Comandi DLO (Oggetti libreria documenti)

Questa tabella elenca i comandi che l'utente può utilizzare per gestire DLO (Oggetti libreria documenti).

Tabella 141. Comandi DLO (Oggetti libreria documenti)

Nome comando	Nome descrittivo	Funzione
ADDDLOAUT	Aggiunta autorizzazione DLO	Fornire ad un utente accesso ad un documento o ad una cartella o di proteggere un documento o una cartella tramite un elenco di autorizzazioni o un codice di accesso.

Tabella 141. Comandi DLO (Oggetti libreria documenti) (Continua)

Nome comando	Nome descrittivo	Funzione
CHGDLOAUD	Modifica controllo DLO	Specificare il livello di controllo oggetto per un DLO (document library object).
CHGDLOAUT	Modifica autorizzazione DLO	Modificare l'autorizzazione per un documento o una cartella.
CHGDLOOWN	Modifica proprietario DLO	Trasferisce la proprietà del documento della cartella da un utente ad un altro.
CHGDLOPGP	Modifica gruppo principale DLO	modificare il gruppo principale per un DLO (document library object).
DSPAUTLDLO	Visualizzazione DLO elenco autorizzazioni)	Visualizzare i documenti e le cartelle protetti dall'elenco di autorizzazioni specificato.
DSPDLOAUD	Visualizzazione controllo DLO	Visualizza il livello di controllo oggetto per un DLO (document library object).
DSPDLOAUT	Visualizzazione autorizzazione DLO	Visualizzare informazioni sull'autorizzazione per un documento o una cartella.
EDTDLOAUT	Editazione autorizzazione DLO	Aggiungere, modificare o rimuovere le autorizzazioni utenti ad un documento o ad una cartella.
GRTUSRPMN	Concessione permesso utente	Concede il permesso ad un utente di gestire documenti e cartelle o di eseguire attività relative a office per conto di un altro utente.
RMVDLOAUT	Rimozione autorizzazione DLO	Rimozione dell'autorizzazione dell'utente da documenti o cartelle.
RVKUSRPMN	Revoca permesso utente	Revoca l'autorizzazione documento da un utente (o da tutti gli utenti) per accedere a documenti per conto di un altro utente.

Comandi voci di autenticazione server

Questi comandi consentono di visualizzare, aggiungere, rimuovere o modificare le voci di autenticazione server per un profilo utente.

Tabella 142. Comandi voci di autenticazione server

Nome comando	Nome descrittivo	Funzione
ADDSVRAUTE	Aggiunta voce autenticazione server	Aggiungere informazioni sull'autenticazione server associate per un profilo utente.
CHGSVRAUTE	Modifica voce autenticazione server	Modificare le voci di autenticazione server esistenti per un profilo utente.
DSPSVRAUTE	Visualizzazione voci autenticazione server	Visualizzare le voci di autenticazione server per un profilo utente.
RMVSVRAUTE	Rimozione voce autenticazione server	Rimuovere le voci di autenticazione server dal profilo utente specificato.
Questi comandi consentono ad un utente di specificare un nome utente, la parola d'ordine associata ed il nome di una macchina server remota. DRDA (Distributed Relational Database Access) utilizza queste voci per eseguire richieste di accesso al database come l'utente specificato sul server remoto.		

Comandi indirizzario distribuzione del sistema

È possibile utilizzare questi comandi per aggiungere, rimuovere o modificare le voci nell'indirizzario distribuzione di sistema.

Tabella 143. Comandi indirizzario distribuzione del sistema

Nome comando	Nome descrittivo	Funzione
ADDDIRE	Aggiunta voce indirizzario	Aggiunge nuove voci all'indirizzario di distribuzione del sistema. L'indirizzario contiene informazioni su un utente, come ad esempio l'ID utente e l'indirizzo, il nome di sistema, il nome del profilo utente, l'indirizzo di posta ed il numero telefonico.
CHGDIRE	Modifica voce indirizzario	Modifica i dati per una specifica voce nell'indirizzario di distribuzione del sistema. Il responsabile di sistema ha l'autorizzazione per aggiornare qualsiasi dato contenuto in una voce indirizzario, eccetto l'ID utente, l'indirizzo e la descrizione dell'utente. Gli utenti possono aggiornare le proprie voci indirizzario, ma sono limitati all'aggiornamento di certi campi.
RMVDIRE	Rimozione voce indirizzario	Elimina una voce specifica dall'indirizzario di distribuzione del sistema. Quando un ID utente ed un indirizzo vengono eliminati dall'indirizzario vengono eliminati anche da qualunque elenco di distribuzione.
WRKDIRE	Gestione indirizzario	Fornisce una serie di pannelli che consentono ad un utente di visualizzare, aggiungere, modificare ed eliminare voci nell'indirizzario di distribuzione del sistema.

Comandi elenchi di convalida

Questi due comandi consentono di creare e cancellare gli elenchi di convalida in una libreria.

Tabella 144. Comandi elenchi di convalida

Nome comando	Nome descrittivo	Funzione
CRTVLDL	Creazione elenco di convalida	Creare un oggetto elenco di convalida che contiene voci costituite da un identificativo, dati che verranno codificati dal sistema in fase di memorizzazione e dati in formato libero.
DLTVLDL	Cancellazione elenco di convalida	Cancellazione dell'elenco di convalida specificato da una libreria.

Comandi informazioni sull'utilizzo della funzione

È possibile utilizzare questi comandi per modificare o visualizzare informazioni sull'utilizzo della funzione.

Tabella 145. Comandi informazioni sull'utilizzo della funzione

Nome comando	Nome descrittivo	Funzione
CHGFCNUSG	Modifica utilizzo funzione	Modificare le informazioni sull'utilizzo di una funzione registrata.
DSPFCNUSG	Visualizzazione utilizzo funzione	Visualizzare un elenco di identificativi funzione e informazioni dettagliate sull'utilizzo per una specifica funzione.

Tabella 145. Comandi informazioni sull'utilizzo della funzione (Continua)

Nome comando	Nome descrittivo	Funzione
WRKFCNUSG	Gestione utilizzo funzione	Visualizzare un elenco di identificativi funzione e modificare o visualizzare informazioni sull'utilizzo della funzione.

Comandi controllo strumenti di sicurezza

Questi comandi consentono di gestire il controllo della sicurezza, le voci dal giornale di controllo sicurezza e i valori di sistema che controllano tale controllo.

Per ulteriori informazioni sugli strumenti della sicurezza, consultare Appendice G, "Comandi e menu per i comandi di sicurezza", a pagina 751.

Tabella 146. Comandi controllo strumenti di sicurezza

Nome comando	Nome descrittivo	Funzione
CHGSECAUD	Modifica controllo sicurezza	Impostare il controllo della sicurezza e modificare i valori di sistema che regolano il controllo della sicurezza.
CPYAUDJRNE	Copia voci giornale di controllo	Copiare voci dal giornale di controllo sicurezza nei file di emissione su cui è possibile eseguire la query. È possibile selezionare tipi di voci specifici, utenti specifici e un periodo di tempo.
DSPAUDJRNE[1]	Visualizzazione voci giornale di controllo	Visualizzare o stampare informazioni sulle voci nel giornale di controllo sicurezza. È possibile selezionare tipi di voci specifici, utenti specifici e un periodo di tempo.
DSPSECAUD	Visualizzazione valori controllo sicurezza	Visualizzare informazioni sul giornale di controllo sicurezza e sui valori di sistema che regolano tale controllo.

1 IBM non fornisce più aggiornamenti per il comando DSPAUDJRNE. Il comando non supporta tutti i tipi di record di controllo sicurezza e non fornisce un elenco di tutti i campi per i record da esso supportati.

Comandi strumenti di sicurezza autorizzazione

È possibile utilizzare questi comandi per eseguire varie attività di stampa correlate alle impostazioni di sicurezza.

Tabella 147. Comandi strumenti di sicurezza autorizzazione

Nome comando	Nome descrittivo	Funzione
PRTJOBDAUT	Stampa autorizzazione descrizione lavoro	Stampare un elenco di descrizioni lavoro la cui autorizzazione pubblica non sia *EXCLUDE. È possibile utilizzare questo comando per stampare informazioni sulle descrizioni lavoro che specificano un profilo utente a cui ogni utente nel sistema può accedere.
PRTPUBAUT	Stampa oggetti autorizzati pubblicamente	Stampare un elenco di oggetti del tipo specificato la cui autorizzazione pubblica non sia *EXCLUDE.
PRTPVTAUT	Stampa autorizzazioni private	Stampare un elenco di autorizzazioni private per oggetti del tipo specificato.

Tabella 147. Comandi strumenti di sicurezza autorizzazione (Continua)

Nome comando	Nome descrittivo	Funzione
PRTQAUT	Stampa autorizzazione coda	Stampare le impostazioni di sicurezza per le code di emissione e le code lavori nel sistema. Tali impostazioni controllano chi può visualizzare e modificare le voci nella coda di emissione o nella coda lavori.
PRTSBSDAUT	Stampa autorizzazione descrizione sottosistema	Stampare un elenco di descrizioni sottosistema in una libreria che contiene un utente predefinito in una voce sottosistema.
PRTTRGPGM	Stampa programmi trigger	Stampare un elenco di programmi trigger associati ai file di database nel sistema.
PRTUSROBJ	Stampa oggetti utente	Stampare un elenco di oggetti utente (oggetti non forniti da IBM) che si trovano in una libreria.

Comandi strumenti sicurezza di sistema

È possibile utilizzare questi comandi per gestire la sicurezza del sistema.

Tabella 148. Comandi strumenti sicurezza di sistema

Nome comando	Nome descrittivo	Funzione
CHGSECA [1]	Modifica attributi sicurezza	Impostare nuovi valori iniziali per la creazione di numeri ID utente o numeri ID gruppo. Gli utenti possono specificare un numero ID utente iniziale ed un numero ID gruppo iniziale.
CFGSYSSEC	Configurazione sicurezza sistema	Impostare i valori di sistema rilevanti per la sicurezza sulle impostazioni consigliate. Il comando imposta inoltre il controllo sicurezza sul sistema.
CLRSVRSEC	Eliminazione dati sicurezza server	Eliminare informazioni di autenticazione decodificabili associate ai profili utente e alle voci elenco convalida (*VLDL). **Nota:** questa sono le stesse informazioni eliminate nei release precedenti a V5R2 quando il valore di sistema QRETSVRSEC è stato modificato da '1' a '0'.
DSPSECA	Visualizzazione attributi sicurezza	Visualizzare i valori correnti e in sospeso di alcuni attributi della sicurezza di sistema.
PRTCMNSEC	Stampa sicurezza comunicazioni	Stampare gli attributi di sicurezza degli oggetti *DEVD, *CTL e *LIND nel sistema.
PRTSYSSECA	Stampa attributi sicurezza di sistema	Stampare un elenco di valori di sistema rilevanti per la sicurezza e di attributi di rete. La documentazione visualizza il valore corrente e il valore consigliato.
RVKPUBAUT	Revoca autorizzazione pubblica	Impostare l'autorizzazione pubblica su *EXCLUDE per una serie di comandi sensibili alla sicurezza sul sistema.

[1] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *SECADM.

Appendice B. Profili utente forniti da IBM

Questa sezione contiene informazioni sui profili utente forniti con il sistema. Questi profili sono utilizzati come proprietari di oggetto per varie funzioni di sistema. Alcune funzioni di sistema vengono anche eseguite tramite specifici profili utente forniti da IBM.

Valori predefiniti per i profili utente

questa tabella indica i valori predefiniti utilizzati per tutti i profili utente forniti da IBM e nel comando CRTUSRPRF (Creazione profilo utente). I parametri sono posti in sequenza nell'ordine in cui appaiono nel pannello Creazione profilo utente.

Tabella 149. Valori predefiniti per i profili utente

	Valori predefiniti	
Parametro profilo utente	**Profili utente forniti da IBM**	**Pannello Creazione profilo utente**
Parola d'ordine (PASSWORD)	*NONE	*USRPRF[4]
Impostazione parola d'ordine come scaduta (PWDEXP)	*NO	*NO
Stato (STATUS)	*ENABLED	*ENABLED
Classe utente (USRCLS)	*USER	*USER
Livello di assistenza (ASTLVL)	*SYSVAL	*SYSVAL
Libreria corrente (CURLIB)	*CRTDFT	*CRTDFT
Programma iniziale (INLPGM)	*NONE	*NONE
Menu iniziale (INLMNU)	PRINCIPALE	PRINCIPALE
Libreria menu iniziale	*LIBL	*LIBL
Possibilità limitate (LMTCPB)	*NO	*NO
Testo (TEXT)	*BLANK	*BLANK
Autorizzazione speciale (SPCAUT)	*ALLOBJ[1] *SAVSYS[1]	*USRCLS[2]
Ambiente specifico (SPCENV)	*SYSVAL	*SYSVAL
Visualizzazione informazioni sull'accesso (DSPSGNINF)	*SYSVAL	*SYSVAL
Intervallo scadenza parola d'ordine (PWDEXPITV)	*SYSVAL	*SYSVAL
Limite sessioni unità (LMTDEVSSN)	*SYSVAL	*SYSVAL
Buffer della tastiera (KBDBUF)	*SYSVAL	*SYSVAL
Memoria massima (MAXSTG)	*NOMAX	*NOMAX
Limite priorità (PTYLMT)	0	3
Descrizione lavoro (JOBD)	QDFTJOBD	QDFTJOBD
Libreria descrizione lavoro	QGPL	*LIBL
Profilo gruppo (GRPPRF)	*NONE	*NONE
Proprietario (OWNER)	*USRPRF	*USRPRF
Autorizzazione gruppo (GRPAUT)	*NONE	*NONE
Tipo autorizzazione gruppo (GRPAUTTYP)	*PRIVATE	*PRIVATE
Gruppi supplementari (SUPGRPPRF)	*NONE	*NONE
Codice account (ACGCDE)	*SYS	*BLANK

Tabella 149. Valori predefiniti per i profili utente (Continua)

Parametro profilo utente	Valori predefiniti	
	Profili utente forniti da IBM	**Pannello Creazione profilo utente**
Parola d'ordine documento (DOCPWD)	*NONE	*NONE
Coda messaggi (MSGQ)	*USRPRF	*USRPRF
Consegna (DLVRY)	*NOTIFY	*NOTIFY
Severità (SEV)	00	00
Unità di stampa (PRTDEV)	*WRKSTN	*WRKSTN
Coda di emissione (OUTQ)	*WRKSTN	*WRKSTN
Programma attenzione (ATNPGM)	*NONE	*SYSVAL
Sequenza di ordinamento (SRTSEQ)	*SYSVAL	*SYSVAL
Identificativo lingua (LANGID)	*SYSVAL	*SYSVAL
Identificativo paese o regione (CNTRYID)	*SYSVAL	*SYSVAL
Coded Character Set Identifier (CCSID)	*SYSVAL	*SYSVAL
Impostazione attributi lavoro (SETJOBATR)	*SYSVAL	*SYSVAL
Locale (LOCALE)	*NONE	*SYSVAL
Opzione utente (USROPT)	*NONE	*NONE
Numeri identificazione utente (UID)	*GEN	*GEN
Numero identificazione gruppo (GID)	*NONE	*NONE
Indirizzario principale (HOMEDIR)	*USRPRF	*USRPRF
Autorizzazione (AUT)	*EXCLUDE	*EXCLUDE
Controllo operazione (AUDLVL) [3]	*NONE	*NONE
Controllo oggetto (OBJAUD) [3]	*NONE	*NONE

[1] Quando il livello di sicurezza del sistema viene modificato dal livello 10 o 20 al livello 30 o superiore, questo valore viene eliminato.

[2] Quando un profilo utente viene creato automaticamente al livello di sicurezza 10, la classe utente *USER fornisce l'autorizzazione speciale *ALLOBJ e *SAVSYS.

[3] Il controllo dell'operazione e dell'oggetto sono specificati utilizzando il comando CHGUSRAUD.

[4] Quando si esegue CRTUSRPRF, non è possibile creare un profilo utente (*USRPRF) in un lotto dischi indipendente. Tuttavia, quando un utente viene autorizzato in forma privata su un oggetto all'interno del lotto dischi indipendente, tale utente è il proprietario di un oggetto su un lotto dischi indipendenti oppure è il gruppo principale di un oggetto in un lotto dischi indipendente, il nome del profilo viene memorizzato sul lotto dischi indipendente. Se il lotto dischi indipendente viene spostato su un altro sistema, l'autorizzazione privata, la proprietà dell'oggetto e le voci del gruppo principali verranno collegate al profilo con lo stesso nome sul sistema di destinazione. Se un profilo non esiste sul sistema di destinazione, verrà creato un profilo. L'utente non disporrà di alcuna autorizzazione speciale e la parola d'ordine verrà impostata su *NONE.

Profili utente forniti da IBM

Questa tabella elenca ogni profilo fornito da IBM, il relativo scopo, e qualsiasi valore per il profilo differente da quelli predefiniti per i profili utente forniti da IBM.

Nota:

I profili utente forniti da IBM ora comprendono profili utente aggiuntivi forniti con i prodotti programmi su licenza. La tabella include solo alcuni, ma non tutti i profili utente per i prodotti programmi su licenza; perciò, l'elenco non è esaustivo.

Attenzione:

- Parola d'ordine per il profilo QSECOFR

  È necessario modificare la parola d'ordine per il profilo QSECOFR dopo l'installazione del sistema. Questa parola d'ordine è uguale per ogni prodotto System i pone un rischio per la sicurezza fino a quando non viene modificata. Tuttavia, non modificare alcun altro valore per i profili utente forniti da IBM. La modifica di questi profili può causare il mancato funzionamento delle funzioni di sistema.
- Autorizzazioni per profili forniti da IBM

  Prestare attenzione quando si eliminano le autorizzazioni che i profili forniti da IBM hanno per gli oggetti inviati con il sistema operativo. Ad alcuni profili forniti da IBM sono concesse autorizzazioni private per oggetti forniti con il sistema operativo. L'eliminazione di una qualsiasi di queste autorizzazioni può causare il mancato funzionamento delle funzioni di sistema.

Tabella 150. Profili utente forniti da IBM

Nome profilo	Nome descrittivo	Parametri differenti dai valori predefiniti
QADSM	Profilo utente ADSM	• USERCLS: *SYSOPR • CURLIB: QADSM • TEXT: profilo ADSM utilizzato dal server ADSM • SPCAUT: *JOBCTL, *SAVSYS • JOBD: QADSM/QADSM • OUTQ: QADSM/QADSM
QAFOWN	Profilo utente APD	• USRCLS: *PGMR • SPCAUT: *JOBCTL • JOBD: QADSM/QADSM • TEXT: Profilo utente APD interno
QAFUSR	Profilo utente APD	• TEXT: Profilo utente APD interno
QAFDFTUSR	Profilo utente APD	• INLPGM: *LIBL/QAFINLPG • LMTCPB: *YES • TEXT: Profilo utente APD interno
QAUTPROF	Profilo utente autorizzazione IBM	
QBRMS	Profilo utente BRM	
QCLUMGT	Profilo gestione cluster	• STATUS: *DISABLED • MSGQ: *NONE • ATNPGM: *NONE
QCLUSTER	Profilo cluster ad alta disponibilità	• SPCAUT: *IOSYSCFG
QCOLSRV	Profilo utente servizi raccolta Management Central	
QDBSHR	Profilo condivisione database	• AUT: *ADD, *DELETE
QDBSHRDO	Profilo condivisione database	• AUT: *ADD, *DELETE

Tabella 150. Profili utente forniti da IBM (Continua)

Nome profilo	Nome descrittivo	Parametri differenti dai valori predefiniti
QDFTOWN	Profilo utente predefinito	• PTYLMT: 3
QDIRSRV	Profilo utente server i5/OS Directory Server	• LMTCPB: *YES • JOBD: QGPL/QBATCH • DSPSGNINF: *NO • LMTDEVSSN: *NO • DLVRY: *HOLD • SPCENV: *NONE • ATNPGM: *NONE
QDLFM	Profilo DataLink File Manager	• SRTSEQ: *HEX
QDOC	Profilo documento	• AUT: *CHANGE
QDSNX	Profilo esecutivo nodo sistemi distribuiti	• PTYLMT: 3 • CCSID: *HEX • SRTSEQ: *HEX
QEJBSVR	Profilo utente WebSphere Application Server	
QEJB	Profilo utente Enterprise Java	
QFNC	Profilo finanza	• PTYLMT: 3
QGATE	Profilo bridge VM/MVS*	• CCSID: *HEX • SRTSEQ: *HEX
QIPP	Profilo stampa Internet	• MSGQ: QUSRSYS/QIPP
QLPAUTO	Profilo installazione automatica programma su licenza	• USRCLS: *SYSOPR • INLMNU: *SIGNOFF • SPCAUT: *ALLOBJ, *JOBCTL ,*SAVSYS, *SECADM, *IOSYSCFG • INLPGM: QSYS/QLPINATO • DLVRY: *HOLD • SEV: 99
QLPINSTALL	Profilo installazione programma su licenza	• USRCLS: *SYSOPR • DLVRY: *HOLD • SPCAUT: *ALLOBJ, *JOBCTL, *SAVSYS, *SECADM, *IOSYSCFG
QMGTC	Profilo Management Central	• JOBD: QSYS/QYPSJOBD
QMSF	Profilo framework server di posta	• CCSID: *HEX • SRTSEQ: *HEX
QMQM	Profilo utente MQSeries	• USRCLS: *SECADM • SPCAUT: *NONE • PRTDEV: *SYSVAL • TEXT: Utente MQM che possiede la libreria QMQM
QNFSANON	Profilo utente NFS	

Tabella 150. Profili utente forniti da IBM (Continua)

Nome profilo	Nome descrittivo	Parametri differenti dai valori predefiniti
QNETSPLF	Profilo utente spool di rete	
QNTP	Profilo ora rete	• JOBD: QTOTNTP • JOBD LIBRARY: QSYS
QOIUSER	Sottosistema di comunicazione OSI	• USRCLS: *SYSOPR • SPCAUT: *JOBCTL, *SAVSYS, *IOSYSCFG • CURLIB: QOSI • MSGQ: QOSI/QOIUSER • DLVRY: *HOLD • OUTQ: *DEV • PRTDEV: *SYSVAL • ATNPGM: *NONE • CCSID: *HEX • TEXT: Profilo utente sottosistema di comunicazione OSI interno
QOSIFS	Profilo utente server file OSI	• USRCLS: *SYSOPR • SPCAUT: *JOBCTL, *SAVSYS • OUTQ: *DEV • CURLIB: *QOSIFS • CCSID: *HEX • TEXT: Profilo utente OSI File Services interno
QPGMR	Profilo programmatore	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1] *SAVSYS *JOBCTL • PTYLMT: 3 • ACGCDE: *BLANK
QPEX	Profilo utente Performance Explorer	• PTYLMT: 3 • ATNPGM: *SYSVAL • TEXT: Profilo utente fornito IBM
QPM400	IBM Performance Management per System i(PM System i)	• SPCAUT: *IOSYSCFG, *JOBCTL
QPRJOWN	Profilo utente proprietario parti e progetti	• STATUS: *DISABLED • CURLIB: QADM • TEXT: Profilo utente del proprietario di parti e progetti
QRDARSADM	Profilo utente R/DARS	• INLMNU: *SIGNOFF • TEXT: Profilo gestione R/DARS
QRDAR	Profilo di proprietà R/DARS	• USRCLS: *PGMR • INLMNU: *SIGNOFF • OUTQ: *DEV • TEXT: Profilo di proprietà R/DARS-400
QRDARS4001	Profilo di proprietà R/DARS 1	• INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Profilo di proprietà R/DARS-400 1

Tabella 150. Profili utente forniti da IBM (Continua)

Nome profilo	Nome descrittivo	Parametri differenti dai valori predefiniti
QRDARS4002	Profilo di proprietà R/DARS 2	• INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Profilo di proprietà R/DARS-400 2
QRDARS4003	Profilo di proprietà R/DARS 3	• INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Profilo di proprietà R/DARS-400 4
QRDARS4004	Profilo di proprietà R/DARS 4	• INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Profilo di proprietà R/DARS-400 4
QRDARS4005	Profilo di proprietà R/DARS 5	• INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Profilo di proprietà R/DARS-400 5
QRMTCAL	Profilo utente calendario remoto	• TEXT: Utente calendario remoto OfficeVision
QRJE	Profilo voce lavoro remoto	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1] *SAVSYS [1] *JOBCTL
QSECOFR	Profilo responsabile della riservatezza	• PWDEXP: *YES • USRCLS: *SECOFR • SPCAUT: *ALLOBJ, *SAVSYS, *JOBCTL, *SECADM, *SPLCTL, *SERVICE, *AUDIT, *IOSYSCFG • UID: 0 • PASSWORD: QSECOFR
QSNADS	Profilo servizi distribuzione SNA	• CCSID: *HEX • SRTSEQ: *HEX
QSOC	Profilo utente OptiConnect	• USRCLS: *SYSOPR • CURLIB: *QSOC • SPCAUT: *JOBCTL • MSGQ: QUSRSYS/QSOC
QSPL	Profilo spool	
QSPLJOB	Profilo lavoro spool	• AUT: *EXCLUDE
QSRV	Profilo servizio	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1], *SAVSYS [1], *JOBCTL, *SERVICE • ASTLVL: *INTERMED • ATNPGM: QSYS/QSCATTN
QSRVAGT	Profile utente Service Agent	

Tabella 150. Profili utente forniti da IBM (Continua)

Nome profilo	Nome descrittivo	Parametri differenti dai valori predefiniti
QSRVBAS	Profilo base servizio	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1] *SAVSYS [1] *JOBCTL • ASTLVL: *INTERMED • ATNPGM: QSYS/QSCATTN
QSVCCS	Profilo utente Server CC	• USRCLS: *SYSOPR • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Profilo utente Server CC
QSVCM	Profilo utente Server di gestione client	• TEXT: Profilo utente Server di gestione client
QSVSM	Profilo utente ECS	• USRCLS: *SYSOPR • STATUS: *DISABLED • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Profilo utente SystemView System Manager
QSVSMSS	Profilo utente Managed System Service	• STATUS: *DISABLED • USRCLS: *SYSOPR • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Profilo utente Managed System Service
QSYS	Profilo di sistema	• USRCLS: *SECOFR • SPCAUT: *ALLOBJ, *SECADM, *SAVSYS, *JOBCTL, *AUDIT, *SPLCTL, *SERVICE, *IOSYSCFG
QSYSOPR	Profilo operatore di sistema	• USRCLS: *SYSOPR • SPCAUT: *ALLOBJ [1], *SAVSYS, *JOBCTL • INLMNU: SYSTEM • LIBRARY: *LIBL • MSGQ: QSYSOPR • DLVRY: *BREAK • SEV: 40
QTCM	Profilo gestore cache sottoposto a trigger	• STATUS: *DISABLED
QTCP	Profilo TCP (Transmission control protocol)	• USRCLS: *SYSOPR • SPCAUT: *JOBCTL • CCSID: *HEX • SRTSEQ: *HEX
QTFTP	Trivial File Transfer Protocol	
QTMPLPD	Profilo supporto di stampa TCP/IP (Transmission control protocol/Internet protocol)	• PTYLMT: 3 • AUT: *USE

Tabella 150. Profili utente forniti da IBM (Continua)

Nome profilo	Nome descrittivo	Parametri differenti dai valori predefiniti
QTMPLPD	Profilo utente LPR remoto	• JOBD: QGPL/QDFTJOBD • PWDEXPITV: *NOMAX • MSGQ: QTCP/QTMPLPD
QTMTWSG	Profilo utente HTML Workstation Gateway Profile	• MSGQ: QUSRSYS/QTMTWSG • TEXT: HTML Workstation Gateway Profile
QTMHHTTP	Profilo utente HTML Workstation Gateway Profile	• MSGQ: QUSRSYS/QTMHHTTP • TEXT: Profilo utente server HTTP
QTMHHTP1	Profilo utente HTML Workstation Gateway Profile	• MSGQ: QUSRSYS/QTMHHTTP • TEXT: Profilo CGI server HTTP
QTSTRQS	Profilo richiesta di verifica	
QUMB	Profilo utente Ultimedia System Facilities	
QUMVUSER	Profilo utente Ultimedia Business Conferencing	
QUSER	Profilo utente stazione di lavoro	• PTYLMT: 3
QX400	Profilo utente OSI Messages Services File Services	• CURLIB: *QX400 • USRCLS: *SYSOPR • MSGQ: QX400/QX400 • DLVRY: *HOLD • OUTQ: *DEV • PRTDEV: *SYSVAL • ATNPGM: *NONE • CCSID: *HEX • TEXT: Profilo utente OSI Messages Services interno
QYCMCIMOM	Profilo utente server	
QYPSJSVR	Profilo Management Central Java Server	
QYPUOWN	Profilo utente APU interno	• TEXT: APU interno — Profilo utente

[1] Quando il livello di sicurezza del sistema viene modificato dal livello 10 o 20 al livello 30 o superiore, questo valore viene eliminato.

Appendice C. Comandi forniti con autorizzazione pubblica *EXCLUDE

Questa sezione indica quali comandi hanno un'autorizzazione limitata (l'autorizzazione pubblica è *EXCLUDE) quando viene fornito il sistema. Mostra quali profili utente forniti da IBM sono autorizzati ad utilizzare questi comandi limitati.

Per ulteriori informazioni sui profili utente forniti da IBM, consultare l'argomento "profili utente forniti da IBM" a pagina 137.

Nella Tabella 151, i comandi che sono limitati al responsabile della riservatezza e a qualsiasi profilo utente con autorizzazione *ALLOBJ, contengono una **R** nel profilo QSECOFR. I comandi autorizzati in modo specifico per uno o più profili utente forniti da IBM, oltre al responsabile della riservatezza, hanno una **S** sotto i nomi profilo per cui sono autorizzati.

Qualunque comando che non sia elencato in questa tabella è pubblico, il che significa che può essere utilizzato da tutti gli utenti. Tuttavia, alcuni comandi richiedono un'autorizzazione speciale, come ad esempio *SERVICE o *JOBCTL. Le autorizzazioni speciali richieste per un comando sono elencate nell'Appendice D, "Autorizzazione richiesta per gli oggetti utilizzati dai comandi", a pagina 361.

Se si sceglie di concedere ad altri utenti o a tutti l'autorizzazione *USE per questi comandi, aggiornare questa tabella in modo che indichi che i comandi non sono più limitati nel sistema. L'utilizzo di alcuni comandi può richiedere l'autorizzazione per certi oggetti nel sistema ed anche per i comandi stessi. Consultare Appendice D, "Autorizzazione richiesta per gli oggetti utilizzati dai comandi", a pagina 361 per le autorizzazioni oggetto richieste per i comandi.

Tabella 151. Autorizzazioni di profili utente forniti da IBM per comandi limitati

Nome comando	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ADDCLUNODE	R				
ADDCMDCRQA		S	S	S	S
ADDCRGDEVE	R				
ADDCRGNODE	R				
ADDCRSDMNK	R				
ADDDEVDMNE	R				
ADDDSTQ		S	S		
ADDDSTRTE		S	S		
ADDDSTSYSN		S	S		
ADDEXITPGM	R				
ADDDWDFN					
ADDJWDFN					
ADDMFS	R				
ADDMSTPART					
ADDNETJOBE	R				
ADDOBJCRQA		S	S	S	S
ADDOPTCTG	R				
ADDOPTSVR	R				

Tabella 151. Autorizzazioni di profili utente forniti da IBM per comandi limitati (Continua)

Nome comando	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ADDPEXDFN		S		S	
ADDPEXFTR		S		S	
ADDPRDCRQA		S	S	S	S
ADDPTFCRQA		S	S	S	S
ADDRPYLE		S			
ADDRSCCRQA		S	S	S	S
ADDTRCFTR	R				
ANSQST	R				
ANZBESTMDL	R				
ANZCMDPFR	R				
ANZDBF	R				
ANZDBFKEY	R				
ANZDFTPWD	R				
ANZJVM		S	S	S	S
ANZOBJCVN	R				
ANZPFRDTA	R				
ANZPGM	R				
ANZPRB		S	S	S	S
ANZPRFACT	R				
ANZS34OCL	R				
ANZS36OCL	R				
APYJRNCHG		S		S	
APYPTF				S	
APYRMTPTF		S	S	S	S
CFGDSTSRV		S	S		
CFGRPDS		S	S		
CFGSYSSEC	R				
CHGACTSCDE	R				
CHGASPA	R				
CHGASPACT					
CHGCLUCFG	R				
CHGCLUNODE	R				
CHGCLURCY	R				
CHGCLUVER	R				
CHGCMDCRQA		S	S	S	S
CHGCRG	R				
CHGCRGDEVE	R				
CHGCRGPRI	R				
CHGCRSDMNK	R				
CHGDIRSRVA					

Tabella 151. Autorizzazioni di profili utente forniti da IBM per comandi limitati (Continua)

Nome comando	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CHGDSTQ		S	S		
CHGDSTRTE		S	S		
CHGEXPSCDE	R				
CHGFCNARA	R				
CHGGPHFMT	R				
CHGGPHPKG	R				
CHGJOBTRC	R				
CHGJOBTYP	R				
CHGJRN		S	S	S	
CHGJRNA		S	S		
CHGLICINF	R				
CHGMGDSYSA		S	S	S	S
CHGMGRSRVA		S	S	S	S
CHGMSTK	R				
CHGNETA	R				
CHGNETJOBE	R				
CHGNFSEXP	R				
CHGNWSA	R				
CHGNWSCFG	R				
CHGOBJCRQA		S	S	S	S
CHGOPTA	R				
CHGPEXDFN		S		S	
CHGPRB		S	S	S	S
CHGPRDCRQA		S	S	S	S
CHGPTFCRQA		S	S	S	S
CHGPTR				S	
CHGQSTDB	R				
CHGRCYAP		S	S		
CHGRPYLE		S			
CHGRSCCRQA		S	S	S	S
CHGSYSLIBL	R				
CHGSYSVAL		S	S	S	
CHGS34LIBM	R				
CHKASPBAL	R				
CHKCMNTRC				S	
CHKMSTKVV					
CHKPRDOPT		S	S	S	S
CLRMSTKEY					
CPHDTA	R				
CPYFCNARA	R				

Tabella 151. Autorizzazioni di profili utente forniti da IBM per comandi limitati (Continua)

Nome comando	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CPYFRMLDIF					
CPYGPHFMT	R				
CPYGPHPKG	R				
CPYPFRCOL	R				
CPYPFRDTA	R				
CPYPTF		S	S	S	S
CPYPTFGRP		S	S	S	S
CPYTOLDIF					
CRTADMDMN	R				
CRTAUTHLR	R				
CRTBESTMDL	R				
CRTCLS	R				
CRTCLU	R				
CRTCRG	R				
CRTFCNARA	R				
CRTGPHFMT	R				
CRTGPHPKG	R				
CRTHSTDTA	R				
CRTJOBD	R				
CRTNWSCFG	R				
CRTPFRDTA	R				
CRTPFRSUM					
CRTLASREP		S			
CRTPEXDTA		S		S	
CRTQSTDB	R				
CRTQSTLOD	R				
CRTSBSD		S	S		
CRTUDFS	R				
CRTUDFS	R				
CRTVLDL	R				
CVTBASSTR	R				
CVTBASUNF	R				
CVTBGUDTA	R				
CVTDIR	R				
CVTPFRCOL	R				
CVTPFRDTA	R				
CVTPFRTHD	R				
CVTS36FCT	R				
CVTS36JOB	R				
CVTS38JOB	R				

Tabella 151. Autorizzazioni di profili utente forniti da IBM per comandi limitati (Continua)

Nome comando	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CVTTCPCL		S	S	S	S
DB2LDIF					
DLTADMDMN	R				
DLTAPARDTA		S	S	S	S
DLTBESTMDL	R				
DLTCLU	R				
DLTCMNTRC				S	
DLTCRGCLU	R				
DLTEXPSPLF	R				
DLTFCNARA	R				
DLTGPHFMT	R				
DLTGPHPKG	R				
DLTHSTDTA	R				
DLTLICPGM	R				
DLTNWSCFG	R				
DLTPEXDTA		S		S	
DLTPFRCOL	R				
DLTPFRDTA	R				
DLTPRB		S	S	S	S
DLTPTF		S	S	S	S
DLTQST	R				
DLTQSTDB	R				
DLTRMTPTF		S	S	S	S
DLTSMGOBJ		S	S	S	S
DLTUDFS	R				
DLTVLDL	R				
DLTWNTSVR	R				
DMPDLO		S	S	S	S
DMPJOB		S	S	S	S
DMPJOBINT		S	S	S	S
DMPJVM		S	S	S	S
DMPMEMINF					
DMPOBJ				S	S
DMPSYSOBJ		S	S	S	S
DMPTRC	R	S		S	
DMPUSRPRF					
DSPDSTLOG	R				
DSPHSTGPH	R				
DSPMGDSYSA		S	S	S	S
DSPNWSCFG	R				

Tabella 151. Autorizzazioni di profili utente forniti da IBM per comandi limitati (Continua)

Nome comando	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
DSPPFRDTA	R				
DSPPFRGPH	R				
DSPPTF		S	S	S	S
DSPSRVSTS		S	S	S	S
EDTCPCST			S		
EDTQST	R				
EDTRBDAP			S		
EDTRCYAP		S	S		
ENCCPHK	R				
ENCFRMMSTK	R				
ENCTOMSTK	R				
ENDASPBAL	R				
ENDCHTSVR	R				
ENDCLUNOD	R				
ENDCMNTRC	R			S	
ENDCRG	R				
ENDDBGSVR		S	S	S	S
ENDDW					
ENDHOSTSVR		S	S	S	S
ENDIDXMON	R				
ENDIPSIFC		S	S	S	S
ENDJOBABN		S	S	S	
ENDJOBTRC	R				
ENDJW					
ENDMGDSYS		S	S	S	S
ENDMGRSRV		S	S	S	S
ENDMSF			S	S	S
ENDNFSSVR	R		S	S	S
ENDPEX		S		S	
ENDPFRTRC	R			S	
ENDSRVJOB		S	S	S	S
ENDSYSMGR		S	S	S	S
ENDTCP		S	S	S	S
ENDTCPCNN		S	S	S	S
ENDTCPIFC		S	S	S	S
ENDTCPSVR		S	S	S	S
ENDWCH	R				
GENCPHK	R				
GENCRSDMNK	R				
GENMAC	R				

Tabella 151. Autorizzazioni di profili utente forniti da IBM per comandi limitati (Continua)

Nome comando	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
GENPIN	R				
GENS36RPT	R				
GENS38RPT	R				
GRTACCAUT	R				
HLDCMNDEV		S	S	S	S
HLDDSTQ		S	S		
INSPTF[2]				S	
INSRMTPRD		S	S	S	S
INSWNTSVR	R				
INZDSTQ		S	S		
INZNWSCFG	R				
INZSYS	R				
LDIF2DB					
LODOPTFMW	R				
LODPTF				S	
LODQSTDB	R				
MGRS36	R				
MGRS36APF	R				
MGRS36CBL	R				
MGRS36DFU	R				
MGRS36DSPF	R				
MGRS36ITM	R				
MGRS36LIB	R				
MGRS36MNU	R				
MGRS36MSGF	R				
MGRS36QRY	R				
MGRS36RPG	R				
MGRS36SEC	R				
MGRS38OBJ	R				
MIGRATE	R				
PKGPRDDST		S	S	S	S
PRTACTRPT	R				
PRTCMNTRC				S	
PRTCPTRPT	R				
PRTJOBRPT	R				
PRTJOBTRC	R				
PRTLCKRPT	R				
PRTPOLRPT	R				
PRTRSCRPT	R				
PRTSYSRPT	R				

Tabella 151. Autorizzazioni di profili utente forniti da IBM per comandi limitati (Continua)

Nome comando	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
PRTTNSRPT	R				
PRTTRCRPT	R				
PRTDSKINF	R				
PRTERRLOG		S	S	S	S
PRTINTDTA		S	S	S	S
PRTPRFINT	R				
PWRDWNSYS	R		S		
RCLDBXREF	R				
RCLOBJOWN	R				
RCLOPT	R				
RCLSPLSTG		S	S	S	S
RCLSTG		S	S	S	S
RCLTMPSTG		S	S	S	S
RESMGRNAM	R	S	S	S	S
RLSCMNDEV		S	S	S	S
RLSDSTQ		S	S		
RLSIFSLCK	R				
RLSRMTPHS		S	S		
RMVACC	R				
RMVCLUNODE	R				
RMVCRGDEVE	R				
RMVCRGNODE	R				
RMVCRSDMNK	R				
RMVDEVDMNE	R				
RMVDFRID	R				
RMVDSTQ		S	S		
RMVDSTRTE		S	S		
RMVDSTSYSN		S	S		
RMVDWDFN					
RMVEXITPGM	R				
RMVJRNCHG		S		S	
RMVJWDFN					
RMVLANADP	R				
RMVMFS	R				
RMVNETJOBE	R				
RMVOPTCTG	R				
RMVOPTSVR	R				
RMVPEXDFN		S		S	
RMVPEXFTR		S		S	
RMVPTF				S	

Tabella 151. Autorizzazioni di profili utente forniti da IBM per comandi limitati (Continua)

Nome comando	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
RMVRMTPTF		S	S	S	S
RMVRPYLE		S			
RMVTRCFTR	R				
RSTAUT	R				
RST[3]					
RSTCFG	R				
RSTDFROBJ	R				
RSTDLO	R				
RSTLIB	R				
RSTLICPGM	R				
RSTOBJ[3]					
RSTPFRCOL	R				
RSTPFRDTA					
RSTS36F	R				
RSTS36FLR	R				
RSTS36LIBM	R				
RSTS38AUT	R				
RSTUSFCNR[4]					
RSTUSRPRF	R				
RTVDSKINF	R				
RTVPRD		S	S	S	S
RTVPTF		S	S	S	S
RTVSMGOBJ		S	S	S	S
RUNLPDA		S	S	S	S
RUNSMGCMD		S	S	S	S
RUNSMGOBJ		S	S	S	S
RVKPUBAUT	R				
SAVAPARDTA		S	S	S	S
SAVLICPGM	R				
SAVPFRCOL	R				
SAVPFRDTA					
SAVRSTCHG	R				
SAVRSTLIB	R				
SAVRSTOBJ	R				
SBMFNCJOB	R				
SBMNWSCMD	R				
SETMSTK	R				
SETMSTKEY					
SNDDSTQ		S	S		
SNDPRD		S	S	S	S

Tabella 151. Autorizzazioni di profili utente forniti da IBM per comandi limitati (Continua)

Nome comando	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
SNDPTF		S	S	S	S
SNDPTFORD				S	S
SNDSMGOBJ		S	S	S	S
SNDSRVRQS				S	S
STRASPBAL	R				
STRBEST	R				
STRCHTSVR	R				
STRCLUNOD	R				
STRCMNTRC				S	
STRCRG	R				
STRDBG		S		S	S
STRDBGSVR		S	S	S	S
STRDW					
STRHOSTSVR		S	S	S	S
STRIDXMON	R				
STRIPSIFC		S	S	S	S
STRJW	R				
STRJOBTRC					
STRMGDSYS		S	S	S	S
STRMGRSRV		S	S	S	S
STRMSF[1]			S	S	S
STRNFSSVR	R				
STROBJCVN	R				
STRPEX		S		S	
STRPFRG	R				
STRPFRT	R				
STRPFRTRC	R			S	
STRRGZIDX	R				
STRSPLRCL	R				
STRSRVJOB		S	S	S	S
STRSST				S	
STRSYSMGR		S	S	S	S
STRS36MGR	R				
STRS38MGR	R				
STRTCP		S	S	S	S
STRTCPIFC		S	S	S	S
STRTCPSVR		S	S	S	S
STRUPDIDX	R				
STRWCH	R				

Tabella 151. Autorizzazioni di profili utente forniti da IBM per comandi limitati (Continua)

Nome comando	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
TRCASPBAL	R				
TRCCPIC	R				
TRCICF	R				
TRCINT		S		S	
TRCJOB		S	S	S	S
TRCTCPAPP				S	S
TRNPIN	R				
UPDPTFINF	R				
VFYCMN		S	S	S	S
VFYLNKLPDA		S	S	S	S
VFYMSTK	R				
VFYPIN	R				
VFYPRT		S	S	S	S
VFYTAP		S	S	S	S
WRKCNTINF				S	S
WRKDEVTBL	R				
WRKDPCQ		S	S		
WRKDSTQ		S	S		
WRKFCNARA	R				
WRKJRN		S	S	S	
WRKLIB					
WRKLIBPDM					
WRKLICINF	R				
WRKNWSCFG	R				
WRKORDINF			S	S	
WRKPEXDFN		S		S	
WRKPEXFTR		S		S	
WRKPGMTBL	R				
WRKPRB		S	S	S	S
WRKPTFGRP		S	S	S	S
WRKPTFORD	R			S	S
WRKSRVPVD				S	S
WRKSYSACT	R				
WRKTRC	R				
WRKTXTIDX	R				
WRKUSRTBL	R				
WRKWCH	R				

Tabella 151. Autorizzazioni di profili utente forniti da IBM per comandi limitati (Continua)

Nome comando	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
[1] Anche il profilo utente QMSF è autorizzato a questo comando.					
[2] QSRV può eseguire questo comando se non viene effettuato un IPL.					
[3] In aggiunta a QSYS, anche il profilo utente QRDARS400 dispone dell'autorizzazione.					
[4] In aggiunta a QSYS, anche il profilo utente QUMB dispone dell'autorizzazione.					

Appendice D. Autorizzazione richiesta per gli oggetti utilizzati dai comandi

Le tabelle in questa sezione mostrano quali autorizzazioni sono necessarie per gli oggetti a cui fanno riferimento i comandi.

Ad esempio, nella voce relativa al comando CHGUSRPR (Modifica profilo utente) la tabella elenca tutti gli oggetti per cui è necessaria l'autorizzazione, quali la coda messaggi dell'utente, la descrizione lavoro e il programma iniziale.

Le tabelle sono organizzate in ordine alfabetico in base al tipo di oggetto. Inoltre, sono incluse tabelle per le voci che non sono oggetti i5/OS (lavori, file di spool, attributi di rete e valori di sistema) e per alcune funzioni (finanza ed emulazione unità). È possibile trovare ulteriori considerazioni (se presenti) per i comandi nelle note a piè di pagina della tabella.

Le sezioni che seguono sono descrizioni delle colonne nelle tabelle.

Oggetto di riferimento

Gli oggetti elencati nella colonna *Oggetto di riferimento* sono oggetti per i quali l'utente ha bisogno dell'autorizzazione quando utilizza il comando.

Autorizzazione richiesta per l'oggetto

Le autorizzazioni specificate nelle tabelle indicano le autorizzazioni per l'oggetto e le autorizzazioni per i dati richieste per l'oggetto quando si utilizza il comando.

Autorizzazione richiesta per la libreria

Questa colonna indica quale autorizzazione è necessaria per la libreria che contiene l'oggetto.

Per molte operazioni, è necessaria l'autorizzazione *EXECUTE per individuare l'oggetto nella libreria. L'aggiunta di un oggetto ad una libreria richiede l'autorizzazione *READ e *ADD.

Tipo oggetto

Il valore fa riferimento al tipo di oggetto specificato nella colonna Oggetto di riferimento.

File system

Il valore fa riferimento al tipo di file system a cui appartiene l'oggetto di riferimento.

Per l'IFS (integrated file system) nel sistema operativo i5/OS, fare riferimento a Integrated file system.

La seguente tabella descrive le autorizzazioni specificate nella colonna *Autorizzazione necessaria*. La descrizione include esempi su come viene utilizzata l'autorizzazione. Nella maggior parte dei casi, per accedere a un oggetto è necessaria una combinazione di autorizzazioni oggetto e dati.

Tabella 152. Descrizione dei tipi di autorizzazione

speciale	Nome	Funzioni consentite
Autorizzazioni oggetto:		

Tabella 152. Descrizione dei tipi di autorizzazione (Continua)

speciale	Nome	Funzioni consentite
*OBJOPR	Operativo oggetto	Controllare la descrizione di un oggetto. Utilizzare l'oggetto come stabilito dalle autorizzazioni dati dell'utente.
*OBJMGT	Gestione oggetto	Specificare la sicurezza per l'oggetto. Spostare o rinominare l'oggetto. Tutte le funzioni definite per *OBJALTER e *OBJREF.
*OBJEXIST	Esistenza oggetto	Cancellare l'oggetto. Liberare la memoria dell'oggetto. Eseguire le operazioni di salvataggio e ripristino per l'oggetto [1]. Trasferire la proprietà dell'oggetto.
*OBJALTER	Modifica oggetto	Aggiungere, eliminare, inizializzare e riorganizzare i membri dei file di database. Modificare e aggiungere gli attributi dei file di database: aggiungere e rimuovere i trigger. Modificare gli attributi dei pacchetti SQL. Spostare una libreria o una cartella su un ASP differente.
*OBJREF	Riferimento oggetto	Specificare un file di database come principale in un limite di riferimento. Ad esempio, si presupponga di voler definire una regola secondo la quale un record del cliente deve esistere nel file CUSMAS prima che un ordine per il cliente possa essere aggiunto al file CUSORD. È necessaria l'autorizzazione *OBJREF al file CUSMAS per poter definire questa regola.
*AUTLMGT	Gestione elenco autoriz.	Aggiungere e rimuovere gli utenti e le relative autorizzazioni dall'elenco di autorizzazioni.
Autorizzazioni dati:		
*READ	Lettura	Visualizzare il contenuto dell'oggetto, come ad esempio la visualizzazione dei record in un file.
*ADD	Aggiunta	Aggiungere le voci ad un oggetto, come ad esempio l'aggiunta dei messaggi ad una coda messaggi o l'aggiunta dei record ad un file.
*UPD	Aggiornam.	Modificare le voci in un oggetto, come ad esempio la modifica dei record in un file.
*DLT	Cancellazione	Rimuovere le voci da un oggetto, come ad esempio la rimozione dei messaggi da una coda messaggi o la cancellazione dei record da un file.
*EXECUTE	Esecuz.	Eseguire un programma, programma di manutenzione o pacchetto SQL. Individuare un oggetto in una libreria o in un indirizzario.

[1] Se un utente dispone dell'autorizzazione speciale al sistema di salvataggio (*SAVSYS), non è necessaria l'autorizzazione all'esistenza dell'oggetto per l'esecuzione delle operazioni di salvataggio e ripristino sull'oggetto.

In aggiunta a questi valori, le colonne *Autorizzazione necessaria* della tabella potrebbero mostrare sottoserie definite dal sistema di tali autorizzazioni. La seguente tabella riporta le sottoserie di autorizzazioni oggetto e di autorizzazioni dati.

Tabella 153. Autorizzaz. definita dal sistema

speciale	*ALL	*CHANGE	*USE	*EXCLUDE
Autorizzazioni oggetto				
*OBJOPR	X	X	X	

Tabella 153. Autorizzaz. definita dal sistema (Continua)

speciale	*ALL	*CHANGE	*USE	*EXCLUDE
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
Autorizzazioni dati				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X		
*DLT	X	X		
*EXECUTE	X	X	X	

La seguente tabella riporta le sottoserie di autorizzazioni supplementari supportate dai comandi CHGAUT e WRKAUT.

Tabella 154. Autorizzaz. definita dal sistema

speciale	*RWX	*RW	*RX	*R	*WX	*W	*X
Autorizzazioni oggetto							
*OBJOPR	X	X	X	X	X	X	X
*OBJMGT							
*OBJEXIST							
*OBJALTER							
*OBJREF							
Autorizzazioni dati							
*READ	X	X	X	X			
*ADD	X	X			X	X	
*UPD	X	X			X	X	
*DLT	X	X			X	X	
*EXECUTE	X		X		X		X

Presupposti per l'utilizzo del comando

Vi sono alcuni presupposti predefiniti che è necessario prendere in considerazione prima di utilizzare qualsiasi comando.

1. L'autorizzazione *USE è richiesta per utilizzare qualsiasi commando. Questa autorizzazione non è elencata in maniera specifica nelle tabelle.
2. Per immettere qualsiasi comando di visualizzazione, è necessario disporre di un'autorizzazione operativa al file di visualizzazione fornito da IBM, al file di emissione di stampa o al gruppo pannelli utilizzato dal comando. Questi gruppi di file e di pannelli vengono inviati con l'autorizzazione pubblica *USE.

Regole generali per le autorizzazioni oggetto sui comandi

Questa tabella mostra le regole generali per le autorizzazioni oggetto sui comandi.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
Modifica (CHG) con F4 (Richiesta)[7]	Valori correnti	I valori correnti vengono visualizzati se l'utente dispone dell'autorizzazione per tali valori.	*EXECUTE
Comando con cui è possibile accedere all'oggetto nell'indirizzario	Indirizzari nel prefisso percorso	*X	
	Indirizzario quando viene specificato il modello (* o ?)	*R	
Creazione oggetto nell'indirizzario	Indirizzari nel prefisso percorso	*X	
	Indirizzario che contiene il nuovo oggetto	*WX	
Copia (CPY) dove A file è un file di database	Oggetto da copiare	*OBJOPR, *READ	*EXECUTE
	Comando CRTPF, se viene specificato CRTFILE (*YES)	*OBJOPR	*EXECUTE
	A file, se viene specificato CRTFILE (*YES) [1]		*ADD, *EXECUTE
	A file, se è presente e viene aggiunto un nuovo membro	*OBJOPR, *OBJMGT, *ADD, *DLT	*ADD, *EXECUTE
	A file, se il file e il membro sono presenti ed è stata specificata l'opzione *ADD	*OBJOPR, *ADD	*EXECUTE
	A file, se il file e il membro sono presenti ed è stata specificata l'opzione *REPLACE	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	A file, se presente, un nuovo membro viene aggiunto ed è stata specificata l'opzione *UPDADD.[8]	*OBJOPR, *OBJMGT, *ADD, *UPD	*EXECUTE
	A file, se il file e il membro sono presenti ed è stata specificata l'opzione *UPDADD. [8]	*OBJOPR, *ADD, *UPD	*EXECUTE
Creazione (CRT)	Oggetto che deve essere creato [2]		*READ, *ADD
	Il profilo utente che sarà il proprietario dell'oggetto creato (sia il profilo utente che esegue il lavoro che il profilo di gruppo dell'utente)	*ADD	
Creazione (CRT) se è specificato REPLACE(*YES) [6, 9]	Oggetto che deve essere creato (e sostituito) [2]	*OBJMGT, *OBJEXIST, *READ[5]	*READ, *ADD
	Il profilo utente che sarà proprietario dell'oggetto creato (il profilo utente che esegue il lavoro o il profilo di gruppo dell'utente)	*ADD	

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
Visualizzazione (DSP) o altre operazioni utilizzando il file di emissione (OUTPUT(*OUTFILE))	Oggetto che deve essere visualizzato	*USE	*EXECUTE
	File di emissione, se il file non è presente [3]		*ADD, *EXECUTE
	File di emissione, se il file esiste e viene aggiunto un nuovo membro e se è specificata l'opzione *REPLACE e il membro non esisteva in precedenza	*OBJOPR, *OBJMGT o *OBJALTER, *ADD, *DLT	*ADD, *EXECUTE
	File di emissione, se il file esiste e viene aggiunto un nuovo membro e se è specificata l'opzione *ADD e il membro non esisteva in precedenza	OBJOPR, *OBJMGT o *OBJALTER, *ADD	*ADD, *EXECUTE
	File di emissione, se il file e il membro sono presenti ed è specificata l'opzione *ADD	*OBJOPR, *ADD	*EXECUTE
	File di emissione, se il file e il membro sono presenti ed è specificata l'opzione *REPLACE	*OBJOPR, *OBJMGT o *OBJALTER, *ADD, *DLT	*EXECUTE
	File formato (QA*xxxxx*), se il file di emissione non esiste	*OBJOPR	
Visualizzazione (DSP) utilizzando *PRINT o Gestione (WRK) utilizzando *PRINT	Oggetto che deve essere visualizzato	*USE	*EXECUTE
	Coda di emissione [4]	*READ	*EXECUTE
	File di stampa (QP*xxxxx* in QSYS)	*USE	*EXECUTE
Salvataggio (SAV) o un'altra operazione utilizzando la descrizione unità	Descrizione unità	*USE	*EXECUTE
	File unità associato alla descrizione unità, quale QSYSTAP per la descrizione unità TAP01	*USE	*EXECUTE

[1] Il profilo utente che esegue il comando di copia diventa il proprietario del file di destinazione, a meno che l'utente non sia un membro di un profilo di gruppo e disponga dell'autorizzazione OWNER(*GRPPRF). Se il profilo dell'utente specifica OWNER(*GRPPRF), il profilo di gruppo diventa il proprietario del file di destinazione. In tal caso, l'utente che esegue il comando deve disporre dell'autorizzazione *ADD per il profilo di gruppo e deve disporre dell'autorizzazione per aggiungere un membro e scrivere i dati su un nuovo file. Al file di destinazione viene assegnata la stessa autorizzazione pubblica, l'autorizzazione gruppo principale, le autorizzazioni private e l'elenco di autorizzazioni del file di provenienza.

[2] Il profilo utente che esegue il comando di creazione diventa il proprietario dell'oggetto appena creato, a meno che l'utente non sia un membro di un profilo di gruppo e disponga dell'autorizzazione OWNER(*GRPPRF). Se il profilo dell'utente specifica OWNER(*GRPPRF), il profilo di gruppo diventa il proprietario dell'oggetto appena creato. L'autorizzazione pubblica per l'oggetto viene controllata dal parametro AUT.

[3] Il profilo utente che esegue il comando di visualizzazione diventa il proprietario del file di emissione appena creato, a meno che l'utente non sia un membro di un profilo di gruppo e disponga dell'autorizzazione OWNER(*GRPPRF). Se il profilo dell'utente specifica OWNER(*GRPPRF), il profilo di gruppo diventa il proprietario del file di emissione. L'autorizzazione pubblica per il file di emissione viene controllata dal parametro CRTAUT della libreria del file di emissione.

[4] Se la coda di emissione viene definita come OPRCTL (*YES), un utente con l'autorizzazione speciale *JOBCTL non necessita di ulteriori autorizzazioni per la coda di emissione. Un utente con autorizzazione speciale *SPLCTL non necessita di ulteriori autorizzazioni per la coda di emissione.

[5] Per i file di unità, è inoltre richiesta l'autorizzazione *OBJOPR.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
[6] Il parametro REPLACE non è disponibile nell'ambiente S/38. REPLACE(*YES) equivale all'utilizzo del tasto di funzione dal menu del programmatore per cancellare l'oggetto corrente.			
[7] È inoltre necessaria l'autorizzazione per il comando (DSP) corrispondente.			
[8] L'opzione *UPDADD è disponibile solo sul parametro MBROPT del comando CPYF.			
[9] Ciò non è valido per il parametro REPLACE sul comando CRTJVAPGM.			

Comandi comuni per la maggior parte degli oggetti

Questa tabella elenca i comandi che possono operare sulla maggior parte degli oggetti in ordine alfabetico.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Tabella 155. Comandi comuni per la maggior parte degli oggetti

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ALCOBJ [1,2,11]	Oggetto	*OBJOPR	*EXECUTE
ANZOBJCVN (Q) [20]			
ANZUSROBJ [20]			
CHGOBJAUD [18]	Unità ASP (se specificata)	*USE	
CHGOBJD [3]	Oggetto, se è un file	*OBJOPR, *OBJMGT	*EXECUTE
	Oggetto, se non è un file	*OBJMGT	*EXECUTE
CHGOBJOWN [3,4]	Oggetto	*OBJEXIST	*EXECUTE
	Oggetto (se è una descrizione file, libreria, sottosistema)	*OBJOPR, *OBJEXIST	*EXECUTE
	Oggetto (se *AUTL)	Proprietario o *ALLOBJ	*EXECUTE
	Profilo utente vecchio	*DLT	*EXECUTE
	Nuovo profilo utente	*ADD	*EXECUTE
	Unità ASP (se specificata)	*USE	
CHGOBJPGP [3]	Oggetto	*OBJEXIST	*EXECUTE
	Oggetto (se è una descrizione file, libreria, sottosistema)	*OBJOPR, *OBJEXIST	*EXECUTE
	Oggetto (se *AUTL)	Proprietario e *OBJEXIST o *ALLOBJ	*EXECUTE
	Profilo utente vecchio	*DLT	
	Nuovo profilo utente	*ADD	
	Unità ASP (se specificata)	*USE	

Tabella 155. Comandi comuni per la maggior parte degli oggetti (Continua)

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHKOBJ [3]	Oggetto	Autorizzazione specificata dal parametro AUT [14]	*EXECUTE
CPROBJ	Oggetto	*OBJMGT	*EXECUTE
CHKOBJITG [11](Q)			
CRTDUPOBJ [3,9,11,21]	Nuovo oggetto		*USE, *ADD
	Oggetto copiato, se è *AUTL	*AUTLMGT	*USE, *ADD
	Oggetto copiato, tutti gli altri tipi	*OBJMGT, *USE	*USE
	Comando CRTSAVF (se l'oggetto è un file di salvataggio)	*OBJOPR	
	Unità ASP (se specificata)	*USE	
DCPOBJ	Oggetto	*USE	*EXECUTE
DLCOBJ [1,11]	Oggetto	*OBJOPR	*EXECUTE
DMPOBJ (Q) [3]	Oggetto	*OBJOPR, *READ	*EXECUTE
DMPSYSOBJ (Q)	Oggetto	*OBJOPR, *READ	*EXECUTE
DSPOBJAUT [3]	Oggetto (per visualizzare tutte le informazioni sull'autorizzazione)	Proprietà o autorizzazione speciale *OBJMGT o *ALLOBJ	*EXECUTE
	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	Unità ASP (se specificata)	*USE	
DSPOBJD [2, 28]	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	Autorizzazione	Autorizzazione diversa da *EXCLUDE	*EXECUTE
	Unità ASP (se specificata)	*EXECUTE	
EDTOBJAUT [3,5,6,15]	Oggetto	*OBJMGT	*EXECUTE
	Oggetto (se è un file)	*OBJOPR, *OBJMGT	*EXECUTE
	*AUTL, se utilizzato per proteggere un oggetto	Non *EXCLUDE	
	Unità ASP (se specificata)	*USE	
GRTOBJAUT [3,5,6,15]	Oggetto	*OBJMGT	*EXECUTE
	Oggetto (se è un file)	*OBJOPR, *OBJMGT	*EXECUTE
	*AUTL, se utilizzato per proteggere un oggetto	Non *EXCLUDE	
	Unità ASP (se specificata)	*USE	
	Unità ASP di riferimento (se specificata)	*EXECUTE	
	Oggetto di riferimento	*OBJMGT o proprietà	*EXECUTE

Tabella 155. Comandi comuni per la maggior parte degli oggetti (Continua)

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
MOVOBJ [3,7,12]	Oggetto	*OBJMGT	
	Oggetto (se è *FILE)	*ADD, *DLT, *EXECUTE	
	Oggetto (non *FILE),	*DLT, *EXECUTE	
	Libreria di partenza		*CHANGE
	Libreria di destinazione		*READ, *ADD
	Unità ASP (se specificata)	*USE	
PRTADPOBJ [26](Q)			
PRTPUBAUT [26]			
PRTUSROBJ [26]			
PRTPVTAUT [26]			
RCLDBXREF			
RCLOBJOWN (Q)			
RCLSTG (Q)			
RCLTMPSTG (Q)	Oggetto	*OBJMGT	*EXECUTE
RMVDFRID (Q) [10]			
RNMOBJ [3,11]	Oggetto	*OBJMGT	*UPD, *EXECUTE
	Oggetto, se *AUTL	*AUTLMGT	*EXECUTE
	Oggetto (se è *FILE)	*OBJOPR, *OBJMGT	*UPD, *EXECUTE
	Unità ASP (se specificata)	*USE	
RSTDFROBJ (Q) [10]	Emissione di stampa QSYS/QPSRLDSP, se è specificato OUTPUT(*PRINT)	*USE	*EXECUTE
	File di emissione, se specificato	Fare riferimento alle regole generali	Fare riferimento alle regole generali
	File di riferimento campo QSYS/QASRRSTO per il file di emissione, se viene specificato un file di emissione che non esiste	*USE	*EXECUTE

Tabella 155. Comandi comuni per la maggior parte degli oggetti (Continua)

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
RSTOBJ (Q)[3,13, 31, 33]	Oggetto, se esiste già nella libreria	*OBJEXIST [8]	*EXECUTE, *ADD
	Oggetto, se è *CFGL, *CNNL, *CTLD, *DEVD, *LIND o *NWID	*CHANGE e *OBJMGT	*EXECUTE
	Definizione supporto magnetico	*USE	*EXECUTE
	Code messaggi ripristinate sulla libreria in cui esistono già	*OBJOPR, *OBJEXIST [8]	*EXECUTE, *ADD
	Profilo utente proprietario degli oggetti creati	*ADD [8]	
	Programma che adotta l'autorizzazione	Proprietario o autorizzazione speciale *SECADM e *ALLOBJ	*EXECUTE
	Libreria di destinazione	*EXECUTE, *ADD [8]	
	Libreria per l'oggetto salvato se viene specificato VOL(*SAVVOL)	*USE [8]	
	Salvataggio file	*USE	*EXECUTE
RSTOBJ (Q)	Unità nastro o unità ottica	*USE	*EXECUTE
	File nastro (QSYSTAP) o file minidisco (QSYSDKT)	*USE [8]	*EXECUTE
	File unità ottica (OPTFILE) [22]	*R	Non applicabili
	Indirizzario principale del file unità ottica (OPTFILE)[22]	*X	Non applicabili
	Prefisso percorso di OPTFILE[22]	*X	Non applicabili
	Volume unità ottica[24]	*USE	Non applicabili
	Emissione di stampa QSYS/QPSRLDSP, se è specificato OUTPUT(*PRINT)	*USE	*EXECUTE
	File di emissione, se specificato	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	File di riferimento campo QSYS/QASRRSTO per il file di emissione, se viene specificato un file di emissione che non esiste	*USE	*EXECUTE
	Descrizione unità ASP [25]	*USE	
RSTSYSINF	Salvataggio file	*USE	*EXECUTE
	Unità nastro o unità ottica	*USE	*EXECUTE
	File unità ottica (OPTFILE)[22]	*R	Non applicabili
	Indirizzario principale del file unità ottica (OPTFILE)[22]	*X	Non applicabili
	Prefisso percorso di OPTFILE[22]	*X	Non applicabili
	Volume unità ottica[24]	*USE	Non applicabili
RVKPUBAUT [20]			
RTVOBJD [2, 29]	Oggetto	Autorizzazione diversa da *EXCLUDE	*EXECUTE
RVKOBJAUT [3,5,15, 27]	Unità ASP (se specificata)	*USE	

Tabella 155. Comandi comuni per la maggior parte degli oggetti (Continua)

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
SAVCHGOBJ [3, 32]	Oggetto (8)	*OBJEXIST	*EXECUTE
	Unità nastro o unità ottica	*USE	*EXECUTE
	File di salvataggio, se vuoto	*USE, *ADD	*EXECUTE
	Salvare il file, se contiene i record	*OBJMGT, *USE, *ADD	*EXECUTE
	Salvataggio coda messaggi attivi	*OBJOPR, *ADD	*EXECUTE
	Spazio utente del comando, se specificato	*USE	*EXECUTE
SAVCHGOBJ	File unità ottica (OPTFILE)[22]	*RW	Non applicabili
	Indirizzario principale del file unità ottica (OPTFILE)[22]	*WX	Non applicabili
	Prefisso percorso del file unità ottica (OPTFILE)[22]	*X	Non applicabili
	Indirizzario root (/) del volume unità ottica[22, 23]	*RWX	Non applicabili
	Volume unità ottica[24]	*CHANGE	
	File di emissione, se specificato	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	File di riferimento campo QSYS/QASAVOBJ per il file di emissione, se viene specificato un file di emissione che non esiste	*USE [8]	*EXECUTE
	Emissione di stampa QSYS/QPSAVOBJ	*USE [8]	*EXECUTE
	Descrizione unità ASP [25]	*USE	
SAVOBJ [3, 32]	Oggetto	*OBJEXIST [8]	*EXECUTE
	Definizione supporto magnetico	*USE	*EXECUTE
	Unità nastro o unità ottica	*USE	*EXECUTE
	File di salvataggio, se vuoto	*USE, *ADD	*EXECUTE
	Salvare il file, se contiene i record	*OBJMGT, *USE, *ADD	*EXECUTE
	Salvataggio coda messaggi attivi	*OBJOPR, *ADD	*EXECUTE
	Spazio utente del comando, se specificato	*USE	*EXECUTE

Tabella 155. Comandi comuni per la maggior parte degli oggetti (Continua)

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
SAVOBJ	File unità ottica (OPTFILE)[22]	*RW	Non applicabili
	Indirizzario principale del file unità ottica (OPTFILE)[22]	*WX	Non applicabili
	Prefisso percorso di OPTFILE[22]	*X	Non applicabili
	Indirizzario root (/) del volume unità ottica [22, 23]	*RWX	Non applicabili
	Volume unità ottica[24]	*CHANGE	
	File di emissione, se specificato	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	File di riferimento campo QSYS/QASAVOBJ per il file di emissione, se viene specificato un file di emissione che non esiste	*USE [8]	*EXECUTE
	Emissione di stampa QSYS/QPSAVOBJ	*USE [8]	*EXECUTE
	Descrizione unità ASP [25]	*USE	
SAVSTG [10]			
SAVSYS [10]	Unità nastro, unità ottica	*USE	*EXECUTE
	Indirizzario root (/) del volume unità ottica[22]	*RWX	Non applicabili
	Volume unità ottica[24]	*CHANGE	Non applicabili
SAVSYSINF	Definizione supporto magnetico	*USE	*EXECUTE
	Unità nastro o unità ottica	*USE	*EXECUTE
	File di salvataggio, se vuoto	*USE, *ADD	*EXECUTE
	Salvare il file, se contiene i record	*OBJMGT, *USE, *ADD	*EXECUTE
	File unità ottica (OPTFILE) [22]	*RW	Non applicabili
	Indirizzario principale del file unità ottica (OPTFILE)[22]	*WX	Non applicabili
	Prefisso percorso di OPTFILE[22]	*X	Non applicabili
	Indirizzario root (/) del volume unità ottica [22, 23]	*RWX	Non applicabili
	Volume unità ottica[24]	*CHANGE	
SAVRSTCHG	Sul sistema di origine, è richiesta la stessa autorizzazione del comando SAVCHGOBJ.		
	Sul sistema di destinazione, è richiesta la stessa autorizzazione del comando RSTOBJ.		
	Descrizione unità ASP [25]	*USE	
SAVRSTOBJ	Sul sistema di destinazione, è richiesta la stessa autorizzazione del comando SAVOBJ.		
	Sul sistema di destinazione, è richiesta la stessa autorizzazione del comando RSTOBJ.		
	Descrizione unità ASP [25]	*USE	
SETOBJACC	Oggetto	*OBJOPR	*EXECUTE
STROBJCVN (Q)[20]			

Tabella 155. Comandi comuni per la maggior parte degli oggetti (Continua)

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
STRSAVSYNC[34]			
WRKOBJ [19]	Oggetto	Qualsiasi autorizzazione	*USE
WRKOBJLCK	Oggetto		*EXECUTE
	Unità ASP	*EXECUTE	
WRKOBJOWN [17]	Profilo utente	*READ	*EXECUTE
WRKOBJPGP [17]	Profilo utente	*READ	*EXECUTE
WRKOBJPVT[17]	Profilo utente	*READ	*EXECUTE

[1] Consultare la parola chiave OBJTYPE del comando ALCOBJ per l'elenco di tipi di oggetto che possono essere assegnati o di cui è possibile annullare l'assegnazione.

[2] È richiesta un'autorizzazione per l'oggetto (diversa da *EXCLUDE).

[3] Non è possibile utilizzare il comando per i documenti o per le cartelle. Utilizzare il comando DLO (Document Library Object) equivalente.

[4] È necessario disporre dell'autorizzazione speciale *ALLOBJ e *SECADM per modificare il proprietario oggetto di un programma, il programma di servizio o un pacchetto SQL che adotta l'autorizzazione.

[5] È necessario essere il proprietario o disporre dell'autorizzazione *OBJMGT e delle autorizzazioni concesse o revocate.

[6] È necessario essere il proprietario o disporre dell'autorizzazione speciale *ALLOBJ per concedere l'autorizzazione *OBJMGT o *AUTLMGT.

[7] Questo comando non può essere utilizzato per i profili utente, per le descrizioni programma di controllo, le descrizioni unità, le descrizioni riga, i documenti, le librerie documento e le cartelle.

[8] Se si dispone dell'autorizzazione speciale *SAVSYS, non è necessaria l'autorizzazione specificata.

[9] Se l'utente che sta eseguendo il comando CRTDUPOBJ dispone dell'autorizzazione OWNER(*GRPPRF) per il relativo profilo utente, il proprietario del nuovo oggetto è il profilo di gruppo. Per copiare correttamente le autorizzazioni su un nuovo oggetto di cui il proprietario è il profilo di gruppo, è necessario considerare il seguente:

- L'utente che esegue il comando deve avere l'autorizzazione per l'oggetto di provenienza. Le autorizzazioni possono essere ottenute dall'autorizzazione adottata o tramite il profilo di gruppo.
- Se si verifica un errore durante la copia delle autorizzazioni su un nuovo oggetto, l'oggetto appena creato viene cancellato.

[10] È necessario disporre dell'autorizzazione speciale *SAVSYS.

Tabella 155. Comandi comuni per la maggior parte degli oggetti (Continua)

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
[11] Questo comando non può essere utilizzato per i giornali e i ricevitori del giornale.			
[12] Questo comando non può essere utilizzato per i giornali e per i ricevitori del giornale, a meno che la libreria di provenienza non sia QRCL e la libreria di destinazione non sia la libreria originale per il giornale o il ricevitore del giornale.			
[13] È necessario disporre dell'autorizzazione speciale *ALLOBJ per specificare un valore diverso da *NONE per il parametro ALWOBJDIF (Consenso differenze oggetto).			
[14] Per controllare l'autorizzazione dell'utente per un oggetto, è necessario disporre dell'autorizzazione di cui si sta facendo il controllo. Ad esempio, per controllare se un utente dispone dell'autorizzazione *OBJEXIST per FILEB, è necessario disporre dell'autorizzazione *OBJEXIST per FILEB.			
[15] Per proteggere un oggetto tramite un elenco di autorizzazioni o rimuovere l'elenco di autorizzazioni dall'oggetto, è necessario effettuare una delle seguenti operazioni: • Essere il proprietario dell'oggetto. • Disporre dell'autorizzazione *ALL per l'oggetto. • Disporre dell'autorizzazione speciale *ALLOBJ.			
[16] Se il file originale o il file ridenominato dispone di un archivio autorizzazioni associato, è richiesta l'autorizzazione *ALL per l'archivio autorizzazioni.			
[17] Il comando non supporta il file system QOPT.			
[18] È necessario disporre dell'autorizzazione speciale *AUDIT.			
[19] Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta da tale operazione.			
[20] È necessario disporre dell'autorizzazione speciale *ALLOBJ.			
[21] Tutte le autorizzazioni sull'oggetto di provenienza vengono duplicate per il nuovo oggetto. Il gruppo principale del nuovo oggetto è determinato dal campo (GRPAUTTYP) del tipo di autorizzazione gruppo nel profilo utente che sta eseguendo il comando. Se l'oggetto di provenienza dispone di un gruppo principale, il nuovo oggetto potrebbe non disporre dello stesso gruppo principale, ma l'autorizzazione di tale gruppo sull'oggetto di provenienza verrà duplicata sul nuovo oggetto.			
[22] La verifica dell'autorizzazione viene effettuata solo quando il formato supporto magnetico dell'unità ottica corrisponde all'UDF (Universal Disk Format).			
[23] Tale verifica dell'autorizzazione viene effettuata solo se si sta ripulendo il volume dell'unità ottica.			
[24] I volumi dell'unità ottica non sono oggetti di sistema effettivi. Il collegamento tra il volume dell'unità ottica e l'elenco di autorizzazioni utilizzato per proteggere il volume viene gestito dalla funzione di supporto dell'unità ottica.			
[25] Autorizzazione necessaria solo se l'operazione di salvataggio o ripristino richiede uno switch dello spazio nome libreria.			

Tabella 155. Comandi comuni per la maggior parte degli oggetti (Continua)

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
[26] È necessario disporre dell'autorizzazione speciale *ALLOBJ o *AUDIT per utilizzare questo comando.			
[27] *** **Rischio per la sicurezza** *** La revoca di tutte le autorizzazioni assegnate specificamente ad un utente per un oggetto può fare sì che l'utente abbia un'autorizzazione superiore a quella che aveva prima della revoca. Se un utente dispone dell'autorizzazione *USE per un oggetto e dell'autorizzazione *CHANGE nell'elenco di autorizzazioni che protegge l'oggetto, la revoca dell'autorizzazione *USE può fare sì che l'utente disponga dell'autorizzazione *CHANGE per l'oggetto.			
[28] È necessario disporre dell'autorizzazione speciale *ALLOBJ o *AUDIT perché sia visualizzato il valore di controllo dell'oggetto corrente. Altrimenti, verrà visualizzato il valore *NOTAVL ad indicare che il valore non è disponibile per la visualizzazione.			
[29] È necessario disporre dell'autorizzazione speciale *ALLOBJ o *AUDIT per richiamare il valore di controllo dell'oggetto corrente. Altrimenti, viene restituito il valore *NOTAVL ad indicare che i valori non sono disponibili per il richiamo.			
[30] Esaminare i comandi CHGPGM, CHGSRVPGM e CHGMOD per determinare l'autorizzazione necessaria per convertire programmi, programmi di servizio e moduli.			
[31] È necessario disporre dell'autorizzazione special *ALLOBJ per specificare *YES per il parametro PVTAUT.			
[32] È necessario disporre delle autorizzazioni speciali *ALLOBJ o *SAVSYS per specificare *YES per il parametro PVTAUT.			
[33] È necessario disporre dell'autorizzazione speciale *SAVSYS per specificare un nome per il parametro DFRID.			
[34] È necessario disporre delle autorizzazioni speciali *SAVSYS e *JOBCTL.			

Comandi per il ripristino del percorso di accesso

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi per il ripristino del percorso di accesso

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Questi comandi non richiedono le autorizzazioni per l'oggetto.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGRCYAP [1] (Q)	Unità ASP (se specificata)	*USE	
DSPRCYAP [1]	Unità ASP (se specificata)	*USE	
EDTRBDAP [2] (Q)			
EDTRCYAP [1] (Q)	Unità ASP (se specificata)	*USE	
[1] È necessario disporre dell'autorizzazione speciale *JOBCTL per utilizzare questo comando.			
[2] È necessario disporre dell'autorizzazione speciale *ALLOBJ per utilizzare questo comando.			

Comandi AFP (Advanced Function Presentation)

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi AFP (Advanced Function Presentation).

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDFNTTBLE	Tabella ordine DBCS	*CHANGE	*EXECUTE
CHGCDEFNT	Risorsa font	*CHANGE	*EXECUTE
CHGFNTTBLE	Tabella ordine DBCS	*CHANGE	*EXECUTE
CRTFNTRSC	File di origine	*USE	*EXECUTE
	Risorsa font: REPLACE(*NO)		*READ, *ADD
	Risorsa font: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
CRTFNTTBL	Tabella ordine DBCS		*READ, *ADD
CRTFORMDF	File di origine	*USE	*EXECUTE
	Definizione modulo: REPLACE(*NO)		*READ, *ADD
	Definizione modulo: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
CRTOVL	File di origine	*USE	*EXECUTE
	Sovrapposizione: REPLACE(*NO)		*READ, *ADD
	Sovrapposizione: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
CRTPAGDFN	File di origine	*USE	*EXECUTE
	Definizione pagina: REPLACE(*NO)		*READ, *ADD
	Definizione pagina: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
CRTPAGSEG	File di origine	*USE	*EXECUTE
	Segmento pagina: REPLACE(*NO)		*READ, *ADD
	Segmento pagina: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
DLTFNTRSC	Risorsa font	*OBJEXIST	*EXECUTE
DLTFNTTBL	Tabella ordine DBCS	*CHANGE	*EXECUTE
DLTFORMDF	Definizione modulo	*OBJEXIST	*EXECUTE
DLTOVL	Sovrapposizione	*OBJEXIST	*EXECUTE
DLTPAGDFN	Definizione pagina	*OBJEXIST	*EXECUTE
DLTPAGSEG	Segmento pagina	*OBJEXIST	*EXECUTE
DSPCDEFNT	Risorsa font	*USE	*EXECUTE
DSPFNTRSCA	Risorsa font	*USE	*EXECUTE
DSPFNTTBL	Tabella ordine DBCS	*USE	*EXECUTE
RMVFNTTBLE	Tabella ordine DBCS	*CHANGE	*EXECUTE
WRKFNTRSC [1]	Risorsa font	*USE	*USE
WRKFORMDF [1]	Definizione modulo	*USE	*USE
WRKOVL [1]	Sovrapposizione	*USE	*USE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
WRKPAGDFN [1]	Definizione pagina	Qualsiasi autorizzazione	*USE
WRKPAGSEG [1]	Segmento pagina	*USE	Qualsiasi autorizzazione

[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

Socket AF_INET sui comandi SNA

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi socket AF_INET su SNA.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Questi comandi non richiedono l'autorizzazione agli oggetti:

Questi comandi non richiedono l'autorizzazione agli oggetti:			
ADDIPSIFC[1] ADDIPSRTE[1] ADDIPSLOC[1] CFGIPS	CHGIPSIFC[1] CHGIPSLOC[1] CHGIPSTOS[1] CVTIPSIFC	CVTIPSLOC ENDIPSIFC (Q) PRTIPSCFG RMVIPSIFC[1]	RMVIPSLOC[1] RMVIPSRTE[1] STRIPSIFC (Q)

[1] È necessario disporre dell'autorizzazione speciale *IOSYSCFG per utilizzare questo comando.

Comandi relativi ai messaggi di avviso

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi relativi ai messaggi di avviso.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDALRD	Tabella avvisi	*USE, *ADD	*EXECUTE
CHGALRD	Tabella avvisi	*USE, *UPD	*EXECUTE
CHGALRTBL (Q)	Tabella avvisi	*CHANGE	*EXECUTE
CRTALRTBL (Q)	Tabella avvisi		*READ, *ADD
DLTALR	File fisico QAALERT	*USE, *DLT	*EXECUTE
DLTALRTBL (Q)	Tabella avvisi	*OBJEXIST	*EXECUTE
RMVALRD	Tabella avvisi	*USE, *DLT	*EXECUTE
WRKALR [1]	File fisico QAALERT	*USE	*EXECUTE
WRKALRD [1]	Tabella avvisi	*USE	*EXECUTE
WRKALRTBL [1]	Tabella avvisi	*READ	*USE

[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

Comandi di sviluppo applicazione

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi di sviluppo applicazione.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
FNDSTRPDM	Parte di origine	*READ	*EXECUTE
MRGFORMD	Descrizione modulo	*READ	*EXECUTE
STRAPF [1]	File di origine	*OBJMGT, *CHANGE	*READ, *ADD
	Comandi CRTPF, CRTLF, ADDPFM, ADDLFM e RMVM	*USE	*EXECUTE
STRBGU [1]	Grafico	*OBJMGT, *CHANGE	*EXECUTE
STRDFU [1]	Programma (se è presente l'opzione di creazione programma)		*READ, *ADD
	Programma (se è presente l'opzione di modifica o cancellazione programma)	*OBJEXIST	*EXECUTE
	Programma (se è presente l'opzione di modifica o visualizzazione dati)	*USE	*EXECUTE
	File di database (se è presente l'opzione di modifica dati)	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	File di database (se è presente l'opzione di visualizzazione dati)	*USE	*EXECUTE
	Visualizzare file (se è presente l'opzione di visualizzazione o modifica dati)	*USE	*EXECUTE
	Visualizzare file (se è presente l'opzione di modifica programma)	*USE	*EXECUTE
	Visualizzare file (se è presente l'opzione di cancellazione programma)	*OBJEXIST	*EXECUTE
STRPDM [1]			
STRRLU	File di origine	*READ, *ADD, *UPD, *DLT	*EXECUTE
	Editare, aggiungere o modificare un membro	*OBJOPR, *OBJMGT	*READ, *ADD
	Sfogliare membro	*OBJOPR	*EXECUTE
	Stampare un prospetto prototipo	*OBJOPR	*EXECUTE
	Rimuovere membro	*OBJOPR, *OBJEXIST	*EXECUTE
	Modificare tipo o testo del membro	*OBJOPR	*EXECUTE
STRSDA	File di origine	*READ, *ADD, *UPD, *DLT	*EXECUTE
	Aggiornare e aggiungere un nuovo membro	*CHANGE, *OBJMGT	*READ, *ADD
	Cancellare membro	*ALL	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
STRSEU [1]	File di origine	*USE	*EXECUTE
	Editare o modificare un membro	*CHANGE, *OBJMGT	*EXECUTE
	Aggiungere un membro	*USE, *OBJMGT	*READ, *ADD
	Sfogliare membro	*USE	*EXECUTE
	Stampare membro	*USE	*EXECUTE
	Rimuovere membro	*USE, *OBJEXIST	*EXECUTE
	Modificare tipo o testo di un membro	*USE, *OBJMGT	*EXECUTE
WRKLIBPDM [1, 4]			
WRKMBRPDM [1]	File di origine	*USE	*EXECUTE
WRKOBJPDM [1]	File	*READ o proprietà	*EXECUTE

[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta dall'operazione.

[2] Un gruppo corrisponde a una libreria.

[3] Un progetto è costituito da uno o più gruppi (librerie).

[4] Questo comando richiede l'autorizzazione speciale *ALLOBJ.

Comandi archivio autorizzazioni

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi archivio autorizzazioni.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTAUTHLR (Q)	Oggetti associati se presenti	*ALL	*EXECUTE
DLTAUTHLR	Archivio autorizzazioni	*ALL	*EXECUTE
DSPAUTHLR	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.

Comandi elenco di autorizzazioni

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi elenco autorizzazioni.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria QSYS**
ADDAUTLE [1]	*AUTL	*AUTLMGT o proprietà	*EXECUTE
CHGAUTLE [1]	*AUTL	*AUTLMGT o proprietà	*EXECUTE
CRTAUTL			
DLTAUTL	*AUTL	Proprietario o *ALLOBJ	*EXECUTE
DSPAUTL	*AUTL		*EXECUTE
	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria QSYS**
DSPAUTLDLO	*AUTL	*USE	*EXECUTE
DSPAUTLOBJ	*AUTL	*READ	*EXECUTE
	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
EDTAUTL [1]	*AUTL	*AUTLMGT o proprietà	*EXECUTE
RMVAUTLE [1]	*AUTL	*AUTLMGT o proprietà	*EXECUTE
RTVAUTLE [2]	*AUTL	*AUTLMGT o proprietà	*EXECUTE
WRKAUTL [3,4,5]	*AUTL		

[1] È necessario essere il proprietario o disporre dell'autorizzazione di gestione elenco di autorizzazioni.

[2] Se non si dispone dell'autorizzazione *OBJMGT o *AUTLMGT, è possibile richiamare l'autorizzazione *PUBLIC e la propria autorizzazione. È necessario disporre dell'autorizzazione *READ per il proprio profilo per richiamare la propria autorizzazione.

[3] Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.

[4] È necessario che non si venga esclusi (*EXCLUDE) dall'elenco di autorizzazioni.

[5] È necessaria un'autorizzazione per l'elenco di autorizzazioni.

Comandi indirizzario di collegamento

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi indirizzario di collegamento.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDBNDDIRE	Indirizzario di collegamento	*OBJOPR, *ADD	*USE
CRTBNDDIR	Indirizzario di collegamento		*READ, *ADD
DLTBNDDIR	Indirizzario di collegamento	*OBJEXIST	*EXECUTE
DSPBNDDIR	Indirizzario di collegamento	*READ, *OBJOPR	*USE
RMVBNDDIRE	Indirizzario di collegamento	*OBJOPR, *DLT	*READ, *OBJOPR
WRKBNDDIR [1]	Indirizzario di collegamento	Qualsiasi autorizzazione	*USE
WRKBNDDIRE [1]	Indirizzario di collegamento	*READ, *OBJOPR	*USE

[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione necessaria per l'operazione.

Comandi Modifica descrizione richiesta

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi modifica descrizione richiesta.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDCMDCRQA (Q)	Modifica descrizione richiesta	*CHANGE	*EXECUTE
ADDOBJCRQA (Q)	Modifica descrizione richiesta	*CHANGE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDPRDCRQA (Q)	Modifica descrizione richiesta	*CHANGE	*EXECUTE
ADDPTFCRQA (Q)	Modifica descrizione richiesta	*CHANGE	*EXECUTE
ADDRSCCRQA (Q)	Modifica descrizione richiesta	*CHANGE	*EXECUTE
CHGCMDCRQA (Q)	Modifica descrizione richiesta	*CHANGE	*EXECUTE
CHGOBJCRQA (Q)	Modifica descrizione richiesta	*CHANGE	*EXECUTE
CHGPRDCRQA (Q)	Modifica descrizione richiesta	*CHANGE	*EXECUTE
CHGPTFCRQA (Q)	Modifica descrizione richiesta	*CHANGE	*EXECUTE
CHGCRQD	Modifica descrizione richiesta	*CHANGE	*EXECUTE
CHGRSCCRQA (Q)	Modifica descrizione richiesta	*CHANGE	*EXECUTE
CRTCRQD	Modifica descrizione richiesta		*READ, *ADD
DLTCRQD	Modifica descrizione richiesta	*OBJEXIST	*EXECUTE
RMVCRQDA	Modifica descrizione richiesta	*CHANGE	*EXECUTE
WRKCRQD [1]	Modifica descrizione richiesta		*EXECUTE

1 Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.

Comandi grafico

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi grafico.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
DLTCHTFMT	Formato grafico	*OBJEXIST	*EXECUTE
DSPCHT	Formato grafico	*USE	*USE
	File di database	*USE	*USE
DSPGDF	File di database	*USE	*USE
STRBGU (Opzione 3) [2]	Formato grafico	*CHANGE, *OBJEXIST	*EXECUTE
WRKCHTFMT [1]	Formato grafico	Qualsiasi autorizzazione	*USE

1 Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.

2 L'opzione 3 sul menu BGU (visualizzata quando viene eseguito STRGBU) è l'opzione formato Modifica grafico.

Comandi classe

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi classe.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGCLS	Classe	*OBJMGT, *OBJOPR	*EXECUTE
CRTCLS	Classe		*READ, *ADD
DLTCLS	Classe	*OBJEXIST	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
DSPCLS	Classe	*USE	*EXECUTE
WRKCLS [1]	Classe	*OBJOPR	*USE

[1] Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.

Comandi classe-di-servizio

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi classe di servizio.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGCOSD [3]	Descrizione classe-di-servizio	*CHANGE, OBJMGT	*EXECUTE
CRTCOSD [3]	Descrizione classe-di-servizio		
DLTCOSD	Descrizione classe-di-servizio	*OBJEXIST	*EXECUTE
DSPCOSD	Descrizione classe-di-servizio	*USE	*EXECUTE
WRKCOSD [1,2]	Descrizione classe-di-servizio	*OBJOPR	*EXECUTE

[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

[2] È necessaria un'autorizzazione per l'oggetto.

[3] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *IOSYSCFG.

Comandi cluster

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi cluster.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri utenti.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDCLUNODE (Q)[1]	Programma di servizio QCSTCTL	*USE	
ADDCRGDEVE (Q)[1]	Programma di servizio QCSTCRG1	*USE	
	Gruppo risorse cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Programma di uscita	*EXECUTE[2]	*EXECUTE[2]
	Profilo utente per l'esecuzione del programma di uscita	*USE	
	Descrizione unità	*USE, *OBJMGT	
	Descrizione unità di controllo	*USE, *OBJMGT	
	Descrizione linea	*USE, *OBJMGT	
	Descrizione server di rete	*USE, *OBJMGT	

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDCRGNODE (Q)[1]	Programma di servizio QCSTCRG1	*USE	
	Gruppo risorse cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Programma di uscita	*EXECUTE[2]	*EXECUTE[2]
	Profilo utente per l'esecuzione del programma di uscita	*USE	
	Coda messaggi di failover	*OBJOPR, *ADD	*EXECUTE
	Coda utente informazioni sulla distribuzione	*OBJOPR, *ADD	*EXECUTE
ADDDEVDMNE (Q)[1]	Programma di servizio QCSTDD	*USE	
CHGCLUCFG (Q)[1]	Programma di servizio QCSTCTL2	*USE	
CHGCLUNODE (Q)[1]	Programma di servizio QCSTCTL	*USE	
CHGCLURCY	Gruppo risorse cluster	*USE	
		*JOBCTL	
		*SERVICE o funzione Traccia di servizio	
CHGCLUVER (Q)[1]	Programma di servizio QCSTCTL2	*USE	
CHGCRG (Q)[1]	Programma di servizio QCSTCRG1	*USE	
	Gruppo risorse cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Programma di uscita	*EXECUTE[2]	*EXECUTE[2]
	Profilo utente per l'esecuzione del programma di uscita	*USE	
	Descrizione unità	*USE, *OBJMGT	
	Coda messaggi di failover	*OBJOPR, *ADD	*EXECUTE
	Descrizione unità di controllo	*USE, *OBJMGT	
	Descrizione linea	*USE, *OBJMGT	
	Descrizione server di rete	*USE, *OBJMGT	
CHGCRGDEVE (Q)[1]	Programma di servizio QCSTCRG1	*USE	
	Gruppo risorse cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Programma di uscita	*EXECUTE[2]	*EXECUTE[2]
	Profilo utente per l'esecuzione del programma di uscita	*USE	
	Descrizione unità	*USE, *OBJMGT	
	Descrizione unità di controllo	*USE, *OBJMGT	
	Descrizione linea	*USE, *OBJMGT	
	Descrizione server di rete	*USE, *OBJMGT	

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGCRGPRI (Q)[1]	Programma di servizio QCSTCRG2	*USE	
	Gruppo risorse cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Programma di uscita	*EXECUTE[2]	*EXECUTE[2]
	Profilo utente per l'esecuzione del programma di uscita	*USE	
	Descrizione unità	*USE, *OBJMGT	
	Comando VRYCFG (Modifica stato configurazione)	*USE	
	Descrizione unità di controllo	*USE, *OBJMGT	
	Descrizione linea	*USE, *OBJMGT	
	Descrizione server di rete	*USE, *OBJMGT	
CRTADMDMN (Q)[1, 3]	Profilo utente QCLUSTER	*USE	
CRTCLU (Q)[1]	Programma di servizio QCSTCTL	*USE	
CRTCRG (Q) [1]	Programma di servizio QCSTCRG1	*USE	
	Libreria gruppo risorse cluster		*OBJOPR, *ADD, *READ (QUSRSYS)
	Programma di uscita	*EXECUTE[2]	*EXECUTE[2]
	Profilo utente per l'esecuzione del programma di uscita	*USE	
	Descrizione unità	*USE, *OBJMGT	
	Coda utente informazioni sulla distribuzione	*OBJOPR, *ADD	*EXECUTE
	Coda messaggi di failover	*OBJOPR, *ADD	*EXECUTE
	Descrizione unità di controllo	*USE, *OBJMGT	
	Descrizione linea	*USE, *OBJMGT	
	Descrizione server di rete	*USE, *OBJMGT	
DLTADMDMN (Q) [1]	Gruppo risorse cluster	*OBJEXIST, *USE	
	QUSRSYS	*EXECUTE	
	QCLUSTER	*USE	
DLTCLU (Q)[1]	Programma di servizio QCSTCTL	*USE	
DLTCRG[1]	Gruppo risorse cluster	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)
DLTCRGCLU (Q)[1]	Programma di servizio QCSTCRG1	*USE	
	Gruppo risorse cluster	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)
	Programma di uscita	*EXECUTE[2]	*EXECUTE[2]
	Profilo utente per l'esecuzione del programma di uscita	*USE	
DMPCLUTRC	Gruppo risorse cluster	*USE	
		*SERVICE o funzione Traccia di servizio	
DSPCLUINF			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
DSPCRGINF	Gruppo risorse cluster	*USE	*EXECUTE (QUSRSYS)
ENDCLUNOD (Q)[1]	Programma di servizio QCSTCTL	*USE	
ENDCHTSVR (Q)	Elenco di autorizzazioni	*CHANGE	
ENDCRG (Q)[1]	Programma di servizio QCSTCRG2	*USE	
	Gruppo risorse cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Programma di uscita	*EXECUTE[2]	*EXECUTE[2]
	Profilo utente per l'esecuzione del programma di uscita	*USE	
RMVCLUNODE (Q)[1]	Programma di servizio QCSTCTL	*USE	
RMVCRGDEVE (Q)[1]	Programma di servizio QCSTCRG1	*USE	
	Gruppo risorse cluster	*CHANGE	*EXECUTE
	Programma di uscita	*EXECUTE[2]	*EXECUTE[2]
	Profilo utente per l'esecuzione del programma di uscita	*USE	
	Descrizione unità	*USE, *OBJMGT	
	Descrizione unità di controllo	*USE, *OBJMGT	
	Descrizione linea	*USE, *OBJMGT	
	Descrizione server di rete	*USE, *OBJMGT	
RMVCRGNODE (Q) [1]	Programma di servizio QCSTCRG1	*USE	
	Gruppo risorse cluster	*CHANGE, *OBJEXIST	*EXECUTE
	Programma di uscita	*EXECUTE[2]	*EXECUTE[2]
	Profilo utente per l'esecuzione del programma di uscita	*USE	
	Descrizione unità	*USE, *OBJMGT	
	Descrizione unità di controllo	*USE, *OBJMGT	
	Descrizione linea	*USE, *OBJMGT	
	Descrizione server di rete	*USE, *OBJMGT	
RMVDEVDMNE (Q)[1]	Programma di servizio QCSTDD	*USE	
STRCHTSVR	Elenco di autorizzazioni	*CHANGE	
STRCLUNOD (Q)[1]	Programma di servizio QCSTCTL	*USE	
STRCRG (Q)[1]	Programma di servizio QCSTCRG2	*USE	
	Gruppo risorse cluster	*CHANGE	*EXECUTE
	Programma di uscita	*EXECUTE[2]	*EXECUTE[2]
	Profilo utente per l'esecuzione del programma di uscita	*USE	
	Descrizione unità	*USE, *OBJMGT	
	Descrizione unità di controllo	*USE, *OBJMGT	
	Descrizione linea	*USE, *OBJMGT	
	Descrizione server di rete	*USE, *OBJMGT	

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
WRKCLU[4]	Gruppo risorse cluster	*USE	*EXECUTE

[1] È necessario disporre dell'autorizzazione speciale *IOSYSCFG per utilizzare questo comando.

[2] L'autorizzazione si applica al profilo utente di chiamata e al profilo utente per l'esecuzione del programma di uscita.

[3] Al profilo utente chiamante è concessa l'autorizzazione *CHANGE e *OBJEXIST per il gruppo di risorse del cluster.

[4] L'utente deve disporre dell'autorizzazione speciale *SERVICE o essere autorizzato alla funzione Traccia di servizio i5/OS mediante Gestione applicazione in System i Navigator. È inoltre possibile utilizzare il comando CHGFCNUSG (Modifica utilizzo funzione), con un ID funzione di QIBM_SERVICE_TRACE, per modificare l'elenco di utenti a cui è consentita l'esecuzione di operazioni di traccia.

Comandi del comando (*CMD)

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi relativi alle operazioni sul comando.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGCMD	Comando	*OBJMGT	*EXECUTE
CHGCMDDFT	Comando	*OBJMGT, *USE	*EXECUTE
CHGPRXCMD	Comando proxy	*OBJMGT	*EXECUTE
CRTCMD	File di origine	*USE	*EXECUTE
	Comando: REPLACE(*NO)		*READ, *ADD
	Comando: REPLACE(*YES)	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
CRTPRXCMD	Comando proxy: REPLACE(*NO)		*READ, *ADD
	Comando proxy: REPLACE(*YES)	Consultare Regole generali alla pagina D-2	Consultare Regole generali alla pagina D-2
DLTCMD	Comando	*OBJEXIST	*EXECUTE
DSPCMD	Comando	*USE	*EXECUTE
GENCMDDOC[3]	Comando	*USE	*EXECUTE
	Gruppo pannelli (associato)	*USE	*EXECUTE
	File di emissione: REPLACE = (*YES)	*ALL	*CHANGE
SBMRMTCMD	Comando	*OBJOPR	*EXECUTE
	File DDM	*USE	*EXECUTE
SLTCMD [1]	Comando	Qualsiasi autorizzazione	*USE
WRKCMD [2]	Comando	Qualsiasi autorizzazione	*USE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**

[1] È necessario essere proprietario o disporre di un'autorizzazione per l'oggetto.

[2] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

[3] È necessario disporre dell'autorizzazione all'esecuzione (*X) per gli indirizzari nel percorso per il file generato e delle autorizzazioni alla scrittura e all'esecuzione (*WX) per l'indirizzario principale del file generato.

Comandi controllo sincronizzazione

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi controllo sincronizzazione.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
COMMIT			
ENDCMTCTL	Coda messaggi, come specificato sulla parola chiave NFYOBJ per il comando STRCMTCTL associato.	*OBJOPR, *ADD	*EXECUTE
ROLLBACK			
STRCMTCTL	Coda messaggi, quando specificato sulla parola chiave NFYOBJ	*OBJOPR, *ADD	*EXECUTE
	Area dati, come specificato sulla parola chiave NFYOBJ per il comando STRCMTCTL associato.	*CHANGE	*EXECUTE
	File, come specificato sulla parola chiave NFYOBJ per il comando STRCMTCTL associato.	*OBJOPR *READ	*EXECUTE
WRKCMTDFN [1]			

[1] Un utente può eseguire questo comando per le definizioni di sincronizzazione che appartengono a un lavoro in esecuzione con il profilo utente dell'utente. Un utente che dispone dell'autorizzazione speciale *JOBCTL (controllo lavoro) può eseguire questo comando per qualsiasi definizione di sincronizzazione.

Comandi informazioni lato comunicazioni

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi informazioni lato comunicazioni.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGCSI	Oggetto informazioni lato comunicazioni	*USE, *OBJMGT	*EXECUTE
	Descrizione unità [1]	*CHANGE	
CRTCSI	Oggetto informazioni lato comunicazioni		*READ, *ADD
	Descrizione unità [1]	*CHANGE	
DLTCSI	Oggetto informazioni lato comunicazioni	*OBJEXIST	*EXECUTE
DSPCSI	Oggetto informazioni lato comunicazioni	*READ	*EXECUTE
WRKCSI	Oggetti informazioni lato comunicazioni	*USE	*EXECUTE

[1] L'autorizzazione viene verificata quando si utilizza l'oggetto informazioni lato comunicazioni.

Comandi di configurazione

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi di configurazione.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

		Autorizzazione necessaria	
Comando	**Oggetto di riferimento**	**Per oggetto**	**Per libreria**
PRTDEVADR	Descrizione unità di controllo (CTL)	*USE	*EXECUTE
	Descrizione unità	*USE	*EXECUTE
RSTCFG (Q) [5]	Ciascun oggetto ripristinato da una versione salvata	*OBJEXIST [1]	*EXECUTE
	Libreria di destinazione		*ADD, *EXECUTE [1]
	Profilo utente proprietario degli oggetti creati	*ADD [1]	
	Unità nastro	*USE	*EXECUTE
	File nastro (QSYSTAP)	*USE [1]	*EXECUTE
	Salvataggio file, se specificato	*USE	*EXECUTE
	Emissione di stampa (QPSRLDSP), se è specificato output(*print)	*USE	*EXECUTE
	File di emissione, se specificato	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	File di riferimento campo QSYS/QASRRSTO, se il file di emissione è specificato e non è presente	*USE	*EXECUTE
RTVCFGSTS	Oggetto	*OBJOPR	*EXECUTE
RTVCFGSRC	Oggetto	*USE	*EXECUTE
	File di origine	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
SAVCFG [2]	File di salvataggio, se vuoto	*USE, *ADD	*EXECUTE
	Salvare il file, se contiene i record	*USE, *ADD, *OBJMGT	*EXECUTE
SAVRSTCFG	Sul sistema di origine, è richiesta la stessa autorizzazione del comando SAVCFG.		
	Sul sistema di destinazione, è richiesta la stessa autorizzazione del comando RSTCFG.		
VRYCFG [3, 5, 6, 7]	Oggetto	*USE, *OBJMGT	*EXECUTE
WRKCFGSTS [4]	Oggetto	*OBJOPR	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**

[1] Se si dispone dell'autorizzazione speciale *SAVSYS, non è necessaria l'autorizzazione specificata.

[2] È necessario disporre dell'autorizzazione speciale *SAVSYS.

[3] Se un utente dispone dell'autorizzazione speciale *JOBCTL, l'autorizzazione per l'oggetto non è necessaria.

[4] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta dall'operazione.

[5] È necessario disporre dell'autorizzazione speciale *ALLOBJ per specificare un valore diverso da *NONE per il parametro ALWOBJDIF (Consenso differenze oggetto) o RESETSYS(*YES).

[6] È necessario disporre dell'autorizzazione speciale *IOSYSCFG quando l'oggetto è una libreria supporto magnetico e lo stato è *ALLOCATE o *DEALLOCATE.

[7] L'utente deve disporre delle autorizzazioni speciali *IOSYSCFG e *SECADM per specificare GENPTHCERT(*YES).

Comandi elenco di configurazione

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi elenco di configurazione.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDCFGLE [2]	Elenco di configurazione	*CHANGE, *OBJMGT	*EXECUTE
CHGCFGL [2]	Elenco di configurazione	*CHANGE, *OBJMGT	*EXECUTE
CHGCFGLE [2]	Elenco di configurazione	*CHANGE, *OBJMGT	*EXECUTE
CPYCFGL [2]	Elenco di configurazione	*USE, *OBJMGT	*ADD
CRTCFGL [2]	Elenco di configurazione		
DLTCFGL	Elenco di configurazione	*OBJEXIST	*EXECUTE
DSPCFGL [2]	Elenco di configurazione	*USE, *OBJMGT	*EXECUTE
RMVCFGLE [2]	Elenco di configurazione	*CHANGE, *OBJMGT	*EXECUTE
WRKCFGL [1, 2]	Elenco di configurazione	*OBJOPR	*EXECUTE

[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta dall'operazione.

[2] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *IOSYSCFG.

Comandi elenco collegamenti

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi elenco collegamenti.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
DLTCNNL	Elenco collegamenti	*OBJEXIST	*EXECUTE
DSPCNNL	Elenco collegamenti	*USE	*EXECUTE
WRKCNNL [1]	Elenco collegamenti	*OBJOPR	*EXECUTE

[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta dall'operazione.

Comandi descrizione unità di controllo

Questa tabella elenca le autorizzazioni specifiche richieste per la descrizione unità di controllo.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGCTLAPPC [2]	Descrizione unità di controllo	*CHANGE, *OBJMGT	*EXECUTE
	Descrizione riga (SWTLINLST)	*USE	*EXECUTE
	Elenco collegamenti (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLASC [2]	Descrizione unità di controllo	*CHANGE, *OBJMGT	*EXECUTE
	Descrizione riga (SWTLINLST)	*USE	*EXECUTE
CHGCTLBSC [2]	Descrizione unità di controllo	*CHANGE, *OBJMGT	*EXECUTE
	Descrizione riga (SWTLINLST)	*USE	*EXECUTE
CHGCTLFNC [2]	Descrizione unità di controllo	*CHANGE, *OBJMGT	*EXECUTE
	Descrizione riga (SWTLINLST)	*USE	*EXECUTE
CHGCTLHOST [2]	Descrizione unità di controllo	*CHANGE, *OBJMGT	*EXECUTE
	Descrizione riga (SWTLINLST)	*USE	*EXECUTE
	Elenco collegamenti (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLLWS [2]	Descrizione unità di controllo	*CHANGE, *OBJMGT	*EXECUTE
	Programma (INZPGM)	*USE	*EXECUTE
CHGCTLNET [2]	Descrizione unità di controllo	*CHANGE, *OBJMGT	*EXECUTE
CHGCTLRTL [2]	Descrizione unità di controllo	*CHANGE, *OBJMGT	*EXECUTE
	Descrizione riga (SWTLINLST)	*USE	*EXECUTE
CHGCTLRWS [2]	Descrizione unità di controllo	*CHANGE, *OBJMGT	*EXECUTE
	Descrizione riga (SWTLINLST)	*USE	*EXECUTE
	Elenco collegamenti (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLTAP [2]	Descrizione unità di controllo	*CHANGE, *OBJMGT	*EXECUTE
CHGCTLVWS [2]	Unità di controllo	*CHANGE, *OBJMGT	*EXECUTE
CRTCTLAPPC [2]	Descrizione riga (LINE o SWTLINLST)	*USE	*EXECUTE
	Descrizione unità (DEV)	*USE	*EXECUTE
	Elenco collegamenti (CNNLSTOUT)	*USE	*EXECUTE
	Descrizione unità di controllo		
CRTCTLASC [2]	Descrizione riga (LINE o SWTLINLST)	*USE	*EXECUTE
	Descrizione unità (DEV)	*USE	*EXECUTE
	Descrizione unità di controllo		
CRTCTLBSC [2]	Descrizione riga (LINE o SWTLINLST)	*USE	*EXECUTE
	Descrizione unità (DEV)	*USE	*EXECUTE
	Descrizione unità di controllo		
CRTCTLFNC [2]	Descrizione riga (LINE o SWTLINLST)	*USE	*EXECUTE
	Descrizione unità (DEV)	*USE	*EXECUTE
	Descrizione unità di controllo		

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTCTLHOST [2]	Descrizione riga (LINE o SWTLINLST)	*USE	*EXECUTE
	Descrizione unità (DEV)	*USE	*EXECUTE
	Elenco collegamenti (CNNLSTOUT)	*USE	*EXECUTE
	Descrizione unità di controllo		
CRTCTLLWS [2]	Descrizione unità (DEV)	*USE	*EXECUTE
	Descrizione unità di controllo		
	Programma (INZPGM)	*USE	*EXECUTE
CRTCTLNET [2]	Descrizione riga (LINE)	*USE	*EXECUTE
	Descrizione unità (DEV)	*USE	*EXECUTE
	Descrizione unità di controllo		
CRTCTLRTL [2]	Descrizione riga (LINE o SWTLINLST)	*USE	*EXECUTE
	Descrizione unità (DEV)	*USE	*EXECUTE
	Descrizione unità di controllo		
CRTCTLRWS [2]	Descrizione riga (LINE o SWTLINLST)	*USE	*EXECUTE
	Descrizione unità (DEV)	*USE	*EXECUTE
	Elenco collegamenti (CNNLSTOUT)	*USE	*EXECUTE
	Descrizione unità di controllo		
CRTCTLTAP [2]	Descrizione unità (DEV)	*USE	*EXECUTE
	Descrizione unità di controllo		
CRTCTLVWS [2]	Descrizione unità (DEV)	*USE	*EXECUTE
	Descrizione unità di controllo		
DLTCTLD	Descrizione unità di controllo	*OBJEXIST	*EXECUTE
DSPCTLD	Descrizione unità di controllo	*USE	*EXECUTE
ENDCTLRCY	Descrizione unità di controllo	*USE	*EXECUTE
PRTCMNSEC [3]			
RSMCTLRCY	Descrizione unità di controllo	*USE	*EXECUTE
WRKCTLD [1]	Descrizione unità di controllo	*OBJOPR	*EXECUTE

[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta dall'operazione.

[2] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *IOSYSCFG.

[3] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *ALLOBJ, *IOSYSCFG o *AUDIT.

Comandi crittografia

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi crittografia.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ADDCKMKSFE	File utente	*ADD, *OBJOPR, *READ	
	Libreria utente		*EXECUTE
	Indirizzario utente	*X	
	File di flusso utente	*R	
ADDCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
	Coda messaggi QHST	*OBJOPR, *ADD	*EXECUTE
ADDMSTPART (Q) [1]			
CHGCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	Coda messaggi QHST	*OBJOPR, *ADD	*EXECUTE
CHGMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	Coda messaggi QHST	*OBJOPR, *ADD	*EXECUTE
CHKMSTKVV (Q) [1]			
CLRMSTKEY (Q) [1]			
CPHDTA (Q)			
CRTCKMKSF	Libreria utente		*ADD, *EXECUTE
DSPCKMKSFE	File utente	*OBJOPR, *READ	
	Libreria utente		*EXECUTE
ENCCPHK (Q)			
ENCFRMMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
ENCTOMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
GENCKMKSFE	File utente	*ADD, *OBJOPR, *READ	
	Libreria utente		*EXECUTE
GENCPHK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
GENCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
	QCRP/QPCRGENX *FILE	*OBJOPR, *READ	*EXECUTE
	Coda messaggi QHST	*OBJOPR, *ADD	*EXECUTE
GENMAC (Q)			
GENPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
RMVCKMKSFE	File utente	*DLT, *OBJOPR	
	Libreria utente		*EXECUTE
RMVCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *DLT	*EXECUTE
	Coda messaggi QHST	*OBJOPR, *ADD	*EXECUTE
SETMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	Coda messaggi QHST	*OBJOPR, *ADD	*EXECUTE
SETMSTKEY (Q) [1]			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
TRNCKMKSF	File utente	*OBJOPR, *READ, *UPD	
	Libreria utente		*EXECUTE
TRNPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
VFYMSTK (Q)	Coda messaggi QHST	*OBJOPR, *ADD	*EXECUTE
VFYPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, READ	*EXECUTE

[1] È necessario disporre delle autorizzazioni speciali *ALLOBJ e *SECADM per utilizzare questo comando.

Comandi area dati

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi area dati.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGDTAARA [1]	Area dati	*CHANGE	*EXECUTE
CRTDTAARA [1]	Area dati		*READ, *ADD
	Descrizione unità APPC [4]	*CHANGE	
DLTDTAARA	Area dati	*OBJEXIST	*EXECUTE
DSPDTAARA	Area dati	*USE	*EXECUTE
RTVDTAARA [2]	Area dati	*USE	*EXECUTE
WRKDTAARA [3]	Area dati	Qualsiasi autorizzazione	*USE

[1] Se i comandi dell'area dati di creazione e modifica vengono eseguiti utilizzando le funzioni lingua di livello superiore, queste autorizzazioni sono ancora necessarie sebbene l'autorizzazione per il comando non lo sia.

[2] L'autorizzazione viene verificata l momento dell'esecuzione ma non al momento della compilazione.

[3] Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.

[4] L'autorizzazione viene verificata al momento dell'utilizzo dell'area dati.

Comandi coda dati

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi coda dati.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTDTAQ	Coda messaggi		*READ, *ADD
	Coda dati di destinazione per il programma QSNDDTAQ	*OBJOPR, *ADD	*EXECUTE
	Coda dati di origine per il programma QRCVDTAQ	*OBJOPR, *READ	*EXECUTE
	Descrizione unità APPC [2]	*CHANGE	
DLTDTAQ	Coda messaggi	*OBJEXIST	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
WRKDTAQ [1]	Coda messaggi	*READ	*USE

[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

[2] L'autorizzazione viene verificata al momento dell'utilizzo dell'area dati.

Comandi descrizione unità

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi descrizione unità.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CFGDEVMLB [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGASPA (Q)			
CHGASPACT (Q)[7]	Descrizione unità	*USE	
CHGDEVAPPC [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
	Descrizione modalità (MODE)	*USE	*EXECUTE
CHGDEVASC [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVASP[4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVBSC [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVCRP[4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVDKT [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVDSP [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
	Stampante (PRINTER)	*USE	*EXECUTE
CHGDEVFNC [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVHOST [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVINTR [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVMLB [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVNET [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVNWSH[4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVOPT [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVPRT [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
	Elenco convalide (se specificato)	*READ	*EXECUTE
CHGDEVRTL [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVSNPT [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVSNUF [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVTAP [4]	Descrizione unità	*CHANGE, *OBJMGT	*EXECUTE
CRTDEVAPPC [4]	Descrizione unità di controllo (CTL)	*USE	*EXECUTE
	Descrizione unità		
	Descrizione modalità (MODE)	*USE	*EXECUTE
CRTDEVASC [4]	Descrizione unità di controllo (CTL)	*USE	*EXECUTE
	Descrizione unità		

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
CRTDEVASP [4]	Descrizione unità		*EXECUTE
CRTDEVBSC [4]	Descrizione unità di controllo (CTL)	*USE	*EXECUTE
	Descrizione unità		
CRTDEVCRP[4]	Descrizione unità		*EXECUTE
CRTDEVDKT [4]	Descrizione unità		*EXECUTE
CRTDEVDSP [4]	Descrizione stampante (PRINTER)	*USE	*EXECUTE
	Descrizione unità di controllo (CTL)	*USE	*EXECUTE
	Descrizione unità		
CRTDEVFNC [4]	Descrizione unità di controllo (CTL)	*USE	*EXECUTE
	Descrizione unità		
CRTDEVHOST [4]	Descrizione unità di controllo (CTL)	*USE	*EXECUTE
	Descrizione unità		
CRTDEVINTR [4]	Descrizione unità		
CRTDEVMLB [4]	Descrizione unità		*EXECUTE
CRTDEVNET [4]	Descrizione unità di controllo (CTL)	*USE	*EXECUTE
	Descrizione unità		
CRTDEVNWSH[4]	Descrizione unità		*EXECUTE
CRTDEVOPT [4]	Descrizione unità		*EXECUTE
CRTDEVPRT [4]	Descrizione unità di controllo (CTL)	*USE	*EXECUTE
	Descrizione unità		
	Elenco convalide (se specificato)	*READ	*EXECUTE
CRTDEVRTL [4]	Descrizione unità di controllo (CTL)	*USE	*EXECUTE
	Descrizione unità		
CRTDEVSNPT [4]	Descrizione unità di controllo (CTL)	*USE	*EXECUTE
	Descrizione unità		
CRTDEVSNUF [4]	Descrizione unità di controllo (CTL)	*USE	*EXECUTE
	Descrizione unità		
CRTDEVTAP [4]	Descrizione unità di controllo (CTL)	*USE	*EXECUTE
	Descrizione unità		
DLTDEVD [1]	Descrizione unità	*OBJEXIST	*EXECUTE
DSPASPSTS	Descrizione unità	*USE	
DSPCNNSTS	Descrizione unità	*OBJOPR	*EXECUTE
DSPDEVD	Descrizione unità	*USE	*EXECUTE
ENDASPBAL (Q)			
ENDDEVRCY	Descrizione unità	*USE	*EXECUTE
HLDCMNDEV [2]	Descrizione unità	*OBJOPR	*EXECUTE
PRTCMNSEC [4, 5]			
RLSCMNDEV	Descrizione unità	*OBJOPR	*EXECUTE
RSMDEVRCY	Descrizione unità	*USE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
SETASPGRP[6]	Tutte le descrizioni unità nel gruppo ASP	*USE	
	Tutte le librerie specificate nell'elenco librerie prima della modifica all'elenco librerie e allo spazio nome della libreria	*USE	
STRASPBAL (Q)			
TRCASPBAL (Q)			
WRKDEVD [3]	Descrizione unità	*OBJOPR	*EXECUTE

[1] Per rimuovere una coda di emissione associata, è necessaria l'autorizzazione esistenza oggetto *OBJEXIST per la coda di emissione e l'autorizzazione all'esecuzione *EXECUTE per la libreria QUSRSYS.

[2] È necessario disporre dell'autorizzazione speciale *JOBCTL e dell'autorizzazione operativa sull'oggetto per la descrizione unità.

[3] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

[4] È necessario disporre dell'autorizzazione speciale *IOSYSCFG per eseguire questo comando.

[5] È necessario disporre dell'autorizzazione speciale *ALLOBJ per eseguire questo comando.

[6] Quando *CURUSR si specifica *CURUSR per il gruppo ASP (ASPGRP) o le librerie per il parametro del sottoprocesso (USRLIBL) corrente, è necessario disporre anche dell'autorizzazione alla lettura (*READ) della descrizione lavoro specificata nel profilo utente e dell'autorizzazione all'esecuzione (*EXECUTE) della libreria in cui è ubicata la descrizione del lavoro.

[7] È necessario disporre dell'autorizzazione speciale *JOBCTL per eseguire questo comando.

Comandi emulazione unità

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi emulazione unità.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDEMLCFGE	File di configurazione emulazione	*CHANGE	*EXECUTE
CHGEMLCFGE	File di configurazione emulazione	*CHANGE	*EXECUTE
EJTEMLOUT	descrizione unità di emulazione quando specificato	*OBJOPR	*EXECUTE
	Descrizione unità di emulazione quando l'ubicazione è specificata	*OBJOPR	*EXECUTE
ENDPRTEML	descrizione unità di emulazione quando specificato	*OBJOPR	*EXECUTE
	Descrizione unità di emulazione quando l'ubicazione è specificata	*OBJOPR	*EXECUTE
EMLPRTKEY	descrizione unità di emulazione quando specificato	*OBJOPR	*EXECUTE
	Descrizione unità di emulazione quando l'ubicazione è specificata	*OBJOPR	*EXECUTE
EML3270	Descrizione unità di emulazione	*OBJOPR	*EXECUTE
	Descrizione unità di controllo di emulazione	*OBJOPR	*EXECUTE
RMVEMLCFGE	File di configurazione emulazione	*CHANGE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
STREML3270	File di configurazione emulazione	*OBJOPR	*EXECUTE
	Unità di emulazione, descrizione unità di controllo di emulazione, unità stazione di lavoro e descrizione unità di controllo stazione di lavoro	*OBJOPR	*EXECUTE
	Descrizione unità stampante, programma di uscita utente e tabelle di conversione quando specificati	*OBJOPR	*EXECUTE
STRPRTEML	File di configurazione emulazione	*OBJOPR	*EXECUTE
	Descrizione unità di emulazione e descrizione unità di controllo di emulazione	*OBJOPR	*EXECUTE
	Descrizione unità stampante, emissione di stampa, coda messaggi, descrizione lavoro, coda lavori e tabelle di conversione quando specificate	*OBJOPR	*EXECUTE
SNDEMLIGC	Da file	*OBJOPR	*EXECUTE
TRMPRTEML	Descrizione unità di emulazione	*OBJOPR	*EXECUTE

Comandi shadow indirizzario e indirizzario

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi shadow indirizzario e indirizzario.

Questi comandi non richiedono le autorizzazioni agli oggetti:			
ADDDIRE [2] ADDDIRSHD [1] CHGSYSDIRA [2] CHGDIRE [3]	CHGDIRSHD [1] CPYFRMDIR [1] CPYTODIR [1] DSPDIRE	ENDDIRSHD [4] RMVDIRE [1] RMVDIRSHD [1] RNMDIRE [2]	STRDIRSHD [4] WRKDIRE [3,5] WRKDIRLOC [1,5] WRKDIRSHD [1,5]

1 È necessario disporre dell'autorizzazione speciale *SECADM.

2 È necessario disporre dell'autorizzazione speciale *SECADM o *ALLOBJ.

3 Un utente con l'autorizzazione speciale *SECADM è in grado di gestire tutte le voci indirizzario. Gli utenti che non dispongono dell'autorizzazione speciale *SECADM possono gestire solo le proprie voci.

4 È necessario disporre dell'autorizzazione speciale *JOBCTL.

5 Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.

Comandi server indirizzario

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi server indirizzario.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGDIRSRVA [1]			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CPYTOLDIF [2]	File di flusso LDIF (se già esistente)	*STMF	*W, *OBJEXIST, *OBJMGT
	Indirizzario principale del file di flusso LDIF	*DIR	*WX
CPYFRMLDIF [2]	File di flusso LDIF	*STMF	*R
	Indirizzario principale del file di flusso LDIF	*DIR	*X
DB2LDIF [2]	File di flusso LDIF (se già esistente)	*STMF	*W, *OBJEXIST, *OBJMGT
	Indirizzario principale del file di flusso LDIF	*DIR	*WX
LDIF2DB [2]	File di flusso LDIF	*STMF	*R
	Indirizzario principale del file di flusso LDIF	*DIR	*X

[1] È necessario disporre delle autorizzazioni speciali *ALLOBJ e *IOSYSCFG.

[2] Per utilizzare questo comando, è necessario soddisfare una delle seguenti condizioni:
- Disporre delle autorizzazioni speciali *ALLOBJ e *IOSYSCFG
- Fornire la parola d'ordine e il DN dell'amministratore
- Essere un amministratore server indirizzario

Comandi disco

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi disco.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Questi comandi non richiedono autorizzazione per alcun oggetto:			
ENDDSKRGZ (Q) [1]	STRDSKRGZ (Q) [1]	WRKDSKSTS	

[1] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *ALLOBJ.

Comandi pass-through stazione video

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi pass-through stazione video.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ENDPASTHR			
STRPASTHR	Unità APPC sul sistema di origine	*CHANGE	*EXECUTE
	Unità APPC sul sistema di destinazione	*CHANGE	*EXECUTE
	Unità di controllo virtuale sul sistema di destinazione [1]	*USE	*EXECUTE
	Unità virtuale sul sistema di destinazione [1,2]	*CHANGE	*EXECUTE
	Programma specificato nel valore di sistema QRMTSIGN sul sistema di destinazione, se presente [1]	*USE	*USE
TFRPASTHR			

[1] Il profilo utente che richiede questa autorizzazione è il profilo che esegue il lavoro batch pass-through. Per il pass-through che ignora il pannello di accesso, il profilo utente è quello specificato nel parametro utente remoto (RMTUSER). Per il pass-through che utilizza la normale procedura di accesso (RMTUSER(* NONE)), l'utente corrisponde al profilo utente predefinito specificato nella voce comunicazioni del sottosistema che gestisce la richiesta di pass-through. Solitamente, questo è QUSER.

[2] Se il pass-through è quello che utilizza la normale procedura di accesso, il profilo utente specificato nel pannello di accesso nel sistema di destinazione deve disporre dell'autorizzazione per questo oggetto.

Comandi distribuzione

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi distribuzione.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDDSTQ (Q)			
ADDDSTRTE (Q)			
ADDDSTSYSN (Q)			
CFGDSTSRV (Q)			
CFGRPDS (Q)			
CHGDSTD [1]	Documento [2]	*CHANGE	*EXECUTE
CHGDSTQ (Q)			
CHGDSTRTE (Q)			
DLTDST [1]			
DSPDSTLOG (Q)	Giornale	*USE	*EXECUTE
	Ricevitore di giornale	*USE	*EXECUTE
DSPDSTSRV (Q)			
HLDDSTQ (Q)			
INZDSTQ (Q)			
QRYDST [1]	File richiesto	*CHANGE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
RCVDST [1]	File richiesto	*CHANGE	*EXECUTE
	Cartella	*CHANGE	*EXECUTE
RLSDSTQ (Q)			
RMVDSTQ (Q)			
RMVDSTRTE (Q)			
RMVDSTSYSN (Q)			
SNDDST [1]	File o documento richiesti	*USE	*EXECUTE
SNDDSTQ (Q)			
WRKDSTQ (Q)			
WRKDPCQ (Q)			

1 Se l'utente sta richiedendo la distribuzione per un altro utente, l'utente deve disporre dell'autorizzazione per effettuare una gestione per conto di un altro utente.

2 Quando la distribuzione è archiviata.

Comandi elenco di distribuzione

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi elenco di distribuzione.

Questi comandi non richiedono le autorizzazioni agli oggetti:			
ADDDSTLE [1] CHGDSTL[1]	CRTDSTL DLTDSTL [1]	DSPDSTL RMVDSTLE [1]	RNMDSTL [1] WRKDSTL [2]

1 È necessario disporre dell'autorizzazione speciale *SECADM o essere il proprietario dell'elenco di distribuzione.

2 Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.

Comandi DLO (Document library object)

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi DLO(document library object).

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDDLOAUT	DLO (Document library object)	*ALL o proprietario	*EXECUTE
CHGDLOAUD [1]			
CHGDLOAUT	DLO (Document library object)	*ALL o proprietario	*EXECUTE
CHGDLOOWN	DLO (Document library object)	Proprietario o autorizzazione speciale *ALLOBJ	*EXECUTE
	Profilo utente vecchio	*DLT	*EXECUTE
	Nuovo profilo utente	*ADD	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGDLOPGP	DLO (Document library object)	Proprietario o autorizzazione speciale *ALLOBJ	*EXECUTE
	Profilo di gruppo principale vecchio	*DLT	*EXECUTE
	Profilo di gruppo principale nuovo	*ADD	*EXECUTE
CHGDOCD [2]	Descrizione documento	*CHANGE	*EXECUTE
CHKDLO [2]	DLO (Document library object)	Come richiesto dalla parola chiave AUT	*EXECUTE
CHKDOC	Documento	*CHANGE	*EXECUTE
	Dizionario di ausilio ortografico	*CHANGE	*EXECUTE
CPYDOC	Dal documento	*USE	*EXECUTE
	Al documento, se si sta sostituendo un documento esistente	*CHANGE	*EXECUTE
	Dalla cartella se la voce al documento è nuova	*CHANGE	*EXECUTE
CRTDOC	Nella cartella	*CHANGE	*EXECUTE
CRTFLR	Nella cartella	*CHANGE	*EXECUTE
DLTDLO [3]	DLO (Document library object)	*ALL	*EXECUTE
DLTDOCL[20]	Elenco documenti	*ALL [4]	*EXECUTE
DMPDLO [15]			
DSPAUTLDLO	Elenco di autorizzazioni	*USE	*EXECUTE
	DLO (Document library object)	*USE	*EXECUTE
DSPDLOAUD[21]	File di emissione, se specificato	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
DSPDLOAUT	DLO (Document library object)	*USE o proprietario	*EXECUTE
DSPDLONAM[22]	DLO (Document library object)	*USE	*EXECUTE
DSPDOC	Documento	*USE	*EXECUTE
DSPFLR	Cartella	*USE	*EXECUTE
EDTDLOAUT	DLO (Document library object)	*ALL o proprietario	*EXECUTE
EDTDOC	Documento	*CHANGE	*EXECUTE
FILDOC [2]	File richiesto	*USE	*EXECUTE
	Cartella	*CHANGE	*EXECUTE
MOVDOC	Dalla cartella, se il documento di origine si trova in una cartella	*CHANGE	*EXECUTE
	Dal documento	*ALL	*EXECUTE
	Cartella di destinazione	*CHANGE	*EXECUTE
MRGDOC [5]	Documento	*USE	*EXECUTE
	Dalla cartella	*USE	*EXECUTE
	Al documento se il documento viene sostituito	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	Dalla cartella se la voce al documento è nuova	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
PAGDOC	Documento	*CHANGE	*EXECUTE
PRTDOC	Cartella	*USE	*EXECUTE
	Documento	*USE	*EXECUTE
	Comandi DLTPF, DLTF e DLTOVR, se viene specificata un'istruzione *INDEX*	*USE	*EXECUTE
	Comandi CRTPF, OVRPRTF, DLTSPLF e DLTOVR, se viene specificata un'istruzione *RUN*	*USE	*EXECUTE
	Salvataggio documento, se SAVOUTPUT (*YES) è specificato	*USE	*EXECUTE
	Salvataggio cartella, se SAVOUTPUT (*YES) è specificato	*USE	*EXECUTE
QRYDOCLIB [2,6]	File richiesto	*USE	*EXECUTE
	Elenco documenti, se è presente	*CHANGE	*EXECUTE
RCLDLO	DLO (Document library object)		
	Documenti interni o tutti i documenti e le cartelle[16]		
RGZDLO	DLO (Document library object)	*CHANGE o proprietario	*EXECUTE
	DLO(*ALL), DLO(*ALL) FLR(*ANY) o DLO(*ALL) FLR(*ANY) MAIL(*YES)[16]		
RMVDLOAUT	DLO (Document library object)	*ALL o proprietario	*EXECUTE
RNMDLO	DLO (Document library object)	*ALL	*EXECUTE
	Nella cartella	*CHANGE	*EXECUTE
RPLDOC [2]	File richiesto	*READ	*EXECUTE
	Documento	*CHANGE	*EXECUTE
RSTDLO (Q)[7, 8, 9]	DLO, in fase di sostituzione	*ALL[10]	*EXECUTE
	Cartella principale, se il DLO è nuovo	*CHANGE[10]	*EXECUTE
	Proprietà del profilo utente, se il DLO è nuovo	*ADD[10]	*EXECUTE
	File di emissione, se specificato	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	Salvataggio file	*USE	*EXECUTE
	File unità ottica (OPTFILE)[17]	*R	Non applicabili
	Prefisso percorso del file unità ottica (OPTFILE)[17]	*X	Non applicabili
	Volume unità ottica[19]	*USE	Non applicabili
	Unità nastro e unità ottica	*USE	*EXECUTE
RSTS36FLR [11,12,14]	Cartella S/36	*USE	*EXECUTE
	Cartella di destinazione	*CHANGE	*EXECUTE
	File unità o descrizione unità	*USE	*EXECUTE
RTVDLONAM[22]	DLO (Document library object)	*USE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
RTVDOC [2]	Documento se si sta effettuando una verifica	*CHANGE	*EXECUTE
	Documento se non si sta effettuando una verifica	*USE	*EXECUTE
	File richiesto	*CHANGE	*EXECUTE
SAVDLO [7,13]	DLO (Document library object)	*ALL[10]	*EXECUTE
	Unità nastro e unità ottica	*USE	*EXECUTE
	File di salvataggio, se vuoto	*USE, *ADD	*EXECUTE
	Salvare il file, se contiene i record	*USE, *ADD, *OBJMGT	*EXECUTE
	File di emissione, se specificato	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	File unità ottica (OPTFILE)[17]	*RW	Non applicabili
	Indirizzario principale del file unità ottica (OPTFILE)[17]	*WX	Non applicabili
	Prefisso percorso del file unità ottica (OPTFILE)[17]	*X	Non applicabili
	Indirizzario root (/) del volume [17, 18]	*RWX	Non applicabili
	Volume unità ottica[19]	*CHANGE	Non applicabili
SAVRSTDLO	Sul sistema di origine, è richiesta la stessa autorizzazione del comando SAVDLO.		
	Sul sistema di destinazione, è richiesta la stessa autorizzazione del comando RSTDLO.		
WRKDOC	Cartella	*USE	
WRKFLR	Cartella	*USE	

1 È necessario disporre dell'autorizzazione speciale *AUDIT.

2 Se l'utente sta effettuando una gestione per conto di un altro utente, viene controllata l'autorizzazione dell'altro utente per l'oggetto.

3 L'utente deve disporre dell'autorizzazione *ALL per tutti gli oggetti nella cartella per cancellare la cartella e i relativi oggetti.

4 Se si dispone dell'autorizzazione speciale *ALLOBJ o *SECADM, non è necessario disporre dell'autorizzazione *ALL per l'elenco librerie documento.

5 L'utente deve disporre dell'autorizzazione per l'oggetto utilizzato come origine di integrazione. Ad esempio, se viene specificato MRGTYPE(*QRY), l'utente deve disporre dell'autorizzazione per l'utilizzo della query specificata per il parametro QRYDFN.

6 Solo gli oggetti che soddisfano i criteri della query e per i quali l'utente dispone dell'autorizzazione *USE vengono restituiti nell'elenco documenti o file di emissione.

7 L'utente deve disporre dell'autorizzazione speciale *SAVSYS, *ALLOBJ o deve essere stato registrato nell'indirizzario di distribuzione del sistema.

8 È necessaria l'autorizzazione speciale *SAVSYS o *ALLOBJ per utilizzare la seguente combinazione di parametri: RSTDLO DLO(*MAIL).

9 È necessario disporre dell'autorizzazione speciale *ALLOBJ per specificare un valore diverso da *NONE per il parametro ALWOBJDIF (Consenso differenze oggetto).

10 Se si dispone dell'autorizzazione speciale *SAVSYS o *ALLOBJ, non è necessario che l'utente disponga di un'autorizzazione specificata.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
[11] È necessario disporre dell'autorizzazione *ALL sul comando, se lo si sta sostituendo. È necessaria l'autorizzazione operativa o su tutti i dati per la cartella se si stanno ripristinando le nuove informazioni sulle cartelle oppure è necessaria l'autorizzazione speciale *ALLOBJ. [12] Se utilizzata per un dizionario dati, viene richiesta solo l'autorizzazione sul comando. [13] È necessario disporre dell'autorizzazione speciale *SAVSYS o *ALLOBJ per utilizzare la seguente combinazione di parametri: • SAVDLO DLO(*ALL) FLR(*ANY) • SAVDLO DLO(*MAIL) • SAVDLO DLO(*CHG) • SAVDLO DLO(*SEARCH) OWNER(not *CURRENT) [14] È necessario essere iscritti nell'indirizzario della distribuzione del sistema se la cartella di origine è una cartella di documenti. [15] È necessario disporre dell'autorizzazione speciale *ALLOBJ per effettuare il dump del DLO.			
[16] È necessario disporre dell'autorizzazione speciale *ALLOBJ o *SECADM. [17] Tale verifica dell'autorizzazione viene effettuata solo quando il formato supporto magnetico dell'unità ottica corrisponde all'UDF (Universal Disk Format). [18] La verifica dell'autorizzazione viene effettuata solo quando si sta ripulendo il volume ottico. [19] I volumi dell'unità ottica non sono oggetti di sistema effettivi. Il collegamento tra il volume dell'unità ottica e l'elenco di autorizzazioni utilizzato per proteggere il volume viene gestito dalla funzione di supporto dell'unità ottica. [20] L'utente deve disporre dell'autorizzazione speciale *ALLOBJ quando OWNER (*ALL) o OWNER (name) e Name è un profilo utente differente dal chiamante.			
[21] L'utente deve disporre dell'autorizzazione speciale a tutti gli oggetti (*ALLOBJ) o al controllo (*AUDIT) per utilizzare questo comando. [22] L'utente deve disporre l'autorizzazione speciale a tutti gli oggetti (*ALLOBJ) per utilizzare questo comando quando si specifica *DST per la classe oggetti da individuare.			

Comandi DNS (Domain Name System)

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi DNS (Domain Name System).

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHKDNSCFG [1]	File di configurazione esistente	*R	
	Percorso al file di configurazione esistente	*X	
	File di emissione esistente	*W	
	Percorso al file di emissione esistente	*X	
	Principale di nuovo file di emissione	*RX	

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHKDNSZNE [1]	File di zona esistente	*R	
	Percorso al file di zona esistente	*X	
	File di emissione esistente	*W	
	Percorso al file di emissione esistente	*X	
	Principale di nuovo file di emissione	*RX	
CRTRNDCCFG [1]	File di origine entropia esistente	*R	
	Percorso al file di origine entropia esistente	*X	
	File di emissione esistente	*W	
	Percorso al file di emissione esistente	*X	
	Principale di nuovo file di emissione	*RX	
RUNDNSUPD	File di immissione batch esistente	*R	
	Percorso al file di immissione batch esistente	*X	
	File chiave esistente	*R	
	Percorso al file chiave esistente	*X	
	File di emissione esistente	*W	
	Percorso al file di emissione esistente	*X	
	Principale di nuovo file di emissione	*RX	
RUNRNDCCMD	File di configurazione RNDC esistente	*R	
	Percorso al file di configurazione RNDC esistente	*X	
	File chiave esistente	*R	
	Percorso al file chiave esistente	*X	
	File di emissione esistente	*W	
	Percorso al file di emissione esistente	*X	
	Principale di nuovo file di emissione	*RX	
STRDIGQRY	File di immissione batch esistente	*R	
	Percorso al file di immissione batch esistente	*X	
	File chiave affidabile esistente	*R	
	Percorso al file chiave affidabile esistente	*X	
	File chiave esistente	*R	
	Percorso al file chiave esistente	*X	
	File di emissione esistente	*W	
	Percorso al file di emissione esistente	*X	
	Principale di nuovo file di emissione	*RX	
STRHOSTQRY	File di emissione esistente	*W	
	Percorso al file di emissione esistente	*X	
	Principale di nuovo file di emissione	*RX	

[1] È necessario disporre dell'autorizzazione speciale *IOSYSCFG per eseguire questo comando.

Comandi DBCS (Double-byte character set)

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi DBCS (Double-byte character set).

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CPYIGCTBL	Tabella ordine DBCS (*IN)	*ALL	*EXECUTE
	Tabella ordine DBCS (*OUT)	*USE	*EXECUTE
CRTIGCDCT	Dizionario di conversione DBCS		*READ, *ADD
DLTIGCDCT	Dizionario di conversione DBCS	*OBJEXIST	*EXECUTE
DLTIGCSRT	Tabella ordine DBCS	*OBJEXIST	*EXECUTE
DLTIGCTBL	Tabella ordine DBCS	*OBJEXIST	*EXECUTE
DSPIGCDCT	Dizionario di conversione DBCS	*USE	*EXECUTE
EDTIGCDCT	Dizionario di conversione DBCS	*USE, *UPD	*EXECUTE
	Dizionario utente	*ADD, *DLT	*EXECUTE
STRCGU	Tabella ordine DBCS	*CHANGE	*EXECUTE
	Tabella ordine DBCS	*CHANGE	*EXECUTE
STRFMA	Tabella font DBCS, se è specificata l'opzione copia in	*OBJOPR, *READ *ADD, *UPD	*EXECUTE
	Tabella font DBCS, se è specificata l'opzione copia da	*OBJOPR, *READ	*EXECUTE
	File di lavoro supporto gestione font (QGPL/QAFSVDF)	*CHANGE	*EXECUTE

Comandi di descrizione editazione

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi di descrizione editazione.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTEDTD	Descrizione editazione		*EXECUTE, *ADD
DLTEDTD	Descrizione editazione	*OBJEXIST	*EXECUTE
DSPEDTD	Descrizione editazione	*OBJOPR	*EXECUTE
WRKEDTD [1]	Descrizione editazione	Qualsiasi autorizzazione	*USE

1 Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.

Comandi variabile di ambiente

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi variabile di ambiente.

Questi comandi non richiedono le autorizzazioni per l'oggetto.			
ADDENVVAR[1]	CHGENVVAR [1]	RMVENVVAR[1]	WRKENVVAR[1]

1 Per aggiornare le variabili di ambiente a livello sistema, è necessario disporre dell'autorizzazione speciale *JOBCTL.

Comandi configurazione LAN estesa senza fili

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi configurazione LAN estesa senza fili.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDEWCBCDE	File di origine	*USE	*EXECUTE
ADDEWCM	File di origine	*USE	*EXECUTE
ADDEWCPTCE	File di origine	*USE	*EXECUTE
ADDEWLM	File di origine	*USE	*EXECUTE
CHGEWCBCDE	File di origine	*USE	*EXECUTE
CHGEWCM	File di origine	*USE	*EXECUTE
CHGEWCPTCE	File di origine	*USE	*EXECUTE
CHGEWLM	File di origine	*USE	*EXECUTE
DSPEWCBCDE	File di origine	*USE	*EXECUTE
DSPEWCM	File di origine	*USE	*EXECUTE
DSPEWCPTCE	File di origine	*USE	*EXECUTE
DSPEWLM	File di origine	*USE	*EXECUTE
RMVEWCBCDE	File di origine	*USE	*EXECUTE
RMVEWCPTCE	File di origine	*USE	*EXECUTE

Comandi file

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi file.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDICFDEVE	File ICF	*OBJOPR, *OBJMGT	*EXECUTE
ADDLFM	File logico	*OBJOPR, *OBJMGT o *OBJALTER	*EXECUTE, *ADD
	File a cui si fa riferimento nel parametro DTAMBRS, quando il file logico è con chiave	*OBJOPR, *OBJMGT o *OBJALTER	*EXECUTE
	File a cui si fa riferimento nel parametro DTAMBRS, quando il file logico non è con chiave	*OBJOPR	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDPFCST	File dipendente, se è specificato TYPE(*REFCST)	*OBJMGT o *OBJALTER	*EXECUTE
	File principale, se è specificato TYPE(*REFCST)	*OBJMGT o *OBJREF	*EXECUTE
	File, se è specificato TYPE(*UNQCST) o TYPE(*PRIKEY)	*OBJMGT	*EXECUTE
ADDPFM	File fisico	*OBJOPR, *OBJMGT o *OBJALTER	*EXECUTE, *ADD
ADDPFTRG	File fisico, per inserire il trigger	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	File fisico, per cancellare il trigger	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	File fisico, per aggiornare il trigger	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Programma trigger	*EXECUTE	*EXECUTE
CHGDDMF	File DDM	*OBJOPR, *OBJMGT	*EXECUTE
	Descrizione unità [7]	*CHANGE	
CHGDKTF	File minidisco	*OBJOPR, *OBJMGT	*EXECUTE
	Unità se il nome unità è specificato nel comando	*OBJOPR	*EXECUTE
CHGDSPF	File di visualizzazione	*OBJOPR, *OBJMGT	*EXECUTE
	Unità se il nome unità è specificato	*OBJOPR	*EXECUTE
CHGDTA	File di dati	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	Programma	*USE	*EXECUTE
	File di visualizzazione	*USE	*EXECUTE
CHGICFDEVE	File ICF	*OBJOPR, *OBJMGT	*EXECUTE
CHGICFF	File ICF	*OBJOPR, *OBJMGT	*EXECUTE
CHGLF	File logico	*OBJMGT o *OBJALTER	*EXECUTE
CHGLFM	File logico	*OBJMGT o *OBJALTER	*EXECUTE
CHGPF	File fisico	*OBJMGT o *OBJALTER	*EXECUTE
CHGPFCST	File dipendente	*OBJMGT o *OBJALTER	*EXECUTE
CHGPFM	File fisico	*OBJMGT o *OBJALTER	*EXECUTE
CHGPFTRG	File fisico	*OBJMGT o *OBJALTER	*EXECUTE
CHGPRTF	Emissione di stampa	*OBJOPR, *OBJMGT	*EXECUTE
	Unità se il nome unità è specificato	*OBJOPR	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGSAVF	Salvataggio file	*OBJOPR e (*OBJMGT o *OBJALTER).	*EXECUTE
CHGSRCPF	File fisico di origine	*OBJMGT o *OBJALTER	*EXECUTE
CHGTAPF	File su nastro	*OBJOPR, *OBJMGT	*EXECUTE
	Unità se il nome unità è specificato	*OBJOPR	*EXECUTE
CLRPFM	File fisico	*OBJOPR, *OBJMGT o *OBJALTER, *DLT	*EXECUTE
CLRSAVF	Salvataggio file	*OBJOPR, *OBJMGT	*EXECUTE
CPYF	Da file	*OBJOPR, *READ	*EXECUTE
	A file (file unità)	*OBJOPR, *READ	*EXECUTE
	A file (file fisico)	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	Basato sul file se Da file è un file logico	*READ	*EXECUTE
CPYFRMDKT	Da file	*OBJOPR, *READ	*EXECUTE
	A file (file unità)	*OBJOPR, *READ	*EXECUTE
	A file (file fisico)	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
CPYFRMIMPF	Da file	*OBJOPR, *READ	*USE
	A file (file unità)	*OBJOPR, *READ	*USE
	A file (file fisico)	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	Basato sul file se Da file è un file logico	*READ	*USE
	Comando CRTDDMF	*USE	*USE
CPYFRMQRYF [1]	Da file	*OBJOPR, *READ	*EXECUTE
	A file (file unità)	*OBJOPR, *READ	*EXECUTE
	A file (file fisico)	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
CPYFRMSTMF	File di flusso	*R	
	Indirizzari nel prefisso nome percorso file di flusso	*X	
	File di database di destinazione, se è specificato MBROPT(*ADD)	*WX	*X
	File di database di destinazione, se è specificato MBROPT(*REPLACE o *NONE)	*WX, *OBJMGT	*X
	File di database di destinazione, se viene creato un nuovo membro	*WX	*X, *ADD
	Tabella di conversione *TBL utilizzata per convertire i dati	*R	*X
	File di salvataggio di destinazione presente	*RWX, *OBJMGT	*X
	File di salvataggio di destinazione creato		*RWX

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CPYFRMTAP	Da file	*OBJOPR, *READ	*EXECUTE
	A file (file unità)	*OBJOPR, *READ	*EXECUTE
	A file (file fisico)	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
CPYSRCF	Da file	*OBJOPR, *READ	*EXECUTE
	A file (file unità)	*OBJOPR, *READ	*EXECUTE
	A file (file fisico)	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
CPYTODKT	A file e Da file	*OBJOPR, *READ	*EXECUTE
	Unità se il nome unità è specificato nel comando	*OBJOPR, *READ	*EXECUTE
	Basato sul file fisico se Da file è un file logico	*READ	*EXECUTE
CPYTOIMPF	Da file	*OBJOPR, *READ	*USE
	A file (file unità)	*OBJOPR, *READ	*USE
	A file (file fisico)	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	Basato sul file se Da file è un file logico	*READ	*USE
	Comando CRTDDMF	*USE	*USE
CPYTOSTMF	File di database o di salvataggio	*RX	*X
	File di flusso, se è già presente	*W	
	Indirizzario principale file di flusso, se il file di flusso non è presente	*WX	
	Prefisso nome percorso file di flusso	*X	
	File di database e file di flusso, se se è specificato AUT(*FILE) o AUT(*INDIRFILE)	*OBJMGT	
	Tabella di conversione *TBL utilizzata per convertire i dati	*R	*X
CPYTOTAP	A file e Da file	*OBJOPR, *READ	*EXECUTE
	Unità se il nome unità è specificato	*OBJOPR, *READ	*EXECUTE
	Basato sul file fisico se Da file è un file logico	*READ	*EXECUTE
CRTDDMF	File DDM: REPLACE(*NO)		*READ, *ADD
	File DDM: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Descrizione unità [7]	*CHANGE	
CRTDKTF	Unità se il nome unità è specificato	*OBJOPR	*EXECUTE
	File minidisco: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	File minidisco: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD, *EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTDSPF	File di origine	*USE	*EXECUTE
	Unità se il nome unità è specificato	*OBJOPR	*EXECUTE
	File specificato nelle parole chiave REF e REFFLD	*OBJOPR	*EXECUTE
	File di visualizzazione: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	File di visualizzazione: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD, *EXECUTE
CRTICFF	File di origine	*USE	*EXECUTE
	File specificato nelle parole chiave REF e REFFLD	*OBJOPR	*EXECUTE
	File ICF: REPLACE(*NO)		*READ, *ADD
	File ICF: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
CRTLF	File di origine	*USE	*EXECUTE
	File specificato sulla parola chiave PFILE o JFILE, quando il file logico è con chiave	*OBJOPR, *OBJMGT o *OBJALTER	*EXECUTE
	File specificato sulla parola chiave PFILE o JFILE, quando il file logico non è con chiave	*OBJOPR	*EXECUTE
	Files specificato sulle parole chiave FORMAT e REFACCPTH	*OBJOPR	*EXECUTE
	Tabelle specificate nella parola chiave ALTSEQ	*OBJOPR	*EXECUTE
	File logico		*EXECUTE, *ADD
	File a cui si fa riferimento nel parametro DTAMBRS, quando il file logico è con chiave	*OBJOPR, *OBJMGT o *OBJALTER	*EXECUTE
	File a cui si fa riferimento nel parametro DTAMBRS, quando il file logico non è con chiave	*OBJOPR	*EXECUTE
CRTPF	File di origine	*USE	*EXECUTE
	File specificati nelle parole chiave FORMAT e REFFLD e le tabelle specificate nella parola chiave ALTSEQ	*OBJOPR	*EXECUTE
	File fisico		*EXECUTE, *ADD
CRTPRTF	File di origine	*USE	*EXECUTE
	Unità se il nome unità è specificato	*OBJOPR	*EXECUTE
	File specificato nelle parole chiave REF e REFFLD	*OBJOPR	*EXECUTE
	Emissione di stampa: Replace(*NO)		*READ, *ADD, *EXECUTE
	Emissione di stampa: Replace(*YES)	Fare riferimento alle regole generali.	*READ, *ADD, *EXECUTE
CRTSAVF	Salvataggio file		*READ, *ADD, *EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTSRCPF	File fisico di origine		*READ, *ADD, *EXECUTE
CRTS36DSPF	File di origine a file quando TOMBR non è *NONE	*ALL	*CHANGE
	File di origine QS36SRC	*USE	*EXECUTE
	File di visualizzazione: REPLACE(*NO)		*READ, *ADD
	File di visualizzazione: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Comando CRTDSPF (Creazione file di visualizzazione)	*OBJOPR	*EXECUTE
CRTTAPF	File su nastro: REPLACE(*NO)		*READ, *ADD
	File su nastro: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Unità se il nome unità è specificato	*OBJOPR	*EXECUTE
DLTF	File	*OBJOPR, *OBJEXIST	*EXECUTE
DSPCPCST	File di database con restrizione in sospeso	*OBJOPR, *READ	*EXECUTE
DSPDBR	File di database	*OBJOPR	*EXECUTE
	File di emissione, se specificato	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
DSPDDMF	File DDM	*OBJOPR	
DSPDTA	File di dati	*USE	*EXECUTE
	Programma	*USE	*EXECUTE
	File di visualizzazione	*USE	*EXECUTE
DSPFD [2]	File	*OBJOPR	*EXECUTE
	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	Il file è un file fisico ed è stato specificato TYPE(*ALL, *MBR, OR *MBRLST)	Un'autorizzazione dati diversa da *EXECUTE	*EXECUTE
DSPFFD	File	*OBJOPR	*EXECUTE
	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
DSPPFM	File fisico	*USE	*EXECUTE
DSPSAVF	Salvataggio file	*USE	*EXECUTE
EDTCPCST	Area dati, come specificato sulla parola chiave NFYOBJ per il comando STRCMTCTL associato.	*CHANGE	*EXECUTE
	File, come specificato sulla parola chiave NFYOBJ per il comando STRCMTCTL associato.	*OBJOPR, *ADD	*EXECUTE
GENCAT	File di database	*OBJOPR e un'autorizzazione dati diversa da *EXECUTE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
INZPFM	File fisico, quando viene specificato RECORD(*DFT)	*OBJOPR, *OBJMGT o *OBJALTER, *ADD	*EXECUTE
	File fisico, quando viene specificato RECORD(*DLT)	*OBJOPR, *OBJMGT o *OBJALTER, *ADD, *DLT	*EXECUTE
MRGSRC	File di destinazione	*CHANGE, *OBJMGT	*CHANGE
	File di manutenzione	*USE	*EXECUTE
	File root	*USE	*EXECUTE
OPNDBF	File di database	*OBJOPR e un'autorizzazione dati diversa da *EXECUTE	*EXECUTE
OPNQRYF	File di database	*OBJOPR e un'autorizzazione dati diversa da *EXECUTE	*EXECUTE
PRTTRGPGM [11]			
RGZPFM	File contenente il membro	*OBJOPR, *OBJMGT o *OBJALTER, *READ, *ADD, *UPD, *DLT, *EXECUTE	*EXECUTE
RMVICFDEVE	File ICF	*OBJOPR, *OBJMGT	*EXECUTE
RMVM	File contenente il membro	*OBJEXIST, *OBJOPR	*EXECUTE
RMVPFCST	File	*OBJMGT o *OBJALTER	*EXECUTE
RMVPFTRG	File fisico	*OBJALTER, *OBJMGT	*EXECUTE
RNMM	File contenente il membro	*OBJOPR, *OBJMGT	*EXECUTE, *UPD
RSTS36F [4] (Q)	A file	*ALL	Fare riferimento alle regole generali.
	Da file	*USE	*EXECUTE
	Basato sul file fisico, se il file ripristinato è un file logico (alternativo)	*CHANGE	*EXECUTE
	Descrizione unità per il minidisco o nastro	*USE	*EXECUTE
RTVMBRD	File	*USE	*EXECUTE
SAVSAVFDTA	Descrizione nastro, minidisco o unità ottica	*USE	*EXECUTE
	Salvataggio file	*USE	*EXECUTE
	File di salvataggio/ripristino unità ottica [8] (se precedentemente ne era presente uno)	*RW	Non applicabili
	Indirizzario principale di OPTFILE [8]	*WX	Non applicabili
	Prefisso percorso di OPTFILE[8]	*X	Non applicabili
	Indirizzario root (/) del Volume unità ottica [8,9]	*RWX	Non applicabili
	Volume unità ottica[10]	*CHANGE	Non applicabili

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
SAVS36F	Da file	*USE	*EXECUTE
	File di destinazione, quando si tratta di un file fisico	*ALL	Fare riferimento alle regole generali.
	File unità o descrizione unità	*USE	*EXECUTE
SAVS36LIBM	File di destinazione, quando si tratta di un file fisico	*ALL	Fare riferimento alle regole generali.
	Da file	*USE	*EXECUTE
	File unità o descrizione unità	*USE	*EXECUTE
STRAPF [3]	File di origine	*OBJMGT, *CHANGE	*READ, *ADD
	Comandi CRTPF, CRTLF, ADDPFM, ADDLFM e RMVM	*USE	*EXECUTE
STRDFU [3]	Programma (se è presente l'opzione di creazione programma)		*READ, *ADD
	Programma (se è presente l'opzione di modifica o cancellazione programma)	*OBJEXIST	*READ, *ADD
	File (se è presente l'opzione di modifica o visualizzazione dati)	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	File (se è presente l'opzione di visualizzazione dati)	*READ	*EXECUTE
UPDDTA	File	*CHANGE	*EXECUTE
WRKDDMF [3]	File DDM	*OBJOPR, *OBJMGT, *OBJEXIST	*READ, *ADD
WRKF [3,5]	File	*OBJOPR	*USE
WRKPFCST[3]			*EXECUTE

1 Il comando CPYFRMQRYF utilizza un parametro FROMOPNID piuttosto di FROMFILE. È necessario che un utente disponga dell'autorizzazione sufficiente ad eseguire il comando OPNQRYF prima di eseguire il comando CPYFRMQRYF. Se CRTFILE(*YES) è specificato sul comando CPYFRMQRYF, il primo file specificato sul parametro OPNQRYF FILE corrispondente viene considerato come voce Da file quando vengono stabilite le autorizzazioni per il nuovo A file.

2 È necessaria l'autorizzazione operativa o è necessario essere il proprietario del file.

3 Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

4 Se viene creato un nuovo file ed è presente un titolare autorizzazione per tale file, l'utente deve disporre dell'autorizzazione *ALL per il titolare autorizzazione o deve essere il proprietario del titolare autorizzazione. Se non è presente alcun titolare autorizzazione, il proprietario del file è l'utente che ha immesso il comando RSTS36F e l'autorizzazione pubblica è *ALL.

5 È necessaria un'autorizzazione per l'oggetto.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
[6]	È necessario disporre dell'autorizzazione speciale *ALLOBJ.		
[7]	L'autorizzazione viene verificata quando si utilizza il file DDM.		
[8]	Tale verifica dell'autorizzazione viene effettuata solo quando il formato supporto magnetico dell'unità ottica corrisponde all'UDF (Universal Disk Format).		
[9]	Tale verifica dell'autorizzazione viene effettuata solo se si sta ripulendo il volume dell'unità ottica.		
[10]	I volumi dell'unità ottica non sono oggetti di sistema effettivi. Il collegamento tra il volume dell'unità ottica e l'elenco di autorizzazioni utilizzato per proteggere il volume viene gestito dalla funzione di supporto dell'unità ottica.		
[11]	È necessario disporre dell'autorizzazione speciale *ALLOBJ o *AUDIT per utilizzare questo comando.		

Comandi filtro

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi filtro.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDALRACNE	Filtro	*USE, *ADD	*EXECUTE
ADDALRSLTE	Filtro	*USE, *ADD	*EXECUTE
ADDPRBACNE	Filtro	*USE, *ADD	*EXECUTE
ADDPRBSLTE	Filtro	*USE, *ADD	*EXECUTE
CHGALRACNE	Filtro	*USE, *UPD	*EXECUTE
CHGALRSLTE	Filtro	*USE, *UPD	*EXECUTE
CHGFTR	Filtro	*OBJMGT	*EXECUTE
CHGPRBACNE	Filtro	*USE, *UPD	*EXECUTE
CHGPRBSLTE	Filtro	*USE, *UPD	*EXECUTE
CRTFTR	Filtro		*READ, *ADD
DLTFTR	Filtro	*OBJEXIST	*EXECUTE
RMVFTRACNE	Filtro	*USE, *DLT	*EXECUTE
RMVFTRSLTE	Filtro	*USE, *DLT	*EXECUTE
WRKFTR [1]	Filtro	Qualsiasi autorizzazione	*EXECUTE
WRKFTRACNE [1]	Filtro	*USE	*EXECUTE
WRKFTRSLTE [1]	Filtro	*USE	*EXECUTE
[1]	Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.		

Comandi Finance

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi finance.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
SBMFNCJOB (Q)	Descrizione lavoro e coda messaggi [1]	*OBJOPR	*EXECUTE
SNDFNCIMG (Q)	Descrizione lavoro e coda messaggi [1]	*OBJOPR	*EXECUTE
WRKDEVTBL (Q)	Descrizione unità [1]	Almeno un'autorizzazione dati	*EXECUTE
WRKPGMTBL (Q)			
WRKUSRTBL (Q)			

[1] Il profilo utente QFNC deve disporre di questa autorizzazione.

Comandi i5/OS graphical operations

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi i5/OS graphical operations.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGFCNUSG[5]			
DSPFCNUSG			
EDTWSOAUT	Oggetto stazione di lavoro [1]	*OBJMGT [2,3,4]	*EXECUTE
GRTWSOAUT	Oggetto stazione di lavoro [1]	*OBJMGT [2,3,4]	*EXECUTE
RVKWSOAUT	Oggetto stazione di lavoro [1]	*OBJMGT [2,3,4]	*EXECUTE
SETCSTDTA	Profilo utente Copia da	*CHANGE	*EXECUTE
	Profilo utente Copia in	*CHANGE	*EXECUTE
WRKFCNUSG			

[1] L'oggetto stazione di lavoro è un oggetto interno creato quando si installa il dispositivo i5/OS Graphical Operations. Viene inviato con l'autorizzazione pubblica *USE.

[2] È necessario essere il proprietario o disporre dell'autorizzazione *OBJMGT e delle autorizzazioni concesse o revocate.

[3] È necessario essere il proprietario o disporre dell'autorizzazione *ALLOBJ per assegnare l'autorizzazione *OBJMGT o *AUTLMGT.

[4] Per proteggere l'oggetto stazione di lavoro con un elenco di autorizzazioni o rimuovere l'elenco di autorizzazioni, è necessario:

- Essere il proprietario dell'oggetto stazione di lavoro.
- Disporre dell'autorizzazione *ALL per l'oggetto stazione di lavoro.
- Disporre dell'autorizzazione speciale *ALLOBJ.

[5] È necessario disporre dell'autorizzazione speciale di amministratore della riservatezza (*SECADM) per modificare l'utilizzo di una funzione.

Comandi serie di simboli grafici

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi serie di simboli grafici.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTGSS	File di origine	*USE	*EXECUTE
	Serie di simboli grafici		*READ, *ADD
DLTGSS	Serie di simboli grafici	*OBJEXIST	*EXECUTE
WRKGSS [1]	Serie di simboli grafici	*OBJOPR	*USE
[1] È necessario essere proprietario o disporre di un'autorizzazione per l'oggetto.			

Comandi server host

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi server host.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Questi comandi non richiedono le autorizzazioni per l'oggetto.			
ENDHOSTSVR (Q)		STRHOSTSVR (Q)	

Comandi catalogo immagini

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi catalogo immagini.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Tipo oggetto	Autorizzazione necessaria	
			Per oggetto	**Per libreria[1]**
ADDIMGCLGE	Catalogo immagini	*IMGCLG	*CHANGE	*EXECUTE
	Prefisso percorso indirizzario del catalogo immagini	*DIR	*X	
	Nome unità quando si specifica FROMDEV	*DEVD	*USE	
	File di immagini quando si specifica FROMFILE	*STMF	*R, *OBJMGT	
	Prefisso percorso file di immagini quando si specifica FROMFILE	*DIR	*X	
	Indirizzario principale del file di immagini quando si specifica FROMFILE	*DIR	*RX	
CHGIMGCLG	Catalogo immagini	*IMGCLG	*CHANGE	*EXECUTE
	Prefisso percorso indirizzario del catalogo immagini	*DIR	Fare riferimento alle regole generali.	
	Nuovo prefisso percorso dell'indirizzario del catalogo immagini quando si specifica il parametro DIR	*DIR	Fare riferimento alle regole generali.	

Comando	Oggetto di riferimento	Tipo oggetto	Autorizzazione necessaria	
			Per oggetto	Per libreria[1]
CHGIMGCLGE	Catalogo immagini	*IMGCLG	*CHANGE	*EXECUTE
	Prefisso percorso indirizzario del catalogo immagini	*DIR	Fare riferimento alle regole generali.	
CRTIMGCLG	QUSRSYS	*LIB		*READ, *ADD
	Catalogo immagini se si specifica DIR(*REFIMGCLG)	*IMGCLG	*USE	*OBJOPR, *READ, *ADD, *EXECUTE
	Prefisso percorso indirizzario del catalogo immagini[2]	*DIR	Fare riferimento alle regole generali.	
DLTIMGCLG	Catalogo immagini	*IMGCLG	*OBJEXIST	*EXECUTE
	Prefisso percorso indirizzario del catalogo immagini	*DIR	Fare riferimento alle regole generali.	
LODIMGCLG	Catalogo immagini	*IMGCLG	*USE	*EXECUTE
	Catalogo immagini quando si specifica WRTPTC(*ALL) o WRTPTC(*NONE)	*IMGCLG	*CHANGE	*EXECUTE
	Unità virtuale	*DEVD	*USE	
	Prefisso percorso indirizzario del catalogo immagini	*DIR	Fare riferimento alle regole generali.	
LODIMGCLGE	Catalogo immagini	*IMGCLG	*USE	*EXECUTE
	Prefisso percorso indirizzario del catalogo immagini	*DIR	Fare riferimento alle regole generali.	
RMVIMGCLGE	Catalogo immagini	*IMGCLG	*CHANGE	*EXECUTE
	Prefisso percorso indirizzario del catalogo immagini	*DIR	Fare riferimento alle regole generali.	
RTVIMGCLG	Catalogo immagini	*IMGCLG	*USE	*EXECUTE
	Descrizione unità DEV se si specifica il parametro DEV	*DEVD	*USE	
VFYIMGCLG	Catalogo immagini	*IMGCLG	*USE	*EXECUTE
	Unità virtuale	*DEVD	*USE	
	Prefisso percorso indirizzario del catalogo immagini	*DIR	Fare riferimento alle regole generali.	
WRKIMGCLG	Catalogo immagini	*IMGCLG	*USE	*EXECUTE
WRKIMGCLGE	Catalogo immagini	*IMGCLG	*USE	*EXECUTE

[1] La libreria in cui si trovano gli oggetti del catalogo immagini è QUSRSYS.

[2] Se si crea un indirizzario, è necessaria anche l'autorizzazione alla scrittura (*W) nell'indirizzario che contiene il nuovo indirizzario.

Comandi dell'IFS (Integrated file system)

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi dell'IFS (Integrated file system).

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
ADDLNK	Oggetto quando si specifica LNKTYPE(*HARD)	*STMF	QOpenSys, ″root″ (/),UDFS	*OBJEXIST
	Principale di nuovo collegamento	*DIR	QOpenSys, ″root″ (/), UDFS	*WX
	Prefisso percorso	Fare riferimento alle regole generali.		
CHGATR	Oggetto quando si imposta un attributo diverso da *USECOUNT, *ALWCKPWRT, *DISKSTGOPT,*MAINSTGOPT, *ALWSAV, *SCAN, *CRTOBJSCAN, *SETUID, *SETGID, *RSTRDRNMUNL, *CRTOBJAUD	Qualunque valore	Tutti eccetto QSYS.LIB	*W
	Oggetto quando si imposta *USECOUNT, *DISKSTGOPT, *MAINSTGOPT, *ALWSAV	Qualunque valore	Tutti eccetto QSYS.LIB	*OBJMGT
		*FILE	QSYS.LIB	*OBJOPR, *OBJMGT
		*MBR	QSYS.LIB	*X, *OBJMGT (autorizzazione ereditata da *FILE principale)
		altro	QSYS.LIB	*OBJMGT
	Oggetto quando si imposta *ALWCKPWRT	Qualunque valore	Tutto	*OBJMGT
	Indirizzario contenente gli oggetti, quando specificato SUBTREE(*ALL)	Qualsiasi indirizzario	Tutto	*RX
	Oggetto quando si impostano i seguenti attributi: *CRTOBJSCAN o *SCAN[26]	*DIR e *STMF	QOpenSys, ″root″ (/), UDFS	
	Oggetto quando si impostano i seguenti attributi: *SETUID, *SETGID, *RSTDRNMUNL	Qualunque valore	Tutti eccetto QSYS.LIB e QDLS	Proprietà [15]
	*CRTOBJAUD[9]			
	Prefisso percorso [9]	Fare riferimento alle regole generali.		
CHGAUD [4]				

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
CHGAUT	Oggetto	Tutto	QOpenSys, "root" (/), UDFS	Proprietà [15]
			QSYS.LIB, QOPT[11]	Proprietario o *ALLOBJ
			QDLS	Proprietario, *ALL o *ALLOBJ
				*OBJMGT
	Volume ottico	*DDIR	QOPT[8]	*CHANGE
	Indirizzario contenente gli oggetti, quando si specifica SUBTREE(*ALL)	Qualsiasi indirizzario o libreria	Tutti	*RX
CHGCURDIR	Oggetto	Qualsiasi indirizzario		*R
	Volume ottico	*DDIR	QOPT[8]	*X
	Prefisso percorso	Fare riferimento alle regole generali.		
CHGOWN [24]	Oggetto	Tutto	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		Tutto	QOpenSys, "root" (/), UDFS	Proprietario e *OBJEXIST[15]
		Tutto	QDLS	Proprietario o *ALLOBJ
			QOPT[11]	Proprietario o *ALLOBJ
CHGOWN [24]	Profilo utente del precedente proprietario—tutti eccetto QOPT, QDLS	*USRPRF	Tutto	*DLT
	Profilo utente del precedente proprietario—tutti eccetto QOPT	*USRPRF	Tutto	*ADD
	Volume ottico	*DDIR	QOPT[8]	*CHANGE
	Indirizzario contenente gli oggetti, quando si specifica SUBTREE(*ALL)	Qualsiasi indirizzario o libreria	Tutti	*RX
CHGPGP	Oggetto	Tutto	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		Tutto	QOpenSys, "root" (/), UDFS	Proprietario[5, 15]
		Tutto	QDLS	Proprietario o *ALLOBJ
			QOPT[11]	Proprietario o *ALLOBJ

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
CHGPGP	Profilo utente del gruppo principale—tutti eccetto QOPT	*USRPRF	Tutto	*DLT
	Profilo utente del gruppo principale—tutti eccetto QOPT	*USRPRF	Tutto	*ADD
	Volume ottico	*DDIR	QOPT[8]	*CHANGE
	Indirizzario contenente gli oggetti, quando si specifica SUBTREE(*ALL)	Qualsiasi indirizzario o libreria	Tutti	*RX
CHKIN	Oggetto, se l'utente che ha effettuato il controllo in uscita.	*STMF	QOpenSys, "root" (/), UDFS	*W
		*DOC	QDLS	*W
	Oggetto, se non l'utente che ha effettuato il controllo in uscita.	*STMF	QOpenSys, "root" (/), UDFS	Proprietà *ALL o *ALLOBJ
		*DOC	QDLS	Proprietà *ALL o *ALLOBJ
	Percorso, se non l'utente che ha effettuato il controllo in uscita	*DIR	QOpenSys, "root" (/), UDFS	*X
	Indirizzario contenente gli oggetti, quando si specifica SUBTREE(*ALL)	Qualsiasi indirizzario	Tutti	*RX
	Prefisso percorso	Fare riferimento alle regole generali.		
CHKOUT	Oggetto	*STMF	QOpenSys, "root" (/), UDFS	*W
		*DOC	QDLS	*W
	Indirizzario contenente gli oggetti, quando si specifica SUBTREE(*ALL)	Qualsiasi indirizzario	Tutti	*RX
	Prefisso percorso	Fare riferimento alle regole generali.		

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
CPY[25]	Oggetto copiato, oggetto origine	Qualunque valore	QOpenSys, "root" (/), UDFS	*R e *OBJMGT o proprietario
		*DOC	QDLS	*RWX e *ALL o proprietario
		*MBR	QSYS.LIB	Nessuna
		altri	QSYS.LIB	*RX, *OBJMGT
		*DSTMF	QOPT[11]	*R
	Oggetto destinazione quando specificato REPLACE(*YES) (se oggetto destinazione già esistente)	Qualunque valore	Tutti[10]	*W, *OBJEXIST, *OBJMGT
		*DSTMF	QOPT[11]	*W
		*LIB	QSYS.LIB	*RW, *OBJMGT, *OBJEXIST
		*FILE (PF o LF)	QSYS.LIB	*RW, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*RWX, *ALL
	Indirizzario copiato contenente gli oggetti quando specificato SUBTREE(*ALL), in modo che il contenuto venga copiato	*DIR	QOpenSys, "root" (/), UDFS	*RX, *OBJMGT
CPY[25]	Percorso (destinazione), indirizzario principale dell'oggetto destinazione	*FILE	QSYS.LIB	*RX, *OBJMGT
		*LIB	QSYS.LIB	*RX, *ADD
		*DIR	QOpenSys, "root" (/), UDFS	*WX
		*FLR	QDLS	*RWX
		*DDIR	QOPT[11]	*WX
	Volume ottico origine	*DDIR	QOPT[8]	*USE
	Volume ottico destinazione	*DDIR	QOPT[8]	*CHANGE
CPY[25]	Indirizzario principale dell'oggetto origine	*DIR	QOpenSys, "root" (/), UDFS	*X
		*FLR	QDLS	*X
		Altri	QSYS.LIB	*RX
		*DDIR	QOPT[11]	*X
	Prefisso percorso (destinazione)	*LIB	QSYS.LIB	*WX
		*DIR	QOpenSys, "root" (/), UDFS	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
	Prefisso percorso (oggetto origine)	*DDIR	QOPT[11]	*X
CPYFRMSTMF	Consultare "Comandi file" a pagina 406			

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
CPYTOSTMF	Consultare "Comandi file" a pagina 406			
CRTDIR[21, 22]	Indirizzario principale	*DIR	QOpenSys, "root" (/), UDFS	*WX
		*FLR	QDLS	*CHANGE
		*FILE	QSYS.LIB	*RX, *ADD
		Qualunque valore		*ADD
		*DDIR	QOPT[11]	*WX
CRTDIR	Prefisso percorso	Fare riferimento alle regole generali.		
	Volume ottico	*DDIR	QOPT[8]	*CHANGE
CVTDIR (Q)[16]				
DSPAUT	Oggetto	Tutto	QDLS	*ALL
		Tutto	Tutti gli altri	*OBJMGT o proprietà
		ALL	QOPT[11]	Nessuna
	Volume ottico	*DDIR	QOPT[8]	*USE
	Prefisso percorso	Fare riferimento alle regole generali.		
DSPCURDIR	Prefisso percorso	*DIR	QOpenSys, "root" (/), UDFS	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*DIR		*R
		*DDIR	QOPT[11]	*RX
DSPCURDIR	Indirizzario corrente	*DIR	QOpenSys, "root" (/), UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DIR		*R
		*DDIR	QOPT[11]	*X
	Volume ottico	*DDIR*	QOPT[8]	*USE
DSPF	File di database	*FILE	QSYS.LIB	*USE
	Libreria file database	*LIB	QSYS.LIB	*EXECUTE
	File di flusso	*STMF	QOpenSys, "root" (/), UDFS	*R
		*USRSPC	QSYS.LIB	*USE
	Prefisso percorso	Fare riferimento alle regole generali.		

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
DSPLNK	Qualunque valore	Qualunque valore	"root" (/), QOpenSys, UDFS QSYS.LIB[27], QDLS, QOPT[11]	Nessuna
	File, Opzione 12 (Gestione collegamenti)	*STMF, *SYMLNK, *DIR,*BLKSF, *SOCKET	"root" (/), QOpenSys, UDFS	*R
DSPLNK	Oggetto collegamento simbolico	*SYMLNK	"root" (/), QOpenSys, UDFS	Nessuna
	Volume ottico	*DDIR	QOPT[8]	*USE
	Indirizzario principale dell'oggetto di riferimento - Nessun modello [13]	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Indirizzario principale dell'oggetto di riferimento - Modello specificato[13]	*DIR	"root" (/), QOpenSys, UDFS	*R
		*LIB, *FILE	QSYS.LIB[27]	*R
		*FLR	QDLS	*R
		*DDIR	QOPT[11]	*R
		*DDIR		*R
	Indirizzario principale dell'oggetto di riferimento - Opzione 8 (Visualizzazione attributi)	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Indirizzario principale dell'oggetto di riferimento - Opzione 12 (Gestione collegamenti)	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*SYMLNK	"root" (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
DSPLNK	Prefisso oggetto principale di riferimento - Nessun modello [13]	*DIR	″root″ (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Prefisso oggetto principale di riferimento - Modello specificato [13]	*DIR	″root″ (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Prefisso oggetto di riferimento principale - Opzione 8 (Visualizzazione attributi)	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Prefisso oggetto di riferimento principale - Opzione 12 (Gestione collegamenti)	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*SYMLNK	″root″ (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
DSPLNK	Nome percorso relativo [14] : Indirizzario di lavoro corrente contenente l'oggetto -Nessun modello[13]	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Nome percorso relativo [14] : Indirizzario di lavoro corrente contenente l'oggetto -Modello specificato[13]	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB[27]	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
DSPLNK	Nome percorso relativo [14] : Prefisso indirizzario di lavoro corrente contenente l'oggetto -Nessun modello [13]	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB[27]	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
DSPLNK	Nome percorso relativo [14] : Prefisso indirizzario di lavoro corrente contenente l'oggetto -Modello specificato [13]	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB[27]	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
DSPMFSINF	Oggetto	Qualunque valore	Qualunque valore	Nessuna
	Prefisso percorso	Fare riferimento alle regole generali.		

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
EDTF	File di database, membro esistente	*FILE	QSYS.LIB	*CHANGE
	Libreria file database	*LIB	QSYS.LIB	*EXECUTE
	File di database, nuovo membro	*FILE	QSYS.LIB	*CHANGE, *OBJMGT
	Libreria file di database, nuovo membro	*LIB	QSYS.LIB	*EXECUTE, *ADD
	File di flusso, file esistente	*STMF	QOpenSys, "root" (/), UDFS	*R
	Spazio utente	*USRSPC	QSYS.LIB	*CHANGE
	Indirizzario principale in caso di creazione di un nuovo file di flusso	*DIR	QOpenSys, "root" (/), UDFS	*WX
	Prefisso percorso	Fare riferimento alle regole generali.		
ENDJRN	Oggetto	*DIR se albero secondario (*ALL)	QOpenSys, "root" (/), UDFS	*R, *X, *OBJMGT
		*DIR se albero secondario (*NONE), *SYMLNK, *STMF	QOpenSys, "root" (/), UDFS	*R, *OBJMGT
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT
	Indirizzario principale	*DIR	QOpenSys, "root" (/), UDFS	*X
		*LIB	QSYS.LIB	*X
	Giornale	*JRN	QSYS.LIB	*OBJMGT, *OBJOPR
	Prefisso percorso	Fare riferimento alle regole generali.		
MOV[19]	Oggetto trasferito nello stesso file system	*DIR	QOpenSys, "root" (/)	*OBJMGT, *W
		non *DIR	QOpenSys, "root" (/)	*OBJMGT
		*DOC	QDLS	*ALL
		*FILE	QSYS.LIB	*OBJOPR, *OBJMGT
		*MBR	QSYS.LIB	Nessuna
		altro	QSYS.LIB	Nessuna
		*STMF	QOPT[11]	*W

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
MOV	Percorso (origine), indirizzario principale	*DIR	QOpenSys, ″root″ (/), UDFS	*WX
		*FLR	QDLS	*RWX
		*FILE	QSYS.LIB, ″root″ (/)	*RX, *OBJEXIST
		altri	QOpenSys, ″root″ (/)	*RWX
	Percorso (destinazione), indirizzario principale	*DIR	QSYS.LIB	*WX
		*FLR	QDLS	*CHANGE (*RWX)
		*FILE	QSYS.LIB	*X, *ADD, *DLT, *OBJMGT
		*LIB	QSYS.LIB	*RWX
		*DDIR	QOPT[11]	*WX
MOV	Prefisso percorso (destinazione)	*LIB	QSYS.LIB	*X, *ADD
		*FLR	QDLS	*X
		*DIR	altri	*X
		*DDIR	QOPT[11]	*X
	Oggetto spostato nei file system in QOpenSys, ″root″ (/) o QDLS (solo file di flusso *STMF e *DOC, *MBR).	*STMF	QOpenSys, ″root″ (/), UDFS	*R, *OBJEXIST, *OBJMGT
		*DOC	QDLS	*ALL
		*MBR	QSYS.LIB	Non applicabili
		*DSTMF	QOPT[11]	*RW
MOV	Spostato in QSYS *MBR	*STMF	QOpenSys, ″root″ (/), UDFS	*R, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*ALL
		*DSTMF	QOPT[11]	*RW
MOV	Volume dell'unità ottica (Origine e destinazione)	*DDIR	QOPT[8]	*CHANGE
	Percorso (origine) spostato su file system, indirizzario principale	*DIR	QOpenSys, ″root″ (/), UDFS	*WX
		*FLR	QDLS	*X
		*FILE	QSYS. LIB	proprietario, *RX, *OBJEXIST
		*DDIR	QOPT[11]	*WX
	Prefisso percorso	Fare riferimento alle regole generali.		
RCLLNK[16]				

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
RLSIFSLCK [18]	oggetto	*STMF	″root″ (/), QOpenSys, UDFS	*R
	Prefisso percorso	Fare riferimento alle regole generali.		
RMVDIR[19,20]	Indirizzario	*DIR	QOpenSys, ″root″ (/), UDFS	*OBJEXIST
		*LIB	QSYS.LIB	*RX, *OBJEXIST
		*FILE	QSYS.LIB	*OBJOPR, *OBJEXIST
		*FLR	QDLS	*ALL
		*DDIR	QOPT[11]	*W
RMVDIR	Indirizzario principale	*DIR	QOpenSys, ″root″ (/), UDFS	*WX
		*FLR	QDLS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*DDIR	QOPT[11]	*WX
	Indirizzario contenente gli oggetti, quando si specifica SUBTREE(*ALL)	Qualsiasi indirizzario	Tutti	*RX
	Volume ottico	*DDIR	QOPT[8]	*CHANGE
	Prefisso percorso	Fare riferimento alle regole generali.		
RMVLNK[19]	Oggetto	*DOC	QDLS	*ALL
		*MBR	QSYS.LIB	
		*FILE	QSYS.LIB	*OBJOPR, *OBJEXIST
		*JRNRCV	QSYS.LIB	*OBJEXIST, *R
		altro	QSYS.LIB	*OBJEXIST
		*DSTMF	QOPT[11]	*W
		Qualunque valore	QOpenSys, ″root″ (/), UDFS	*OBJEXIST
RMVLNK	Indirizzario principale	*FLR	QDLS	*X
		*FILE	QSYS.LIB	*X, *OBJEXIST
		*LIB	QSYS.LIB	*X
		*DIR	QOpenSys, ″root″ (/), UDFS	*WX
		*DDIR	QOPT[11]	*WX
	Volume ottico	*DDIR	QOPT[8]	*CHANGE
	Prefisso percorso	Fare riferimento alle regole generali.		

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
RNM[19]	Oggetto	*DIR	QOpenSys, "root" (/), UDFS	*OBJMGT, *W
		Non *DIR	QOpenSys, "root" (/), UDFS	*OBJMGT
		*DOC, *FLR	QDLS	*ALL
		*MBR	QSYS.LIB	Non applicabili
		*FILE	QSYS.LIB	*OBJMGT, *OBJOPR
		altri	QSYS.LIB	*OBJMGT
		*DSTMF	QOPT[11]	*W
	Volume dell'unità ottica (Origine e destinazione)	*DDIR	QOPT[8]	*CHANGE
RNM	Indirizzario principale	*DIR	QOpenSys, "root" (/), UDFS	*WX
		*FLR	QDLS	*CHANGE (*RWX)
		*FILE	QSYS.LIB	*X, *OBJMGT
		*LIB	QSYS.LIB	*X, *UPD
		*DDIR	QOPT[11]	*WX
	Prefisso percorso	*LIB	QSYS.LIB	*X, *UPD
		Qualunque valore	QOpenSys, "root" (/), UDFS, QDLS	*X
RST (Q) [23, 28, 30]	Oggetto, se presente [2]	Qualunque valore	QOpenSys, "root" (/), UDFS	*W, *OBJEXIST
			QSYS.LIB	Varia [10]
			QDLS	*ALL
	Prefisso percorso	Fare riferimento alle regole generali.		
	Indirizzario principale creato dall'operazione di ripristino a causa di CRTPRNDIR(*YES)[2]	*DIR	QOpenSys, "root" (/), UDFS	*WX
	Proprietario dell'indirizzario principale specificato sul parametro PRNDIROWN[2, 6]	*USRPRF	QSYS.LIB	*ADD

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
RST (Q)	Indirizzario principale dell'oggetto ripristinato[2]	*DIR	QOpenSys, "root" (/), UDFS	*WX
	Indirizzario principale dell'oggetto ripristinato, se l'oggetto è inesistente[2]	*FLR	QDLS	*CHANGE
		*DIR		*OBJMGT, *OBJALTER, *READ, *ADD, *UPD
	Profilo utente proprietario del nuovo oggetto ripristinato[2]	*USRPRF	QSYS.LIB	*ADD
	Unità nastro, unità ottica o file di salvataggio	*DEVD, *FILE	QSYS.LIB	*RX
	Definizione supporto magnetico	*MEDDFN	QSYS.LIB	*USE
RST (Q)	Libreria per unità descrizione o file di salvataggio	*LIB	QSYS.LIB	*EXECUTE
	File di emissione, se specificato	*STMF	QOpenSys, "root" (/), UDFS	*W
		*USRSPC	QSYS.LIB	*RWX
	Prefisso percorso file di emissione	*DIR	QOpenSys, "root" (/), UDFS	*X
		*LIB	QSYS.LIB	*RX
RST (Q)	Volume dell'unità ottica ripristino effettuato dall'unità ottica	*DDIR	QOPT[8]	*USE
	Prefisso percorso unità ottica e principale se si effettua il ripristino dall'unità ottica	*DDIR	QOPT[11]	*X
	File dell'unità ottica se si ripristina da un'unità ottica	*DSTMF	QOPT[11]	*R
RTVCURDIR	Prefisso percorso	*DIR	QOpenSys, "root" (/), UDFS, QDLS, QOPT[11]	*RX
		*DDIR	QOPT[11]	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		Qualunque valore		*R

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
RTVCURDIR	Indirizzario corrente	*DIR	QOpenSys, "root" (/), UDFS, QOPT [11]	*X
		*DDIR	QOPT[11]	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		Qualunque valore		*R
SAV[29]	Oggetto[2]	Qualunque valore	QOpenSys, "root" (/), UDFS	*R, *OBJEXIST
			QSYS.LIB	Varia [10]
			QDLS	*ALL
	Prefisso percorso	Fare riferimento alle regole generali.		
	Unità nastro, unità ottica	*DEVD	QSYS.LIB	*RX
	Definizione supporto magnetico	*MEDDFN	QSYS.LIB	*USE
SAV	File di salvataggio, se vuoto	*FILE	QSYS.LIB	*USE, *ADD
	Salvataggio file, se non è vuoto	*FILE	QSYS.LIB	*OBJMGT, *USE, *ADD
	Coda messaggi salva mentre attivo	*MSGQ	QSYS.LIB	*OBJOPR, *ADD
	Librerie per descrizione unità, definizione supporto magnetico, file di salvataggio o coda messaggi salva mentre attivo	*LIB	QSYS.LIB	*EXECUTE
SAV	File di emissione, se specificato	*STMF	QOpenSys, "root" (/), UDFS	*W
		*USRSPC	QSYS.LIB	*RWX
	Prefisso percorso file di emissione	*DIR	QOpenSys, "root" (/), UDFS	*X
		*LIB	QSYS.LIB	*RX
SAV	Volume ottico, se si effettua il salvataggio dall'unità ottica	*DDIR	QOPT[8]	*CHANGE
	Prefisso percorso ottico se si effettua il salvataggio su unità ottica	*DDIR	QOPT[11]	*X
	Indirizzario principale unità ottica se si salva su unità ottica	*DDIR	QOPT[11]	*WX
	File unità ottica (se presente)	*DSTMF	QOPT[11]	*RW
SAVRST	Sul sistema di origine, la stessa autorizzazione necessaria per il comando SAV.			
	Sul sistema di destinazione, la stessa autorizzazione necessaria per il comando RST.			

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
STATFS	Oggetto	Qualunque valore	Qualunque valore	Nessuna
	Prefisso percorso	Fare riferimento alle regole generali.		
STRJRN	Oggetto	*DIR se albero secondario (*ALL)	QOpenSys, ″root″ (/), UDFS	*R, *X, *OBJMGT
		*DIR se albero secondario (*NONE), *SYMLNK, *STMF	QOpenSys, ″root″ (/), UDFS	*R, *OBJMGT
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT
	Indirizzario principale	*DIR	QOpenSys, ″root″ (/), UDFS	*X
		*LIB	QSYS.LIB	*X
	Giornale	*JRN	QSYS.LIB	*OBJMGT, *OBJOPR
	Prefisso percorso	Fare riferimento alle regole generali.		
WRKAUT[6, 7]	Oggetto	*DOC o *FLR	QDLS	*ALL
		Tutto	non QDLS	*OBJMGT o proprietà
		*DDIR e *DSTMF	QOPT[11]	*NONE
	Volume ottico	*DDIR	QOPT[8]	*USE
	Prefisso percorso	Fare riferimento alle regole generali.		
WRKLNK	Qualunque valore	Qualunque valore	″root″ (/), QOpenSys, UDFS, QSYS.LIB[27], QDLS, QOPT[11]	Nessuna
	File, Opzione 12 (Gestione collegamenti)	*STMF, *SYMLNK, *DIR,*BLKSF, *SOCKET	″root″ (/), QOpenSys, UDFS	*R
	Oggetto collegamento simbolico	*SYMLNK	″root″ (/), QOpenSys, UDFS	Nessuna
	Volume ottico	*DDIR	QOPT[8]	*USE

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
WRKLNK	Indirizzario principale dell'oggetto di riferimento - Nessun modello [13]	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Indirizzario principale dell'oggetto di riferimento - Modello specificato	*DIR	"root" (/), QOpenSys, UDFS	*R
		*LIB *FILE	QSYS.LIB[27]	*R
		*FLR	QDLS	*R
		*DDIR	QOPT[11]	*R
		*DDIR		*R
WRKLNK	Indirizzario principale dell'oggetto di riferimento - Opzione 8 (Visualizzazione attributi)	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Indirizzario principale dell'oggetto di riferimento - Opzione 12 (Gestione collegamenti)	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*SYMLNK	"root" (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Prefisso oggetto principale di riferimento - Nessun modello [13]	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
WRKLNK	Prefisso oggetto principale di riferimento - Modello specificato [13]	*DIR	″root″ (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Prefisso oggetto di riferimento principale - Opzione 8 (Visualizzazione attributi)	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Prefisso oggetto di riferimento principale - Opzione 12 (Gestione collegamenti)	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*SYMLNK	″root″ (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Nome percorso relativo [14] : Indirizzario di lavoro corrente contenente l'oggetto -Nessun modello[13]	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Nome percorso relativo [14] : Indirizzario di lavoro corrente contenente l'oggetto -Modello specificato[13]	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB[27]	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]
WRKLNK	Nome percorso relativo [14] : Prefisso indirizzario di lavoro corrente contenente l'oggetto -Nessun modello [13]	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB[27]	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Nome percorso relativo [14] Prefisso indirizzario di lavoro corrente contenente l'oggetto -Modello specificato[13]	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB[27]	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R

[1] L'autorizzazione adottata non viene utilizzata per i comandi IFS (integrated file system).

[2] Se si dispone dell'autorizzazione speciale *SAVSYS, non è necessaria l'autorizzazione specificata per i file system QSYS.LIB, QDLS, QOpenSys e ″root″ (/).

[3] L'autorizzazione necessaria varia a seconda del tipo di oggetto. Consultare la descrizione di QLIRNMO API . Se l'oggetto è un membro di database, consultare le autorizzazioni per il comando RNMM (Ridenominazione membro).

[4] È necessario disporre dell'autorizzazione *AUDIT per modificare un valore di controllo.

[5] Se l'utente che immette il comando non dispone di autorizzazione *ALLOBJ, l'utente deve essere un membro del gruppo principale.

[6] Se il profilo specificato tramite il parametro PRNDIROWN non è l'utente che effettua l'operazione di ripristino, è richiesta l'autorizzazione speciale *SAVSYS o *ALLOBJ.

[7] Per questi comandi sono necessarie le autorizzazioni indicate e le autorizzazioni necessarie per il comando DSPCURDIR.

[8] I volumi dell'unità ottica non sono oggetti di sistema effettivi. Il collegamento tra il volume dell'unità ottica e l'elenco di autorizzazioni utilizzato per proteggere il volume viene gestito dalla funzione di supporto dell'unità ottica.

[9] L'utente deve disporre dell'autorizzazione speciale *AUDIT per modificare l'attributo *CRTOBJAUD e l'utente non ha necessità di alcuna autorizzazione del prefisso del nome percorso normale (*X e *R).

[10] L'autorizzazione necessaria varia a seconda del comando utilizzato. Fare riferimento ai comandi SAVOBJ o RSTOBJ per l'autorizzazione richiesta.

[11] Autorizzazione necessaria per QOPT sul supporto magnetico formattato in UDF (Universal Disk Format).

[12] *ADD è necessario solo quando l'oggetto verso cui si sposta è un *MRB.

[13] Modello: In alcuni comandi, un asterisco (*) o un punto interrogativo (?) nell'ultimo componente del nome del percorso per ricercare il nome corrispondente al modello.

[14] Nome percorso relativo: se il nome di percorso non inizia con una barra, l'elemento che precede il primo componente del percorso viene considerato l'indirizzario di lavoro corrente del processo. Ad esempio se viene specificato un nome di percorso 'a/b' e l'indirizzario di lavoro corrente è '/home/john', l'oggetto cui si accede è '/home/john/a/b'.

[15] Se si dispone dell'autorizzazione speciale *ALLOBJ, non è necessario disporre delle autorizzazioni elencate.

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto[1]

[16] È necessario disporre dell'autorizzazione speciale *ALLOBJ per utilizzare questo comando.

[17] Nella tabella precedente, QSYS.LIB si riferisce ai file system QSYS.LIB dell'ASP indipendente ed anche al file system QSYS.LIB.

[18] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *IOSYSCFG.

[19] Se l'attributo ridenominazioni e scollegamenti limitati (anche noto come S_ISVTX bit) viene attivato per un'indirizzario, esso limita gli oggetti di scollegamento dall'indirizzario a meno che non si rilevi uno dei seguenti:

- L'utente dispone dell'autorizzazione speciale a tutti gli oggetti (*ALLOBJ).
- L'utente è il proprietario dell'oggetto scollegato.
- L'utente è il proprietario dell'indirizzario.

[20] Se si specifica RMVLNK (*YES), l'utente deve anche disporre dell'autorizzazione *OBJEXIST a tutti gli oggetti specificati nell'indirizzario.

[21] Per QSYS.LIB, "root" (/), QOpenSys e i file di sistema definiti dall'utente, è necessario disporre dell'autorizzazione speciale (*AUDIT) se viene specificato un valore diverso da *SYSVAL per il parametro CRTOBJAUD.

[22] L'utente deve disporre delle autorizzazioni speciali a tutti gli oggetti (*ALLOBJ) e amministratore della riservatezza (*SECADM) per specificare un valore per il parametro Scansione opzione per oggetti (CRTOBJSCAN) diverso da *PARENT.

[23] È necessario disporre dell'autorizzazione speciale *ALLOBJ per specificare un valore diverso da *NONE per il parametro ALWOBJDIF (Consenso differenze oggetto). Inoltre, è necessario disporre dell'autorizzazione speciale *SAVSYS o *ALLOBJ per specificare *UDFS come valore per il parametro RBDMFS.

[24] L'utente deve disporre dell'autorizzazione speciale a tutti gli oggetti (*ALLOBJ) e di quella di amministratore della riservatezza (*SECADM) quando modifica il proprietario di un file di flusso (*STMF) con un programma Java collegato il cui controllo dell'autorizzazione in fase di esecuzione del programma include l'utente e il proprietario.

[25] L'utente deve disporre dell'autorizzazione speciale a tutti gli oggetti (*ALLOBJ) e di quella di amministratore della riservatezza (*SECADM) quando copia un file di flusso (*STMF) con un programma Java collegato il cui controllo dell'autorizzazione include l'utente e il proprietario.

[26] L'utente deve disporre dell'autorizzazione speciale a tutti gli oggetti (*ALLOBJ) e di quella di amministratore della riservatezza (*SECADM) per specificare gli attributi *CRTOBJSCAN e *SCAN.

[27] Quando viene visualizzato il contenuto dell'indirizzario /QSYS.LIB, gli oggetti (*USRPRF) del profilo utente a cui il chiamante non dispone di alcuna autorizzazione (come ad esempio *EXCLUDE) non vengono restituiti.

[28] L'utente deve disporre dell'autorizzazione speciale *ALLOBJ per specificare *YES per il parametro PVTAUT.

[29] L'utente deve disporre dell'autorizzazione speciale *ALLOBJ o *SAVSYS per specificare *YES per il parametro PVTAUT.

[30] È necessario disporre dell'autorizzazione speciale *SAVSYS o *ALLOBJ per specificare *UDFS come valore per il parametro RBDMFS.

Comandi definizione dati interattivi

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi definizione dati interattivi.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ADDDTADFN	Dizionario di dati	*CHANGE	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE
CRTDTADCT	Dizionario di dati		*READ, *ADD
DLTDTADCT [3]	Dizionario di dati	OBJEXIST, *USE	
DSPDTADCT	Dizionario di dati	*USE	*EXECUTE
LNKDTADFN [1]	Dizionario di dati	*USE	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE
STRIDD			
WRKDTADCT [2]	Dizionario di dati	*OBJOPR	*EXECUTE
WRKDBFIDD [2]	Dizionario di dati	*USE [4]	*EXECUTE
	File di database	*OBJOPR	*EXECUTE
WRKDTADFN [1]	Dizionario di dati	*USE, *CHANGE	*EXECUTE

[1] L'autorizzazione a un dizionario di dati non è necessaria per scollegare un file.

[2] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

[3] Prima della cancellazione di un dizionario, tutti i file collegati vengono scollegati. Fare riferimento al comando LNKDTADFN per l'autorizzazione richiesta per scollegare un file.

[4] È necessario disporre dell'autorizzazione per l'utilizzo del dizionario di dati per creare un nuovo file. Non è necessaria alcuna autorizzazione per il dizionario di dati per immettere dati in un file esistente.

Comandi IPX (Internetwork Packet Exchange)

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi IPX (Internetwork Packet Exchange).

Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
DLTIPXD	Descrizione IPX	*OBJEXIST	*EXECUTE
DSPIPXD	Descrizione IPX	*USE	*EXECUTE
WRKIPXD	Descrizione IPX	*OBJOPR	*EXECUTE

Comandi indice di ricerca informazioni

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi indice di ricerca informazioni.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ADDSCHIDXE	Indice di ricerca	*CHANGE	*USE
	Gruppo pannelli	*USE	*EXECUTE
CHGSCHIDX	Indice di ricerca	*CHANGE	*USE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
CRTSCHIDX	Indice di ricerca		*READ, *ADD
DLTSCHIDX	Indice di ricerca	*OBJEXIST	*EXECUTE
RMVSCHIDXE	Indice di ricerca	*CHANGE	*USE
STRSCHIDX	Indice di ricerca	*USE	*EXECUTE
WRKSCHIDX [1]	Indice di ricerca	*ANY	*USE
WRKSCHIDXE	Indice di ricerca	*USE	*USE

Comandi attributo IPL

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi attributo IPL.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Questi comandi non richiedono l'autorizzazione per gli oggetti:
CHGIPLA (Q) [1] DSPIPLA
1 Per utilizzare questo comando, è necessario disporre delle autorizzazioni speciali *SECADM e *ALLOBJ.

Comandi Java

Questa tabella elenca le autorizzazioni specifiche richieste per comandi Java.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ANZJVM	Comando QSYS/STRSRVJOB	*USE	
	Comando QSYS/STRDBG	*USE	
DSPJVMJOB[1]	Lavori Java Virtual Machine		
GENJVMDMP [1]			
PRTJVMJOB [1]			
WRKJVMJOB [1]			
1 È necessario disporre dell'autorizzazione speciale *JOBCTL per utilizzare questo comando.			

Comandi lavoro

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi lavoro.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
BCHJOB	Descrizione lavoro [9,11]	*USE	*EXECUTE
	Librerie nell'elenco librerie (sistema, corrente e utente)[7]	*USE	
	Profilo utente nella descrizione lavoro [10]	*USE	
	Tabella sequenza ordinamento [7]	*USE	*EXECUTE
	Coda messaggi [10]	*USE, *ADD	*EXECUTE
	Coda lavori [10,11]	*USE	*EXECUTE
	Coda emissione [7]	*READ	*EXECUTE
CHGACGCDE [1]			
CHGGRPA [4]	Coda messaggi, se associa una coda messaggi a un gruppo	*OBJOPR	*EXECUTE
CHGJOB [1,2,3]	Nuova coda lavori, se modifica la coda lavori [10,11]	*USE	*EXECUTE
	Nuova coda emissione, se modifica la coda emissione[7]	*READ	*EXECUTE
	Coda emissione corrente, se modifica la coda emissione	*READ	*EXECUTE
	Tabella sequenza ordinamento [7]	*USE	*EXECUTE
CHGPJ	Profilo utente per la richiesta di avvio del programma per specificare *PGMSTRRQS	*USE	*EXECUTE
	Descrizione profilo utente e lavoro	*USE	*EXECUTE
CHGSYSJOB(Q) [13]			
CHGUSRTRC[14]	Buffer traccia utente quando si utilizza CLEAR (*YES).[15]	*OBJOPR	*EXECUTE
	Buffer traccia utente quando si utilizza MAXSTG[15]	*CHANGE, *OBJMGT	*USE
	Buffer traccia utente quando si utilizza TRCFULL. [15]	*OBJOPR	*EXECUTE
DLTUSRTRC	Buffer traccia utente [15]	*OBJOPR, *OBJEXIST	*EXECUTE
DLYJOB [4]			
DMPUSRTRC	Buffer traccia utente [15]	*OBJOPR	*EXECUTE
DSCJOB [1]			
DSPACTPJ	Descrizione unità ASP (Auxiliary storage pool)	*USE	
	Libreria programma		*EXECUTE
DSPJOB [1]			
DSPJOBTBL			
DSPJOBLOG [1,5]	File di emissione e membro esistente	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Membro non esistente	*OBJOPR, *OBJMGT, *ADD	*EXECUTE, *ADD
	Il file di emissione non esiste	*OBJOPR	*EXECUTE, *ADD
ENDGRPJOB			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ENDJOB [1]			
ENDJOBABN [1]			
ENDLOGSVR[6]			
ENDPJ [6]	Descrizione unità ASP (Auxiliary storage pool)	*USE	
	Libreria programma		*EXECUTE
HLDJOB [1]			
RLSJOB [1]			
RRTJOB			
RTVJOBA			
SBMDBJOB	File di database	*USE	*EXECUTE
	Coda lavori	*READ	*EXECUTE
SBMDKTJOB	Coda messaggi	*USE, *ADD	*EXECUTE
	Descrizione coda lavori e unità	*READ	*EXECUTE
SBMJOB [2, 12, 17, 18]	Descrizione lavoro [9,11]	*USE	*EXECUTE
	Librerie nell'elenco librerie (sistema, corrente e utente)[7]	*USE	
	Coda messaggi [10]	*USE, *ADD	*EXECUTE
	Profilo utente [10,11]	*USE	
	Profilo utente nella descrizione lavoro [10]	*USE (a livello 40)	
	Coda lavori [10,11]	*USE	*EXECUTE
	Coda emissione [7]	*READ	*EXECUTE
	Tabella sequenza ordinamento [7]	*USE	*EXECUTE
	Unità ASP nel gruppo ASP iniziale	*USE	
SBMNETJOB	File di database	*USE	*EXECUTE
STRLOGSVR[6]			
STRPJ [6]	Descrizione sottosistema	*USE	
	Programma	*USE	*EXECUTE
	Descrizione unità ASP (Auxiliary storage pool)	*USE	
TFRBCHJOB	Coda lavori	*READ	*EXECUTE
TFRGRPJOB	Programma primo gruppo	*USE	*EXECUTE
TFRJOB [8]	Coda lavori	*USE	*EXECUTE
	Descrizione sottosistema cui è assegnata la coda lavori	*USE	
TFRSECJOB			
WRKACTJOB			
WRKARMJOB[16]			
WRKASPJOB	Descrizione unità	*USE	
WRKJOB [1]			
WRKJOBLOG			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
WRKSBMJOB			
WRKSBSJOB			
WRKUSRJOB			

[1] Qualsiasi utente può eseguire questi comandi per i lavori in esecuzione sotto il proprio profilo utente. L'utente provvisto di autorizzazione speciale (*JOBCTL) (controllo lavoro) può eseguirli per qualsiasi lavoro. Se si dispone dell'autorizzazione speciale *SPLCTL, non è necessaria alcuna autorizzazione alla coda lavori. È necessario, tuttavia, disporre dell'autorizzazione alla libreria che contiene la coda lavori.

[2] È necessario disporre dell'autorizzazione (specificata nel profilo utente) per la priorità di pianificazione ed emissione specificate.

[3] Per modificare alcuni attributi del lavoro, anche se relativi al lavoro dell'utente, è necessario disporre dell'autorizzazione speciale al controllo lavoro (*JOBCTL). Gli attributi sono RUNPTY, TIMESLICE, PURGE, DFTWAIT e TSEPOOL.

[4] Questo comando ha effetti solo sul lavoro nel quale viene specificato.

[5] Per visualizzare una registrazione lavoro per un lavoro con autorizzazione speciale a tutti gli oggetti (*ALLOBJ), è necessario disporre dell'autorizzazione speciale *ALLOBJ o essere autorizzati alla funzione Registrazione lavoro tutti gli oggetti di i5/OS mediante la gestione applicazione in System i Navigator. Il comando CHGFCNUSG (Modifica utilizzo funzione), con l'ID funzione QIBM_ALLOBJ_JOBLOG, può essere utilizzato anche per modificare l'elenco di utenti abilitati a visualizzare una registrazione lavoro con autorizzazione speciale *ALLOBJ.

[6] Per utilizzare questo comando, è necessario disporre dell'autorizzazione al controllo del lavoro *JOBCTL.

[7] Nel profilo utente sotto cui è in esecuzione il lavoro inoltrato viene ricercata l'autorizzazione all'oggetto di riferimento. L'autorizzazione adottata dell'utente che inoltra o modifica il lavoro non viene utilizzata.

[8] Se il lavoro trasferito è un lavoro interattivo, vengono applicate le seguenti limitazioni:

- La coda lavori in cui è inserito il lavoro deve essere associata a un sottosistema attivo.
- La stazione di lavoro associata al lavoro deve avere una voce stazione di lavoro corrispondente nella descrizione sottosistema associata al nuovo sottosistema.
- La stazione di lavoro associata al lavoro non deve avere un altro lavoro associato ad essa che sia stato sospeso mediante il tasto Sys Req (Richiesta sistema). Il lavoro sospeso deve essere cancellato, perché il comando Trasferimento lavoro possa essere eseguito.
- Il lavoro non deve essere un lavoro di gruppo.

[9] Viene controllato che sia l'utente che inoltra il lavoro sia il profilo utente sotto cui è in esecuzione il lavoro dispongano dell'autorizzazione all'oggetto di riferimento.

[10] Viene controllato che l'utente che inoltra il lavoro disponga dell'autorizzazione all'oggetto di riferimento.

[11] Viene utilizzata l'autorizzazione adottata dell'utente che immette il comando CHGJOB o SBMJOB.

[12] È necessario disporre dell'autorizzazione al profilo utente e alla descrizione lavoro; il profilo utente deve inoltre essere autorizzato alla descrizione lavoro.

[13] Per modificare alcuni attributi del lavoro, anche se relativi al lavoro dell'utente, è necessario disporre delle autorizzazioni speciali al controllo lavoro (*JOBCTL) e a tutti gli oggetti (*ALLOBJ).

[14] Qualsiasi utente può eseguire questi comandi per i lavori in esecuzione sotto il proprio profilo utente. L'utente provvisto di autorizzazione speciale (*JOBCTL) (controllo lavoro) può eseguire questi comandi per qualsiasi lavoro.

[15] Un buffer traccia utente è un oggetto spazio utente (*USRSPC) nella libreria QUSRSYS dal nome QPOZ*nnnnnn*, dove '*nnnnnn*' è il numero lavoro del lavoro che utilizza la funzione traccia utente.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
[16] per gestire un lavoro specifico o per visualizzare i dettagli di un lavoro specifico, deve verificarsi una delle seguenti condizioni: • Il comando deve essere emesso dall'interno del lavoro. • Il comando deve essere emesso da un profilo utente uguale all'identità utente del lavoro. • Il comando deve essere emesso da un profilo utente che dispone dell'autorizzazione speciale controllo del lavoro (*JOBCTL). [17] È necessario disporre dell'autorizzazione utente (*USE) al comando CHGACGCDE (Modifica codice account) per specificare un codice account valore-carattere sul parametro parametro codice account (ACGCDE). [18] È necessario disporre dell'autorizzazione speciale sul controllo del lavoro (*JOBCTL) per utilizzare il parametro Inoltro per (SBMFOR).			

Comandi descrizione lavoro

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi descrizione lavoro.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGJOBD	Descrizione lavoro	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Profilo utente (Utente)	*USE	
CPYAUDJRNE[8]	Il file di emissione esiste già	*OBJOPR *OBJMGT *ADD *DLT	*EXECUTE
	Il file di emissione non esiste		*EXECUTE *ADD
CRTJOBD (Q)	Descrizione lavoro		*READ, *ADD
	Profilo utente (Utente)	*USE	
DLTJOBD	Descrizione lavoro	*OBJEXIST	*EXECUTE
DSPJOBD	Descrizione lavoro	*OBJOPR, *READ	*EXECUTE
PRTJOBDAUT [1]			
WRKJOBD	Descrizione lavoro	Qualunque valore	*USE
[1] È necessario disporre dell'autorizzazione speciale *ALLOBJ o *AUDIT per utilizzare questo comando.			

Comandi coda lavori

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi coda lavori.

Comando	Oggetto di riferimento	Parametri coda lavori [4]		Autorizzaz. speciale	Autorizzazione necessaria	
		AUTCHK	OPRCTL		Per oggetto	Per libreria
CHGJOBQ	Coda lavori	*DTAAUT			*READ, *ADD, *DLT, *OBJMGMT	*EXECUTE
		*OWNER			Proprietario [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CLRJOBQ [1]	Coda lavori	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietario [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CRTJOBQ [1]	Coda lavori					*READ, *ADD
DLTJOBQ	Coda lavori				*OBJEXIST	*EXECUTE
HLDJOBQ [1]	Coda lavori	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietario [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
PRTQAUT [5]						
RLSJOBQ [1]	Coda lavori	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietario [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKJOBQ [1,3]	Coda lavori	*DTAAUT			*READ	*EXECUTE
		*OWNER			Proprietario [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKJOBQD	Coda lavori				*READ	*EXECUTE
			*YES	*JOBCTL		*EXECUTE

[1] Se si dispone dell'autorizzazione speciale *SPLCTL, non è necessaria alcuna autorizzazione alla coda lavori, ma è necessaria l'autorizzazione alla libreria che contiene la coda lavori.

[2] È necessario essere il proprietario della coda lavori.

[3] Se si richiede di gestire tutte le code lavori, il pannello dell'elenco include tutte le code lavori presenti nelle librerie per cui si dispone di autorizzazione *EXECUTE.

[4] Per visualizzare i parametri della coda lavori, utilizzare l'API QSPRJOBQ.

[5] È necessario disporre dell'autorizzazione speciale *ALLOBJ o *AUDIT per utilizzare questo comando.

Comandi pianificazione lavoro

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi pianificazione lavoro.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDJOBSCDE	Pianificazione lavoro	*CHANGE	*EXECUTE
	Descrizione lavoro [1]	*USE	*EXECUTE
	Coda lavori [1,2]	*READ	*EXECUTE
	Profilo utente	*USE	*EXECUTE
	Coda messaggi [1]	*USE, *ADD	*EXECUTE
CHGJOBSCDE [3]	Pianificazione lavoro	*CHANGE	*EXECUTE
	Descrizione lavoro [1]	*USE	*EXECUTE
	Coda lavori [1,2]	*READ	*EXECUTE
	Profilo utente	*USE	*EXECUTE
	Coda messaggi [1]	*USE, *ADD	*EXECUTE
HLDJOBSCDE [3]	Pianificazione lavoro	*CHANGE	*EXECUTE
RLSJOBSCDE [3]	Pianificazione lavoro	*CHANGE	*EXECUTE
RMVJOBSCDE [3]	Pianificazione lavoro	*CHANGE	*EXECUTE
WRKJOBSCDE [4]	Pianificazione lavoro	*USE	*EXECUTE

1 Viene controllato che sia il profilo utente che aggiunge la voce sia il profilo utente sotto cui viene eseguito il lavoro dispongano dell'autorizzazione per l'oggetto di riferimento.

2 L'autorizzazione alla coda lavori non può provenire dall'autorizzazione adottata.

3 È necessario disporre dell'autorizzazione speciale *JOBCTL o aver aggiunto la voce.

4 Per visualizzare i dettagli di una voce (opzione 5 o formato stampa *FULL), occorre disporre dell'autorizzazione speciale *JOBCTL o aver aggiunto la voce.

Comandi giornale

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi giornale.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**per libreria o indirizzario**
ADDRMTJRN	Giornale di origine	*CHANGE, *OBJMGT	*EXECUTE
	Giornale di destinazione		*EXEC, *ADD
APYJRNCHG (Q)	Giornale	*USE	*EXECUTE
	Ricevitore di giornale	*USE	*EXECUTE
	Oggetti non IFS di cui si stanno applicando le modifiche registrate su giornale	*OBJMGT, *CHANGE, *OBJEXIST	*EXECUTE, *ADD
	Oggetti IFS di cui si stanno applicando le modifiche registrate su giornale	*RW, *OBJMGT	*RX (se albero secondario *ALL)

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	per libreria o indirizzario
APYJRNCHGX (Q)	Giornale	*USE	
	Ricevitore di giornale	*USE	
	File	*OBJMGT, *CHANGE, *OBJEXIST'	*EXECUTE, *ADD
CHGJRN (Q)	Ricevitore di giornale, se specificato	*OBJMGT, *USE	*EXECUTE
	Ricevitore di giornale collegato	*OBJMGT, *USE	*EXECUTE
	Giornale	*OBJOPR, *OBJMGT, *UPD	*EXECUTE
	Giornale se specificato RCVSIZOPT(*MINFIXLEN).	*OBJOPR, *OBJMGT, *UPD, *OBJALTER	*EXECUTE
CHGJRNA (Q) [10]			
CHGJRNOBJ [9]	Giornale	*OBJOPR, *OBJMGT	
	Oggetti non IFS	*READ, *OBJMGT	
	Oggetti IFS	*R, *OBJMGT	*X
	Percorso oggetto SUBTREE(*ALL)	*RX, *OBJMGT	
	Percorso oggetto SUBTREE(*NONE)	*R, *OBJMGT	
CHGRMTJRN	Giornale di origine	*CHANGE, *OBJMGT	*EXECUTE
	Giornale di origine	*USE, *OBJMGT	*EXECUTE
CMPJRNIMG	Giornale	*USE	*EXECUTE
	Ricevitore di giornale	*USE	*EXECUTE
	File	*USE	*EXECUTE
CPYAUDJRNE[8]	Il file di emissione esiste già	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Il file di emissione non esiste		*EXECUTE, *ADD
CRTJRN	Giornale		*READ, *ADD
	Ricevitore di giornale	*OBJOPR, *OBJMGT, *READ	*EXECUTE
DLTJRN	Giornale	*OBJOPR, *OBJEXIST	*EXECUTE
DSPAUDJRNE[8]			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**per libreria o indirizzario**
DSPJRN [6]	Giornale	*USE	*EXECUTE
	Giornale se è specificato FILE(*ALLFILE) se non si specifica alcuna selezione di oggetti, se l'oggetto specificato è stato cancellato dal sistema, se l'oggetto specificato non è mai stato registrato su giornale, se si specifica *IGNFILSLT o *IGNOBJSLT per uno qualsiasi dei codici di giornale selezionati, oppure quando OBJJID è specificato o se il giornale è un giornale remoto.	*OBJEXIST, *USE	*EXECUTE
	Ricevitore di giornale	*USE	*EXECUTE
	Oggetto non IFS, se specificato	*USE	*EXECUTE
	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	Oggetto IFS, se specificato	*R (può essere anche *X se l'oggetto è un indirizzario e si specifica SUBTREE (*ALL))	*X
DSPJRNMNU[1]			
ENDJRN	Consultare "Comandi dell'IFS (Integrated file system)" a pagina 417.		
ENDJRNAP	Giornale	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE
ENDJRNLIB	Giornale	*OBJOPR, *OBJMGT	*EXECUTE
	Libreria	*OBJOPR, *OBJMGT, *READ	
ENDJRNOBJ	Giornale	*OBJOPR, *OBJMGT	*EXECUTE
	Oggetto	*OBJOPR, *READ, *OBJMGT	*EXECUTE
ENDJRNPF	Giornale	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT, *READ	*EXECUTE
JRNAP [2]			
JRNPF [3]			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**per libreria o indirizzario**
RCVJRNE	Giornale	*USE	*EXECUTE
	Giornale se è specificato FILE(*ALLFILE) se non si specifica alcuna selezione di oggetti, se l'oggetto specificato è stato cancellato dal sistema, se l'oggetto spacificato non è mai stato registrato su giornale, se si specifica *IGNFILSLT o *IGNOBJSLT per uno qualsiasi dei codici di giornale selezionati, oppure quando OBJJID è specificato o se il giornale è un giornale remoto.	*OBJEXIST, *USE	*EXECUTE
	Ricevitore di giornale	*USE	*EXECUTE
	Oggetto non IFS, se specificato	*USE	*EXECUTE
	Oggetto IFS, se specificato	*R (può essere anche *X se l'oggetto è un indirizzario e si specifica SUBTREE (*ALL))	*X
	Programma di uscita	*EXECUTE	*EXECUTE
RMVJRNCHG (Q)	Giornale	*USE	*EXECUTE
	Ricevitore di giornale	*USE	*EXECUTE
	Oggetti non IFS di cui si stanno rimuovendo le modifiche registrate su giornale	*OBJMGT, *CHANGE	*EXECUTE
RTVJRNE	Giornale	*USE	*EXECUTE
	Giornale se è specificato FILE(*ALLFILE) se non si specifica alcuna selezione di oggetti, se l'oggetto specificato è stato cancellato dal sistema, se l'oggetto spacificato non è mai stato registrato su giornale, se si specifica *IGNFILSLT o *IGNOBJSLT per uno qualsiasi dei codici di giornale selezionati, oppure quando OBJJID è specificato o se il giornale è un giornale remoto.	*OBJEXIST, *USE	*EXECUTE
	Ricevitore di giornale	*USE	*EXECUTE
	Oggetto non IFS, se specificato	*USE	*EXECUTE
	Oggetto IFS, se specificato	*R (può essere anche *X se l'oggetto è un indirizzario e si specifica SUBTREE (*ALL))	*X
RMVRMTJRN	Giornale di origine	*CHG, *OBJMGT	
SNDJRNE	Giornale	*OBJOPR, *ADD	*EXECUTE
	Oggetto non IFS, se specificato	*OBJOPR	*EXECUTE
	Oggetto IFS, se specificato	*R	*X
STRJRN	Consultare "Comandi dell'IFS (Integrated file system)" a pagina 417.		
STRJRNAP	Giornale	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**per libreria o indirizzario**
STRJRNLIB	Giornale	*OBJOPR, *OBJMGT	*EXECUTE
	Libreria	*OBJOPR, *OBJMGT, *READ	
STRJRNPF	Giornale	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE
STRJRNOBJ	Giornale	*OBJOPR, *OBJMGT	*EXECUTE
	Oggetto	*OBJOPR, *READ, *OBJMGT	*EXECUTE
WRKJRN [4] (Q)	Giornale	*USE	*READ[7]
	Ricevitore giornali	*USE	*EXECUTE
WRKJRNA [6]	Giornale	*OBJOPR e un'autorizzazione dati diversa da *EXECUTE	*EXECUTE
	Ricevitore di giornale [5]	*OBJOPR e un'autorizzazione dati diversa da *EXECUTE	*EXECUTE

[1] Consultare il comando WRKJRN (questo comando ha la stessa funzione).

[2] Consultare il comando STRJRNAP.

[3] Consultare il comando STRJRNPF.

[4] È necessario disporre di autorizzazione aggiuntiva per funzioni specifiche richiamate durante l'operazione selezionata. Ad esempio, per ripristinare un oggetto è necessario disporre dell'autorizzazione richiesta per il comando RSTOBJ o RST.

[5] Se si sceglie l'opzione per cancellare i ricevitori, è necessario disporre delle autorizzazioni *OBJOPR e *OBJEXIST per i ricevitori di giornale.

[6] Per specificare JRN(*INTSYSJRN), è necessario disporre dell'autorizzazione speciale *ALLOBJ.

[7] Per visualizzare il menu WRKJRN, è necessario disporre dell'autorizzazione *READ alla libreria del giornale. Per utilizzare un'opzione presente nel menu, è necessaria l'autorizzazione *EXECUTE alla libreria.

[8] È necessario disporre dell'autorizzazione speciale *AUDIT per utilizzare questo comando.

[9] Per specificare PTLTNS(*ALWUSE), è necessario disporre dell'autorizzazione speciale *ALLOBJ.

[10] È necessario disporre dell'autorizzazione speciale *JOBCTL per utilizzare questo comando.

Comandi ricevitore di giornale

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi ricevitore di giornale.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTJRNRCV	Ricevitore di giornale		*READ, *ADD
DLTJRNRCV	Ricevitore di giornale	*OBJOPR, *OBJEXIST e autorizzazione dati diversa da *EXECUTE	*EXECUTE
	Giornale	*OBJOPR	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
DSPJRNRCVA	Ricevitore di giornale	*OBJOPR e un'autorizzazione dati diversa da *EXECUTE	*EXECUTE
	Giornale, se collegato	*OBJOPR	*EXECUTE
WRKJRNRCV [1], [2], [3]	Ricevitore di giornale	Qualsiasi autorizzazione	*USE

[1] Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.

[2] Se si sceglie l'opzione per cancellare i ricevitori, è necessario disporre delle autorizzazioni *OBJOPR e *OBJEXIST per i ricevitori di giornale.

[3] È necessario *OBJOPR ed un'autorizzazione dati diversa da *EXECUTE per i ricevitori di giornale se si seleziona l'opzione per visualizzare la descrizione.

Comandi Kerberos

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi Kerberos.

Comando	Oggetto di riferimento	Tipo oggetto	Autorizzaz. necessaria per l'oggetto
ADDKRBKTE	Ogni indirizzario nel nome percorso che precede file tabella chiave di destinazione da aprire.	*DIR	*X
	L'indirizzario principale del file keytab di destinazione quando si specifica l'aggiunta, se il file non è già esistente.	*DIR	*WX
	File keytab quando è specificato l'elenco.	*STMF	*R
	File keytab di destinazione quando è specificato aggiunta o cancellazione.	*STMF	*RW
	Ciascun indirizzario nel percorso ai file di configurazione.	*DIR	*X
	File di configurazione	*STMF	*R
ADDKRBTKT	Ciascun indirizzario nel nome percorso che precede il file tabella chiave	*DIR	*X
	File tabella chiave	*STMF	*R
	Ciascun indirizzario nel nome percorso che precede il file della cache credenziali	*DIR	*X
	File della cache credenziale	*STMF	*RW
	Indirizzario principale del file della cache da utilizzare, se specificato dalla variabile di ambiente KRB5CCNAME e se si sta creando il file	*DIR	*WX
	Ciascun indirizzario nel nome percorso ai file di configurazione	*DIR	*X
	File di configurazione	*STMF	*R
CHGKRBPWD			

Comando	Oggetto di riferimento	Tipo oggetto	Autorizzaz. necessaria per l'oggetto
DLTKRBCCF	Ciascun indirirzzario nel nome percorso che precede il file della cache credenziali, se il file della cache credenziali non risiede nell'indirizzario predefinito.	*DIR	*X
	Indirizzario principale del file della cache credenziali, se il file della cache credenziali non risiede nell'indirizzario predefinito.	*DIR	*WX
	File della cache credenziali, se il file della cache credenziali non risiede nell'indirizzario predefinito.	*STMF	*RW, *OBJEXIST
	Ciascun indirirzzario nel nome percorso ai file di configurazione, se il file della cache credenziali non risiede nell'indirizzario predefinito.	*DIR	*X
	File di configurazone, se il file della cache credenziali non risiede nell'indirizzario predefinito.	*STMF	*R
DLTKRBCCF	Tutti gli indirizzari nel nome percorso, se il file della cache credenziali risiede nell'indirizzario predefinito.	*DIR	*X
	File della cache credenziali, se il file della cache credenziali risiede nell'indirizzario predefinito.	*STMF	*RW
	Ciascun indirizzario nel percorso ai file di configurazione, se il file della cache credenziali risiede nell'indirizzario predefinito.	*DIR	*X
	File di configurazone, se il file della cache credenziali risiede nell'indirizzario predefinito.	*STMF	*R
DSPKRBCCF	Ciascun indirizzario nel nome percorso che precede il file tabella chiave	*DIR	*X
	File tabella chiave	*STMF	*R
	Ciascun indirizzario nel nome percorso che precede il file della cache credenziali	*DIR	*X
	File della cache credenziale	*STMF	*RW
DSPKRBKTE	Ogni indirizzario nel nome percorso che precede file tabella chiave di destinazione da aprire.	*DIR	*X
	L'indirizzario principale del file keytab di destinazione quando si specifica l'aggiunta, se il file non è già esistente.	*DIR	*WX
	File keytab quando è specificato l'elenco.	*STMF	*R
	File keytab di destinazione quando è specificato aggiunta o cancellazione.	*STMF	*RW
	Ciascun indirizzario nel percorso ai file di configurazione.	*DIR	*X
	File di configurazione	*STMF	*R

Comando	Oggetto di riferimento	Tipo oggetto	Autorizzaz. necessaria per l'oggetto
RMVKRBKTE	Ogni indirizzario nel nome percorso che precede file tabella chiave di destinazione da aprire.	*DIR	*X
	L'indirizzario principale del file keytab di destinazione quando si specifica l'aggiunta, se il file non è già esistente.	*DIR	*WX
	File keytab quando è specificato l'elenco.	*STMF	*R
	File keytab di destinazione quando è specificato aggiunta o cancellazione.	*STMF	*RW
	Ciascun indirizzario nel percorso ai file di configurazione.	*DIR	*X
	File di configurazione	*STMF	*R

Comandi linguaggio

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi linguaggio.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
CLOSE	comando per chiusura	*USE	*EXECUTE
CRTBNDC	File di origine	*USE	*EXECUTE
	File unità e di database descritti esternamente cui si fa riferimento nel programma di origine	*OBJOPR	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Indirizzario specificato nel parametro OUTPUT, PPSRCSTMF o MAKEDEP	*USE	*EXECUTE
	File specificato nel parametro OUTPUT, PPSRCSTMF o MAKEDEP	Fare riferimento alle regole generali.	*READ, *ADD
CRTBNDCBL	File di origine	*USE	*EXECUTE
	File unità e di database descritti esternamente cui si fa riferimento nel programma di origine	*OBJOPR	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Indirizzario di collegamento	*USE	*EXECUTE
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTBNDCL	File di origine	*USE	*EXECUTE
	Inclusione file	*USE	*EXECUTE
	File unità e di database descritti esternamente cui si fa riferimento nel programma di origine	*OBJOPR	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
CRTBNDCPP	File di origine	*USE	*EXECUTE
	File unità e di database descritti esternamente cui si fa riferimento nel programma di origine	*OBJOPR	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Indirizzario specificato nel parametro OUTPUT, PPSRCSTMF, TEMPLATE o MAKEDEP	*USE	*EXECUTE
	File specificato nel parametro OUTPUT, PPSRCSTMF, TEMPLATE o MAKEDEP	Fare riferimento alle regole generali.	*READ, *ADD
	Intestazioni generate dal parametro TEMPLATE	*USE	*EXECUTE
CRTBNDRPG	File di origine	*USE	*EXECUTE
	File unità e di database descritti esternamente cui si fa riferimento nel programma di origine	*OBJOPR	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Indirizzario di collegamento	*USE	*EXECUTE
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
CRTCBLMOD	File di origine	*USE	*EXECUTE
	File unità e di database descritti esternamente cui si fa riferimento nel programma di origine	*OBJOPR	*EXECUTE
	Modulo: REPLACE(*NO)		*READ, *ADD
	Modulo: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
CRTCLD	File di origine	*USE	*EXECUTE
	Oggetto locale - REPLACE(*NO)		*READ, *ADD
	Oggetto locale - REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
CRTCLMOD	File di origine	*USE	*EXECUTE
	Inclusione file	*USE	*EXECUTE
	File unità e di database descritti esternamente cui si fa riferimento nel programma di origine	*OBJOPR	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
CRTCLPGM	File di origine	*USE	*EXECUTE
	Inclusione file	*USE	*EXECUTE
	File unità e di database descritti esternamente cui si fa riferimento nel programma di origine	*OBJOPR	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
CRTCBLPGM (programma su licenza COBOL/400* o ambiente S/38)	File di origine	*USE	*EXECUTE
	File unità e di database descritti esternamente cui si fa riferimento nel programma di origine	*OBJOPR	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
CRTCMOD	File di origine	*USE	*EXECUTE
	File unità e di database descritti esternamente cui si fa riferimento nel programma di origine	*OBJOPR	*EXECUTE
	Modulo: REPLACE(*NO)		*READ, *ADD
	Modulo: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	File specificato nel parametro OUTPUT, PPSRCSTMF o MAKEDEP	*USE	*EXECUTE
	File specificato nel parametro OUTPUT, PPSRCSTMF o MAKEDEP	Fare riferimento alle regole generali.	*READ, *ADD

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTCPPMOD	File di origine	*USE	*EXECUTE
	File unità e di database descritti esternamente cui si fa riferimento nel programma di origine	*OBJOPR	*EXECUTE
	Modulo: REPLACE(*NO)		*READ, *ADD
	Modulo: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Indirizzario specificato nel parametro OUTPUT, PPSRCSTMF, TEMPLATE o MAKEDEP	*USE	*EXECUTE
	File specificato nel parametro OUTPUT, PPSRCSTMF, TEMPLATE o MAKEDEP	Fare riferimento alle regole generali.	*READ, *ADD
	Intestazioni generate dal parametro TEMPLATE	*USE	*EXECUTE
CRTRPGMOD	File di origine	*USE	*EXECUTE
	File unità e di database descritti esternamente cui si fa riferimento nel programma di origine	*OBJOPR	*EXECUTE
	Modulo: REPLACE(*NO)		*READ, *ADD
	Modulo: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
CRTRPGPGM (programma su licenza RPG/400* e ambiente S/38)	File di origine	*USE	*EXECUTE
	File unità e di database descritti esternamente cui si fa riferimento nel programma di origine	*OBJOPR	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
CRTRPTPGM (programma su licenza RPG/400 e ambiente S/38)	File di origine	*USE	*EXECUTE
	Programma - REPLACE(*NO)		*READ, *ADD
	Programma - REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	File origine per programma RPG generato	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	File unità e di database descritti esternamente cui si fa riferimento nel programma di origine	*OBJOPR	*EXECUTE
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
CRTS36CBL (ambiente S/36)	File di origine	*USE	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTS36RPG	File di origine	*USE	*READ, *ADD
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma - REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
CRTS36RPGR	File di origine	*USE	*READ, *ADD
	File di visualizzazione: REPLACE(*NO)		*READ, *ADD
	File di visualizzazione: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
CRTS36RPT	File di origine	*USE	*EXECUTE
	File origine per programma RPG generato	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
CRTSQLCI (DB2 Query Manager e SQL Development per programma su licenza i5/OS) [1]	File di origine	*OBJOPR, *READ	*EXECUTE
	Nel file di origine	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specifiche descrizione dati	*OBJOPR	*EXECUTE
	Oggetto: REPLACE(*NO)		*READ, *ADD
	Oggetto: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
CRTSQLCBL (DB2 Query Manager e SQL Development per programma su licenza i5/OS) [1]	File di origine	*OBJOPR, *READ	*EXECUTE
	Nel file di origine	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specifiche descrizione dati	*OBJOPR	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
CRTSQLCBLI (DB2 Query Manager e SQL Development per programma su licenza i5/OS) [1]	File di origine	*OBJOPR, *READ	*EXECUTE
	Nel file di origine	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specifiche descrizione dati	*OBJOPR	*EXECUTE
	Oggetto: REPLACE(*NO)		*READ, *ADD
	Oggetto: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTSQLCPPI (DB2 Query Manager e SQL Development per programma su licenza i5/OS) [1]	File di origine	*OBJOPR, *READ	*EXECUTE
	Nel file di origine	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specifiche descrizione dati	*OBJOPR	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
CRTSQLFTN (DB2 Query Manager e SQL Development per programma su licenza i5/OS) [1]	File di origine	*OBJOPR, *READ	*EXECUTE
	Nel file di origine	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specifiche descrizione dati	*OBJOPR	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
CRTSQLPLI (DB2 Query Manager e SQL Development per programma su licenza i5/OS) [1]	File di origine	*OBJOPR, *READ	*EXECUTE
	Nel file di origine	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specifiche descrizione dati	*OBJOPR	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
CRTSQLRPG (DB2 Query Manager e SQL Development per programma su licenza i5/OS) [1]	File di origine	*OBJOPR, *READ	*EXECUTE
	Nel file di origine	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specifiche descrizione dati	*OBJOPR	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTSQLRPGI (DB2 Query Manager e SQL Development per programma su licenza i5/OS) [1]	File di origine	*OBJOPR, *READ	*EXECUTE
	Nel file di origine	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specifiche descrizione dati	*OBJOPR	*EXECUTE
	Oggetto: REPLACE(*NO)		*READ, *ADD
	Oggetto: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
CVTRPGSRC	File di origine	*USE	*EXECUTE
	File di emissione	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	File di log	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
CVTSQLCPP [1]	File di origine	*OBJOPR, *READ	*EXECUTE
	Nel file di origine	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specifiche descrizione dati	*OBJOPR	*EXECUTE
	Programma: REPLACE(*NO)		*READ, *ADD
	Programma: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Tabella specificata nel parametro SRTSEQ	*USE	*EXECUTE
ENDCBLDBG (programma su licenza COBOL/400 o ambiente S/38)	Programma	*CHANGE	*EXECUTE
ENTCBLDBG (ambiente S/38)	Programma	*CHANGE	*EXECUTE
DLTCLD	Oggetto locale	*OBJEXIST, *OBJMGT	*EXECUTE
INCLUDE	File di origine	*USE	*EXECUTE
RTVCLDSRC	Oggetto locale	*USE	*EXECUTE
	A file	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
RUNSQLSTM[1]	File di origine	*OBJOPR, *READ	*EXECUTE
STRCBLDBG	Programma	*CHANGE	*EXECUTE
STRREXPRC	File di origine	*USE	*EXECUTE
	Programma di uscita	*USE	*EXECUTE
STRSQL (DB2 Query Manager e SQL Development per programma su licenza i5/OS) [1]	Tabella sequenza ordinamento	*USE	*EXECUTE
	Descrizione unità stampante	*USE	*EXECUTE
	Coda emissione di stampa	*USE	*EXECUTE
	File di stampa	*USE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
[1] Consultare Authorization, privileges and object ownership per ulteriori informazioni sui requisiti di sicurezza per le istruzioni SQL (structured query language).			

Comandi libreria

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi libreria.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per la libreria su cui si lavora
ADDLIBLE	Libreria		*USE
CHGCURLIB	Nuova libreria corrente		*USE
CHGLIB [8]	Libreria		*OBJMGT
CHGLIBL	Tutte le librerie inserite nell'elenco delle librerie		*USE
CHGSYSLIBL (Q)	Librerie nel nuovo elenco		*USE
CLRLIB [3]	Tutti gli oggetti cancellati dalla libreria	*OBJEXIST	*USE
	Tipi di oggetto *DTADCT[14], *JRN[14],*JRNRCV[14], *MSGQ[14], *SBSD[14]	Verificare l'autorizzazione richiesta dal comando DLT*xxx* per il tipo di oggetto	
	Unità ASP (se specificata)	*USE	
CPYLIB [4]	Libreria di provenienza		*USE
	Libreria di destinazione, se presente		*USE, *ADD
	Comandi CHKOBJ, CRTDUPOBJ	*USE	
	Comando CRTLIB, se la creazione della libreria di destinazione è in corso	*USE	
	Oggetto copiato	L'autorizzazione necessaria quando si utilizza il comando CRTDUPOBJ per copiare il tipo di oggetto.	
CRTLIB [9]	Unità ASP (se specificata)	*USE	

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per la libreria su cui si lavora**
DLTLIB [3]	Tutti gli oggetti cancellati dalla libreria	*OBJEXIST	*USE, *OBJEXIST
	Tipi di oggetto *DTADCT[14], *JRN[14],*JRNRCV[14], *MSGQ, *SBSD[14]	Verificare l'autorizzazione richiesta dal comando DLT*xxx* per il tipo di oggetto	
	Unità ASP (se specificata)	*USE	
DSPLIB	Libreria		*READ
	Oggetti presenti nella libreria [5]	Autorizzazione diversa da *EXCLUDE	
	Unità ASP (se specificata)	*EXECUTE	
DSPLIBD	Libreria		Autorizzazione diversa da *EXCLUDE
EDTLIBL	Libreria da aggiungere all'elenco		*USE
RCLLIB	Libreria		*USE, *OBJEXIST
RSTLIB (Q)[7, 17, 19]	Definizione supporto magnetico	*USE	*EXECUTE
	Libreria, se esiste		*READ, *ADD
	Code messaggi ripristinate sulla libreria in cui esistono già	*OBJOPR, *OBJEXIST [7]	*EXECUTE. *READ, *ADD
	Programmi che adottano l'autorizzazione	Proprietario di *ALLOBJ e *SECADM	*EXECUTE
	Libreria salvata se specificato VOL(*SAVVOL)		*USE [6]
	Tutti gli oggetti ripristinati nella libreria	*OBJEXIST [3]	*EXECUTE, *READ, *ADD
	Profilo utente proprietario degli oggetti creati	*ADD [6]	
	Unità nastro, unità minidisco, unità ottica	*USE	*EXECUTE
	File di emissione, se specificato	Consultare Regole generali	Consultare Regole generali
	File di riferimento campo QSYS/QASAVOBJ per il file di emissione, se viene specificato un file di emissione che non esiste	*USE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per la libreria su cui si lavora
RSTLIB (Q)	File nastro (QSYSTAP) o minidisco (QSYSDKT)	*USE [6]	*EXECUTE
	Emissione di stampa QSYS/QPSRLDSP, se è specificato OUTPUT(*PRINT)	*USE	*EXECUTE
	Salvataggio file	*USE	*EXECUTE
	File unità ottica (OPTFILE)[12]	*R	Non applicabili
	Prefisso percorso del file unità ottica (OPTFILE)[12]	*X	Non applicabili
	Volume unità ottica[11]	*USE	
	Descrizione unità ASP[15]	*USE	
RSTS36LIBM	Da file	*USE	*EXECUTE
	A file	*CHANGE	*EXECUTE
	Libreria di destinazione	*CHANGE	*EXECUTE
	File unità o descrizione unità	*USE	*EXECUTE
RTVLIBD	Libreria		Autorizzazione diversa da *EXCLUDE
SAVLIB[18]	Tutti gli oggetti nella libreria	*OBJEXIST [6]	*READ, *EXECUTE
	Definizione supporto magnetico	*USE	*EXECUTE
	File di salvataggio, se vuoto	*USE, *ADD	*EXECUTE
	Salvare il file, se contiene i record	*USE, *ADD, *OBJMGT	*EXECUTE
	Salvataggio coda messaggi attivi	*OBJOPR, *ADD	*EXECUTE
	Unità nastro, unità minidisco, unità ottica	*USE	*EXECUTE
	File di emissione, se specificato	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	File di riferimento campo QSYS/QASAVOBJ, se il file di emissione è specificato e non presente	*USE [6]	*EXECUTE
	Emissione di stampa QSYS/QPSAVOBJ	*USE [6]	*EXECUTE
	Spazio utente del comando, se specificato	*USE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per la libreria su cui si lavora**
SAVLIB	File unità ottica[12]	*RW	Non applicabili
	Indirizzario principale file unità ottica (OPTFILE)[12]	*WX	Non applicabili
	Prefisso percorso del file unità ottica (OPTFILE)[12]	*X	Non applicabili
	Indirizzario root (/) del Volume unità ottica[12, 13]	*RWX	Non applicabili
	Volume unità ottica[11]	*CHANGE	
	Descrizione unità ASP[15]	*USE	
SAVRSTLIB	Sul sistema di origine, è richiesta la stessa autorizzazione del comando SAVLIB.		
	Sul sistema di destinazione, è richiesta la stessa autorizzazione del comando RSTLIB.		
SAVS36LIBM	Salvataggio in file fisico	*OBJOPR, *OBJMGT	*EXECUTE
	QSYSDKT per minidischi o QSYSTAP per nastro e tutti i comandi necessitano di autorizzazione all'unità	*OBJOPR	*EXECUTE
	Salvataggio in file fisico, se specificato MBROPT(*ADD)	*ADD	*READ, *ADD
	Salvataggio in file fisico, se specificato MBROPT(*REPLACE)	*ADD, *DLT	*EXECUTE
	Libreria di partenza		*USE
WRKLIB [10, 16]	Libreria		*USE

[1] L'autorizzazione necessaria per la libreria su cui si sta operando è indicata in questa colonna. Ad esempio per aggiungere la libreria CUSTLIB all'elenco delle librerie utilizzando il comando ADDLIBLE è necessario disporre di autorizzazione all'utilizzo per la libreria CUSTLIB.

[2] L'autorizzazione necessaria per la libreria QSYS viene indicata in questa colonna in quanto tutte le librerie si trovano nella libreria QSYS.

[3] Se per alcuni oggetti presenti nella libreria non viene rinvenuta l'esistenza oggetti, questi non vengono cancellati e la libreria non viene completamente eliminata e cancellata. Vengono cancellati solo gli oggetti per cui è presente l'autorizzazione.

[4] Tutte le limitazioni applicate al comando CRTDUPOBJ, si applicano anche a questo comando.

[5] Se non si dispone di autorizzazione a un oggetto presente nella libreria, il testo per l'oggetto indicherà *NOT AUTHORIZED.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per la libreria su cui si lavora
[6] Se si dispone dell'autorizzazione speciale *SAVSYS, non è necessaria l'autorizzazione specificata.			
[7] È necessario disporre dell'autorizzazione speciale *ALLOBJ per specificare un valore diverso da *NONE per il parametro ALWOBJDIF (Consenso differenze oggetto).			
[8] Per modificare il valore CRTOBJAUD per una libreria, è necessario disporre dell'autorizzazione speciale *AUDIT. Se si modifica solo il valore CRTOBJAUD, **non** è necessario *OBJMGT. *OBJMGT **è** necessario se si modifica il valore CRTOBJAUD e altri valori.			
[9] Per specificare un valore CRTOBJAUD diverso da *SYSVAL, è necessario disporre dell'autorizzazione speciale *AUDIT.			
[10] È necessario disporre dell'autorizzazione richiesta dall'operazione per utilizzare una singola operazione.			
[11] I volumi dell'unità ottica non sono oggetti di sistema effettivi. Il collegamento tra il volume dell'unità ottica e l'elenco di autorizzazioni utilizzato per proteggere il volume viene gestito dalla funzione di supporto dell'unità ottica.			
[12] La verifica dell'autorizzazione viene effettuata solo quando il formato supporto magnetico dell'unità ottica corrisponde all'UDF (Universal Disk Format).			
[13] La verifica dell'autorizzazione viene effettuata solo quando si sta ripulendo il volume ottico.			
[14] Questo oggetto è consentito su ASP indipendenti.			
[15] Autorizzazione necessaria solo se l'operazione di salvataggio o ripristino richiede uno switch dello spazio nome libreria.			
[16] Questo comando richiede l'autorizzazione speciale *ALLOBJ.			
[17] È necessario disporre dell'autorizzazione special *ALLOBJ per specificare *YES per il parametro PVTAUT.			
[18] È necessario disporre delle autorizzazioni speciali *ALLOBJ o *SAVSYS per specificare *YES per il parametro PVTAUT.			
[19] È necessario disporre dell'autorizzazione speciale *SAVSYS per specificare un nome per il parametro DFRID.			

Comandi chiave di licenza

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi chiave di licenza.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ADDLICKEY (Q)	File di emissione	*USE	*EXECUTE
DSPLICKEY (Q)	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
RMVLICKEY (Q)	File di emissione	*CHANGE	*EXECUTE

Comandi programma su licenza

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi programma su licenza.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

		Autorizzazione necessaria	
Comando	**Oggetto di riferimento**	**Per oggetto**	**Per libreria**
CHGLICINF (Q)	comando WRKLICINF	*USE	*EXECUTE
DLTLICPGM [1,2] (Q)			
DSPTM			
INZSYS (Q)			
RSTLICPGM [1,2] (Q)			
SAVLICPGM [1,2] (Q)			
WRKLICINF (Q)			

[1] È possibile cancellare, salvare o ripristinare alcuni programmi su licenza solo se si è registrati nell'indirizzario di distribuzione del sistema.

[2] Se si cancella, ripristina o si salva un programma su licenza che contiene cartelle, tutte le restrizioni relative al comando DLTDLO vengono applicate a tale comando.

[3] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

Comandi descrizione linea

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi descrizione linea.

		Autorizzazione necessaria	
Comando	**Oggetto di riferimento**	**Per oggetto**	**Per libreria**
CHGLINASC [2]	Descrizione linea	*CHANGE, *OBJMGT	*EXECUTE
	Descrizione unità di controllo (SWTCTLLST)	*USE	*EXECUTE
CHGLINBSC [2]	Descrizione linea	*CHANGE, *OBJMGT	*EXECUTE
	Descrizione unità di controllo (SWTCTLLST)	*USE	*EXECUTE
CHGLINDDI [2]	Descrizione linea	*CHANGE, *OBJMGT	*EXECUTE
CHGLINETH [2]	Descrizione linea	*CHANGE, *OBJMGT	*EXECUTE
CHGLINFAX [2]	Descrizione linea	*CHANGE, *OBJMGT	*EXECUTE
CHGLINFR [2]	Descrizione linea	*CHANGE, *OBJMGT	*EXECUTE
CHGLINPPP[2]	Descrizione linea	*CHANGE, *OBJMGT	*EXECUTE
CHGLINSDLC [2]	Descrizione linea	*CHANGE, *OBJMGT	*EXECUTE
CHGLINTDLC [2]	Descrizione linea	*CHANGE, *OBJMGT	*EXECUTE
CHGLINTRN [2]	Descrizione linea	*CHANGE, *OBJMGT	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGLINX25 [2]	Descrizione linea	*CHANGE, *OBJMGT	*EXECUTE
	Descrizione unità di controllo (SWTCTLLST)	*USE	*EXECUTE
	Elenco collegamenti (CNNLSTIN o CNNLSTOUT)	*USE	*EXECUTE
	Descrizione interfaccia di rete (SWTNWILST)	*USE	*EXECUTE
CHGLINWLS [2]	Descrizione linea	*CHANGE, *OBJMGT	*EXECUTE
	Programma (INZPGM)	*USE	*EXECUTE
CRTLINASC [2]	Descrizione unità di controllo (CTL e SWTCTLLST)	*USE	*EXECUTE
	Descrizione linea		*READ, *ADD
CRTLINBSC [2]	Descrizione unità di controllo (SWTCTLLST e CTL)	*USE	*EXECUTE
	Descrizione linea		*READ, *ADD
CRTLINDDI [2]	Descrizione linea		*READ, *ADD
	Descrizione interfaccia di rete (NWI)	*USE	*EXECUTE
	Descrizione unità di controllo (NETCTL)	*USE	*EXECUTE
CRTLINETH [2]	Descrizione unità di controllo (NETCTL)	*USE	*EXECUTE
	Descrizione linea		*READ, *ADD
	Descrizione interfaccia di rete (NWI)	*USE	*EXECUTE
	Descrizione server di rete (NWS)	*USE	*EXECUTE
CRTLINFAX [2]	Descrizione linea		*READ, *ADD
	Descrizione unità di controllo	*USE	*EXECUTE
CRTLINFR [2]	Descrizione linea		*READ, *ADD
	Descrizione interfaccia di rete (NWI)	*USE	*EXECUTE
	Descrizione unità di controllo (NETCTL)	*USE	*EXECUTE
CRTLINPPP[2]	Descrizione unità di controllo (NETCTL)	*USE	*EXECUTE
	Descrizione linea		*READ, *ADD
CRTLINSDLC [2]	Descrizione unità di controllo (CTL)	*USE	*EXECUTE
	Descrizione linea		*READ, *ADD
CRTLINTDLC [2]	Descrizione unità di controllo (WSC e CTL)	*USE	*EXECUTE
	Descrizione linea		*READ, *ADD
CRTLINTRN [2]	Descrizione unità di controllo (NETCTL)	*USE	*EXECUTE
	Descrizione linea		*READ, *ADD
	Descrizione interfaccia di rete (NWI)	*USE	*EXECUTE
	Descrizione server di rete (NWS)	*USE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTLINX25 [2]	Descrizione unità di controllo (SWTCTLLST)	*USE	*EXECUTE
	Descrizione unità di controllo PVC (Permanent virtual circuit) (LGLCHLE)	*USE	*EXECUTE
	Descrizione linea		*READ, *ADD
	Elenco collegamenti (CNNLSTIN o CNNLSTOUT)	*USE	*EXECUTE
	Descrizione interfaccia di rete (NWI o SWTNWILST)	*USE	*EXECUTE
CRTLINWLS [2]	Descrizione linea		*READ, *ADD
	Descrizione unità di controllo (NETCTL)	*USE	*EXECUTE
	Programma (INZPGM)	*USE	*EXECUTE
DLTLIND	Descrizione linea	*OBJEXIST	*EXECUTE
DSPLIND	Descrizione linea	*USE	*EXECUTE
ENDLINRCY	Descrizione linea	*OBJOPR	*EXECUTE
PRTCMNSEC [2, 3]			
RSMLINRCY	Descrizione linea	*OBJOPR	*EXECUTE
WRKLIND [1]	Descrizione linea	*OBJOPR	*EXECUTE

[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

[2] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *IOSYSCFG.

[3] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *ALLOBJ.

Comandi LAN (Local Area Network)

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi LAN (Local Area Network).

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Questi comandi non richiedono le autorizzazioni agli oggetti:			
ADDLANADPI CHGLANADPI	DSPLANADPP DSPLANSTS	RMVLANADPT (Q) RMVLANADPI	WRKLANADPT

Comandi locale

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi locale.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTLOCALE	File di origine	*USE	*USE, *ADD
DLTLOCALE	Locale	*OBJEXIST	*EXECUTE

Comandi framework server di posta

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi framework server di posta.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Questo comando non richiede autorizzazioni oggetto:			
ENDMSF (Q)	STRMSF (Q)		

Comandi supporto magnetico

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi relativi al supporto magnetico.

		Autorizzazione necessaria	
Comando	**Oggetto di riferimento**	**Per oggetto**	**Per libreria**
ADDTAPCTG	Descrizione libreria nastro	*USE	*EXECUTE
CFGDEVMLB[1]	Descrizione libreria nastro	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVMLB (Q)	Descrizione libreria nastro	*CHANGE, *OBJMGT	*EXECUTE
CHGJOBMLBA[4]	Descrizione libreria nastro	*CHANGE	*EXECUTE
CHGTAPCTG	Descrizione libreria nastro	*USE	*EXECUTE
CHKDKT	Descrizione unità minidisco	*USE	*EXECUTE
CHKTAP	Descrizione unità nastro	*USE	*EXECUTE
CLRDKT	Descrizione unità minidisco	*USE	*EXECUTE
CRTTAPCGY	Descrizione libreria nastro		
DLTDKTLBL	Descrizione unità minidisco	*USE	*EXECUTE
DLTMEDDFN	Definizione supporto magnetico	*OBJEXIST	*EXECUTE
DLTTAPCGY	Descrizione libreria nastro		
DMPTAP (Q)[5]	Descrizione unità nastro	*USE	*EXECUTE
DSPDKT	Descrizione unità minidisco	*USE	*EXECUTE
DSPTAP	Descrizione unità nastro	*USE	*EXECUTE
DSPTAPCGY	Descrizione libreria nastro		
DSPTAPCTG	Descrizione libreria nastro	*USE	*EXECUTE
DSPTAPSTS	Descrizione libreria nastro	*USE	*EXECUTE
DUPDKT	Descrizione unità minidisco	*USE	*EXECUTE
DUPTAP	Descrizione unità nastro	*USE	*EXECUTE
INZDKT	Descrizione unità minidisco	*USE	*EXECUTE
INZTAP	Descrizione unità nastro	*USE	*EXECUTE
RMVTAPCTG	Descrizione libreria nastro	*USE	*EXECUTE
RNMDKT	Descrizione unità minidisco	*USE	*EXECUTE
SETTAPCGY	Descrizione libreria nastro	*USE	*EXECUTE
WRKMLBRSCQ [3]	Descrizione libreria nastro	*USE	*EXECUTE
WRKMLBSTS [2] (Q)	Descrizione libreria nastro	*USE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
WRKTAPCTG	Descrizione libreria nastro	*USE	*EXECUTE

[1] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *IOSYSCFG.

[2] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione necessaria per l'operazione.

[3] Per modificare gli attributi della libreria supporto magnetico della sessione, è necessario disporre dell'autorizzazione *CHANGE per la descrizione Libreria nastro. Per modificare la priorità o gestire il lavoro di un altro utente è necessario disporre dell'autorizzazione speciale *JOBCTL.

[4] Per modificare la priorità o gestire il lavoro di un altro utente è necessario disporre dell'autorizzazione speciale *JOBCTL.

[5] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *ALLOBJ quando si specifica TYPE(*HEX) o il nastro dispone dell'indicatore di volume protetto o della serie di indicatori file protetti.

Comandi menu e gruppo pannelli

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi menu e gruppo pannelli.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
CHGMNU	Menu	*CHANGE	*USE
CRTMNU	File di origine	*USE	*EXECUTE
	Menu: REPLACE(*NO)		*READ, *ADD
	Menu: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
CRTPNLGRP	Gruppo pannelli: Replace(*NO)		*READ, *ADD
	Gruppo pannelli: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	File di origine	*USE	*EXECUTE
	Inclusione file	*USE	*EXECUTE
CRTS36MNU	Menu: REPLACE(*NO)		*READ, *ADD
	Menu: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	File di origine	*USE	*EXECUTE
	File di messaggi denominati nell'origine	*OBJOPR, *OBJEXIST	*EXECUTE
	File di origine a file quando TOMBR non è *NONE	*OBJOPR, *OBJMGT, *OBJEXIST, *ADD	*READ, *ADD
	File di visualizzazione menu quando viene specificato REPLACE(*YES)	*OBJOPR, *OBJEXIST	*EXECUTE
	File di messaggio testo comando	*OBJOPR, *OBJEXIST	*EXECUTE
	Comando CRTMSGF (Creazione file messaggi)	*OBJOPR	*EXECUTE
	Comando ADDMSGD (Aggiunta descrizione messaggio)	*OBJOPR	*EXECUTE
	Comando CRTDSPF (Creazione file di visualizzazione)	*OBJOPR	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
DLTMNU	Menu	*OBJOPR, *OBJEXIST	*EXECUTE
DLTPNLGRP	Gruppo pannelli	*OBJEXIST	*EXECUTE
DSPMNUA	Menu	*USE	*USE
GO	Menu	*USE	*USE
	Visualizzazione file e file di messaggi con *DSPF specificato	*USE	*EXECUTE
	Librerie prodotto e correnti	*USE	
	Programma con *PGM specificato	*USE	*EXECUTE
WRKMNU [1]	Menu	Qualunque valore	*USE
WRKPNLGRP [1]	Gruppo pannelli	Qualunque valore	*EXECUTE
[1] Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.			

Comandi messaggi

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi messaggi.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
DSPMSG	Coda messaggi	*USE	*USE
	Coda messaggi che riceve la risposta a un messaggio di interrogazione	*USE, *ADD	*USE
	Rimozione messaggi dalla coda messaggi	*USE, *DLT	*USE
RCVMSG	Coda messaggi	*USE	*EXECUTE
	Rimozione messaggi dalla coda	*USE, *DLT	*EXECUTE
RMVMSG	Coda messaggi	*OBJOPR, *DLT	*EXECUTE
RTVMSG	File di messaggi	*USE	*EXECUTE
SNDBRKMSG	Coda messaggi che riceve la risposta ai messaggi di interrogazione	*OBJOPR, *ADD	*EXECUTE
SNDMSG	Coda messaggi	*OBOPR, *ADD	*EXECUTE
	Coda messaggi che riceve la risposta a un messaggio di interrogazione	*OBJOPR, *ADD	*EXECUTE
SNDPGMMSG	Coda messaggi	*OBJOPR, *ADD	*EXECUTE
	File messaggi, quando si invia il messaggio predefinito	*USE	*EXECUTE
	Coda messaggi che riceve la risposta a un messaggio di interrogazione	*OBJOPR, *ADD	*EXECUTE
SNDRPY	Coda messaggi	*USE, *ADD	*EXECUTE
	Rimozione messaggi dalla coda	*USE, *ADD, *DLT	*EXECUTE
SNDUSRMSG	Coda messaggi	*OBJOPR, *ADD	*EXECUTE
	File messaggi, quando si invia il messaggio predefinito	*USE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
WRKMSG	Coda messaggi	*USE	*USE
	Coda messaggi che riceve la risposta a un messaggio di interrogazione	*USE, *ADD	*USE
	Rimozione messaggi dalla coda messaggi	*USE, *DLT	*USE

Comandi descrizione messaggio

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi descrizione messaggio.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDMSGD	File di messaggi	*USE, *ADD	*EXECUTE
CHGMSGD	File di messaggi	*USE, *UPD	*EXECUTE
DSPMSGD	File di messaggi	*USE	*EXECUTE
RMVMSGD	File di messaggi	*OBJOPR, *DLT	*EXECUTE
WRKMSGD [1]	File di messaggi	*USE	*EXECUTE

[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

Comandi file messaggi

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi file messaggi.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGMSGF	File di messaggi	*USE, *DLT	*EXECUTE
CRTMSGF	File di messaggi		*READ, *ADD
DLTMSGF	File di messaggi	*OBJEXIST	*EXECUTE
DSPMSGF	File di messaggi	*USE	*EXECUTE
MRGMSGF	File messaggi di provenienza	*USE	*EXECUTE
	File messaggi di destinazione	*USE, *ADD, *DLT	*EXECUTE
	File messaggi di sostituzione	*USE, *ADD	*EXECUTE
WRKMSGF [1.]	File di messaggi	Qualsiasi autorizzazione	*USE

[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

Comandi coda messaggi

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi coda messaggi.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGMSGQ	Coda messaggi	*USE, *DLT	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CLRMSGQ	Coda messaggi	*OBJOPR, *DLT	*EXECUTE
CRTMSGQ	Coda messaggi		*READ, *ADD
DLTMSGQ	Coda messaggi	*OBJEXIST, *USE, *DLT	*EXECUTE
DSPLOG			*EXECUTE
WRKMSGQ [1]	Coda messaggi	Qualsiasi autorizzazione	*USE
[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.			

Comandi migrazione

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi migrazione.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
RCVMGRDTA	File	*ALL	*READ, *ADD
	Unità	*CHANGE	*EXECUTE
SNDMGRDTA	File	*ALL	*READ, *ADD
	Unità	*CHANGE	*EXECUTE
I seguenti comandi non richiedono un'autorizzazione per l'oggetto. Essi vengono forniti con l'autorizzazione pubblica *EXCLUDE. È necessario disporre dell'autorizzazione speciale *ALLOBJ per utilizzare tali comandi.			
ANZS34OCL ANZS36OCL CHGS34LIBM CHKS36SRCA CVTBASSTR CVTBASUNF CVTBGUDTA CVTS36FCT	CVTS36JOB CVTS38JOB GENS36RPT GENS38RPT MGRS36 MGRS36APF [1] MGRS36CBL MGRS36DFU [1]	MGRS36DSPF MGRS36ITM MGRS36LIB MGRS36MNU MGRS36MSGF MGRS36QRY [1] MGRS36RPG MGRS36SEC MGRS38OBJ	MIGRATE QMUS36 RESMGRNAM RSTS38AUT STRS36MGR STRS38MGR
[1] È necessario disporre dell'autorizzazione speciale *ALLOBJ ed è necessario che l'opzione 4 di i5/OS sia installata.			

Comandi descrizione modalità

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi descrizione modalità.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGMODD [2]	Descrizione modalità	*CHANGE, *OBJMGT	*EXECUTE
CRTMODD [2]	Descrizione modalità		*READ, *ADD
CHGSSNMAX	Descrizione unità	*OBJOPR	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
DLTMODD	Descrizione modalità	*OBJEXIST	*EXECUTE
DSPMODD	Descrizione modalità	*USE	*EXECUTE
DSPMODSTS	Unità	*OBJOPR	*EXECUTE
	Descrizione modalità	*OBJOPR	*EXECUTE
ENDMOD	Descrizione unità	*OBJOPR	*EXECUTE
STRMOD	Descrizione unità	*OBJOPR	*EXECUTE
WRKMODD [1]	Descrizione modalità	*OBJOPR	*EXECUTE

[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

[2] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *IOSYSCFG.

Comandi modulo

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi modulo.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGMOD	Modulo	*OBJMGT, *USE	*USE
	Modulo, se OPTIMIZE è specificato	*OBJMGT, *USE	*USE, *ADD, *DLT
	Modulo, se FRCCRT(*YES) è specificato	*OBJMGT, *USE	*USE, *ADD, *DLT
	Modulo, se ENBPRFCOL è specificato	*OBJMGT, *USE	*USE, *ADD, *DELETE
DLTMOD	Modulo	*OBJEXIST	*EXECUTE
DSPMOD	Modulo	*USE	*EXECUTE
RTVBNDSRC [1]	Modulo	*USE	*EXECUTE
	*SRVPGMs e i moduli specificati con *SRVPGMs	*USE	*EXECUTE
	File di origine database se il file e il membro sono presenti e MBROPT(*REPLACE) è specificato.	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	File di origine database se il file e il membro sono presenti e MBROPT(*ADD) è specificato	*OBJOPR, *ADD	*EXECUTE
	File di origine database se il file è presente ed è necessario creare il membro.	*OBJOPR, *OBJMGT, *ADD	*EXECUTE, *READ, *ADD
	File di origine database se è necessario creare il file e il membro.		*EXECUTE, *READ, *ADD
	Comando CRTSCRPF se il file non è presente		*EXECUTE
	Comando ADDPFM se il membro non è presente		*EXECUTE
	Comando RGZPFM per riorganizzare il membro del file di origine	*OBJMGT	*EXECUTE
WRKMOD [2]	Modulo	Qualsiasi autorizzazione	*USE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**

[1] È necessario disporre dell'autorizzazione *USE per il:
- Comando CRTSRCPF se il file non è presente.
- Comando ADDPFM se il membro non è presente.
- Comando RGZPFM in modo tale che il membro del file di origine venga riorganizzato. È necessario disporre dell'autorizzazione *CHANGE, *OBJALTER o *OBJMGT per riorganizzare il membro del file di origine. La funzione del comando RTVBNDSRC viene completata con il membro del file di origine riorganizzato con il numero sequenza corrispondente a zero.

[2] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

Comandi descrizione NetBIOS

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi descrizione NetBIOS.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGNTBD [2]	Descrizione NetBIOS	*CHANGE, *OBJMGT	*EXECUTE
CRTNTBD [2]	Descrizione NetBIOS		*EXECUTE
DLTNTBD	Descrizione NetBIOS	*OBJEXIST	*EXECUTE
DSPNTBD	Descrizione NetBIOS	*USE	*EXECUTE
WKRNTBD[1]	Descrizione NetBIOS	*OBJOPR	*EXECUTE

[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

[2] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *IOSYSCFG.

Comandi rete

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi rete.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDNETJOBE (Q)	Profilo utente nella voce lavoro di rete	*USE	
APING	Descrizione unità	*CHANGE	
AREXEC	Descrizione unità	*CHANGE	
CHGNETA (Q) [4]			
CHGNETJOBE (Q)	Profilo utente nella voce lavoro di rete	*USE	
DLTNETF [2]	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
DSPNETA			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
RCVNETF [2]	Il membro del file di destinazione non è presente, MBROPT(*ADD) specificato	*OBJMGT, *USE	*EXECUTE, *ADD
	Il membro del file di destinazione non è presente, MBROPT(*REPLACE) specificato	*OBJMGT, *CHANGE	*EXECUTE, *ADD
	Membro del file di destinazione presente, MBROPT(*ADD) specificato	*USE	*EXECUTE
	Membro del file di destinazione presente, MBROPT(*REPLACE) specificato	*OBJMGT, *CHANGE	*EXECUTE
RMVNETJOBE (Q)	Profilo utente nella voce lavoro di rete	*USE	
RTVNETA			
RUNRMTCMD	Descrizione unità	*CHANGE	
SNDNETF	File fisico o salvataggio file	*USE	*EXECUTE
SNDNETMSG su un utente locale	Coda messaggi	*OBJOPR, *ADD	*EXECUTE
VFYAPPCCNN	Descrizione unità	*CHANGE	
WRKNETF [2,3]			
WRKNETJOBE [3]	QUSRSYS/QANFNJE	*USE	*EXECUTE

[1] È necessario disporre dell'autorizzazione speciale *ALLOBJ.

[2] Un utente può eseguire questi comandi sui file di rete di proprietà dell'utente o sui file di rete di proprietà del profilo di gruppo dell'utente. È necessario disporre dell'autorizzazione speciale *ALLOBJ per elaborare i file di rete per un altro utente.

[3] Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta da tale operazione.

[4] Per modificare alcuni attributi di rete, è necessario disporre delle autorizzazioni speciali *IOSYSCFG o *ALLOBJ e *IOSYSCFG.

Comandi NFS (Network file system)

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi NFS (network file system).

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto
ADDMFS [1,3]	dir_to_be_ mounted_over	*DIR	"root" (/)	*W
CHGNFSEXP [1,2]	Prefisso percorso	Fare riferimento alle regole generali.		
DSPMFSINF	some_dirs	*DIR	"root" (/)	*RX
	Prefisso percorso	Fare riferimento alle regole generali.		
ENDNFSSVR [1,4]	nessuno			
EXPORTFS [1,2]	Prefisso percorso	Fare riferimento alle regole generali.		
MOUNT [1,3]	dir_to_be_ mounted_over	*DIR	"root" (/)	*W
RLSIFSLCK [1]	oggetto	*STMF	"root" (/), QOpenSys, UDFS	*R
	Prefisso percorso	Fare riferimento alle regole generali.		
RMVMFS [1]				

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto
STATFS	some_dirs	*DIR	″root″ (/)	*RX
	Prefisso percorso	Fare riferimento alle regole generali.		
STRNFSSVR [1]	nessuno			
UNMOUNT [1]				

[1] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *IOSYSCFG.

[2] Quando si specifica l'indicatore -F e il file /etc/exports non è presente, è necessario disporre dell'autorizzazione alla scrittura e all'esecuzione (*WX) per l'indirizzario /etc. Quando si specifica l'indicatore -F e il file /etc/exports è presente, è necessario disporre dell'autorizzazione alla scrittura e alla lettura (*RW) per il file /etc/exports e dell'autorizzazione *X per l'indirizzario /etc.

[3] L'indirizzario caricato (dir_to_be_mounted_over) è un qualsiasi indirizzario file system integrato che può essere caricato.

[4] Per terminare qualsiasi lavoro daemon avviato da un altro utente, è necessario disporre dell'autorizzazione speciale *JOBCTL.

Comandi descrizione interfaccia di rete

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi descrizione interfaccia di rete.

		Autorizzazione necessaria	
Comando	Oggetto di riferimento	Per oggetto	Per libreria
CHGNWIFR [2]	Descrizione interfaccia di rete	*CHANGE, *OBJMGT	*EXECUTE
CRTNWIFR [2]	Descrizione interfaccia di rete		*READ, *ADD
	Descrizione linea (DLCI)	*USE	*EXECUTE
DLTNWID	Descrizione interfaccia di rete	*OBJEXIST	*EXECUTE
DSPNWID	Descrizione interfaccia di rete	*USE	*EXECUTE
WRKNWID [1]	Descrizione interfaccia di rete	*OBJOPR	*EXECUTE

[1] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta dall'operazione.

[2] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *IOSYSCFG.

Comandi server di rete

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi server di rete.

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto
ADDNWSSTGL [2]	Percorso (/QFPNWSSTG)	*DIR	″root″ (/)	*X
	Indirizzario principale (nome dello spazio di memoria)	*DIR	″root″ (/)	*WX
	File che compongono lo spazio di memoria	*STMF	″root″ (/)	*RW
	Descrizione server di rete	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto
CHGNWSSTG[2]	Percorso (root e /QFPNWSSTG)	*DIR	″root″ (/)	*WX
CHGNWSUSRA [4]	Profilo utente	*USRPRF		*OBJMGT, *USE
CRTNWSSTG [2]	Percorso (root e /QFPNWSSTG)	*DIR	″root″ (/)	*WX
DLTNWSSTG [2]	Percorso (/QFPNWSSTG)	*DIR	″root″ (/)	*WX
	Indirizzario principale (nome dello spazio di memoria)	*DIR	″root″ (/)	*RWX, *OBJEXIST
	File che compongono lo spazio di memoria	*STMF	″root″ (/)	*OBJEXIST
DLTWNTSVR[5]	Descrizione server di rete	*NWSD	QSYS.LIB	*OBJEXIST
	Descrizione linea	*LIND	QSYS.LIB	*OBJEXIST
	Configurazione server di rete	*NWSCFG	QSYS.LIB	*OBJEXIST
	Spazio memoria server di rete - Percorso (/QFPNWSSTG)	*DIR	″root″ (/)	*WX
	Indirizzario principale (nome dello spazio di memoria)	*DIR	″root″ (/)	*RWX, *OBJEXIST
	File che compongono lo spazio di memoria	*STMF	″root″ (/)	*OBJEXIST
DSPNWSSTG	Prefisso percorso	Fare riferimento alle regole generali		
	File che compongono lo spazio di memoria	*STMF	″root″ (/)	*R
INSWNTSVR[6, 7]	Descrizione server di rete	*NWSD	Non applicabili	*USE
	Descrizione linea	*LIND	Non applicabili	*USE
	Configurazione server di rete	*NWSCFG	Non applicabili	*USE
	Spazio memoria server di rete - Percorso (/QFPNWSSTG)	*DIR	″root″ (/)	*WX
RMVNWSSTGL [2]	Percorso (/QFPNWSSTG)	*DIR	″root″ (/)	*X
	Indirizzario principale (nome dello spazio di memoria)	*DIR	″root″ (/)	*WX
	File che compongono lo spazio di memoria	*STMF	″root″ (/)	*RW
	Descrizione server di rete	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
WRKNWSSTG	Prefisso percorso	Fare riferimento alle regole generali		
	File che compongono lo spazio di memoria	*STMF	″root″ (/)	*R
Questi comandi non richiedono le autorizzazioni agli oggetti:				

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto
ADDRMTSVR CHGNWSA [4](Q) CHGNWSALS CRTNWSALS DLTNWSALS DSPNWSA	DSPNWSALS DSPNWSSSN DSPNWSSTC DSPNWSUSRA SBMNWSCMD (Q) [3]		SNDNWSMSG WRKNWSALS WRKNWSENR WRKNWSSSN WRKNWSSTS	

[1] Autorizzazione adottata non utilizzata per i comandi Server di rete.

[2] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *IOSYSCFG.

[3] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *JOBCTL.

[4] È necessario disporre dell'autorizzazione speciale *SECADM per specificare un valore diverso da *NONE per i parametri NDSTREELST e NTW3SVRLST.

[5] Per utilizzare questo comando, è necessario disporre delle autorizzazioni speciali *IOSYSCFG e *ALLOBJ.

[6] Per utilizzare questo comando, è necessario disporre delle autorizzazioni speciali *IOSYSCFG, *ALLOBJ e *JOBCTL.

[7] È necessario disporre dell'autorizzazione speciale *SECADM per specificare un valore non predefinito per il parametro IPSECRULE, CHAPAUT o SPCERTID.

Comandi di configurazione server di rete

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi di configurazione server di rete.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria QUSRSYS
CHGNWSCFG[1, 3]	Configurazione server di rete	*CHANGE	*EXECUTE
CRTNWSCFG [1, 3]	Configurazione server di rete	*USE	*READ, *ADD
DLTNWSCFG[1, 3]	Configurazione server di rete	*OBJEXIST	*EXECUTE
DSPNWSCFG[1, 3]	Configurazione server di rete	*USE	*EXECUTE
INZNWSCFG[1, 2]	Configurazione server di rete	*CHANGE	*EXECUTE
WRKNWSCFG[1]	Configurazione server di rete	*USE	*EXECUTE

[1] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *IOSYSCFG.

[2] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *SECADM.

[3] È necessario disporre dell'autorizzazione speciale *SECADM di amministratore della sicurezza per specificare o visualizzare un valore non predefinito per il parametro IPSECRULE, CHAPAUT o SPCERTID.

Comandi descrizione server di rete

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi descrizione server di rete.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria QSYS**
CHGNWSD [2]	Descrizione server di rete	*CHANGE, *OBJMGT	*EXECUTE
	Descrizione NetBIOS (NTB)	*USE	*EXECUTE
CRTNWSD [2]	Descrizione NetBIOS (NTB)	*USE	*EXECUTE
	Descrizione linea (PORTS)	*USE	*EXECUTE
DLTNWSD	Descrizione server di rete	*OBJEXIST	*EXECUTE
DSPNWSD	Descrizione server di rete	*USE	*EXECUTE
WRKNWSD[1]	Descrizione server di rete	*OBJOPR	*EXECUTE

1 Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.

2 Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *IOSYSCFG.

Comandi elenco nodi

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi elenco nodi.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDNODLE	Elenco nodi	*OBJOPR, *ADD	*EXECUTE
CRTNODL	Elenco nodi		*READ, *ADD
DLTNODL	Elenco nodi	*OBJEXIST	*EXECUTE
RMVNODLE	Elenco nodi	*OBJOPR, *READ, *DLT	*EXECUTE
WRKNODL [1]	Elenco nodi	*USE	*USE
WRKNODLE	Elenco nodi	*USE	*EXECUTE

1 Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta dall'operazione.

Comandi servizi office

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi descrizione servizi office.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Questi comandi non richiedono le autorizzazioni per l'oggetto.			
ADDACC (Q) DSPACC DSPACCAUT DSPUSRPMN	GRTACCAUT [2,3,6] (Q) GRTUSRPMN [1,2] RMVACC [1] (Q) RVKACCAUT [1]	RVKUSRPMN [1,2] WRKDOCLIB [4] WRKDOCPRTQ [5]	

[1]	È necessario disporre dell'autorizzazione speciale *ALLOBJ per assegnare o revocare l'autorizzazione codice di accesso o l'autorizzazione documento per altri utenti.
[2]	L'accesso è limitato per i documenti, le cartelle e la posta non personali.
[3]	Il codice di accesso deve essere definito sul sistema (utilizzando il comando Aggiunta codice di accesso (ADDACC)) prima di poter assegnare l'autorizzazione codice di accesso. L'utente a cui è stata concessa l'autorizzazione codice di accesso deve essere registrato sull'indirizzario di distribuzione del sistema.
[4]	È necessario disporre dell'autorizzazione speciale *SECADM.
[5]	Sono necessarie ulteriori autorizzazioni per funzioni specifiche richiamate delle operazioni selezionate. Inoltre, l'utente deve disporre di ulteriori autorizzazioni per i comandi richiamati durante una funzione specifica.
[6]	È necessaria l'autorizzazione speciale a tutti gli oggetti (*ALLOBJ) o di responsabile della della sicurezza (*SECADM) per concedere l'autorizzazione codice di accesso per altri utenti.

Comandi addestramento in linea

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi addestramento in linea.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

		Autorizzazione necessaria	
Comando	**Oggetto di riferimento**	**Per oggetto**	**Per libreria**
CVTEDU			
STREDU			

Comendi Operational Assistant

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi Operational Assistant.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

		Autorizzazione necessaria	
Comando	**Oggetto di riferimento**	**Per oggetto**	**Per libreria**
CHGBCKUP [1]	QUSRSYS/QEZBACKUPL *USRIDX	*CHANGE	*EXECUTE
CHGCLNUP[2]			
CHGPWRSCD [3]			
CHGPWRSCDE [3]			
DSPBCKSTS	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
DSPBCKUP	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
DSPBCKUPL	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*USE	*EXECUTE
DSPPWRSCD			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
EDTBCKUPL [1]	QUSRSYS/QEZBACKUPL *USRIDX	*CHANGE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*CHANGE	*EXECUTE
ENDCLNUP [4]	ENDJOB *CMD	*USE	*EXECUTE
PRTDSKINF (Q)	QUSRSYS/QAEZDISK *FILE, membro QCURRENT	*USE	*EXECUTE
	Unità ASP (se specificata)	*USE	
RTVBCKUP	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
RTVCLNUP			
RTVDSKINF (Q) [5]	Unità ASP (se specificata)	*USE	
RTVPWRSCDE	Comando DSPPWRSCD	*USE	
RUNBCKUP [1]	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*USE	*EXECUTE
	Comandi: SAVLIB, SAVCHGOBJ, SAVDLO, SAVSECDTA, SAVCFG, SAVCAL, SAV	*USE	*EXECUTE
STRCLNUP[4]	Profilo utente QPGMR	*USE	
	Coda lavori	*USE	*EXECUTE

[1] È necessario disporre dell'autorizzazione speciale *ALLOBJ o *SAVSYS.

[2] È necessario disporre delle autorizzazioni speciali *ALLOBJ, *SECADM e *JOBCTL.

[3] È necessario disporre delle autorizzazioni speciali *ALLOBJ e *SECADM.

[4] È necessario disporre dell'autorizzazione speciale *JOBCTL.

[5] È necessario disporre dell'autorizzazione speciale *ALLOBJ.

Comandi unità ottica

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi unità ottica.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria		
		Oggetto	Libreria	Volume unità ottica [1]
ADDOPTCTG (Q)	Unità ottica	*USE	*EXECUTE	
ADDOPTSVR (Q)	Server CSI	*USE	*EXECUTE	
CHGDEVOPT [4]	Unità ottica	*CHANGE, *OBJMGT	*EXECUTE	
CHGOPTA (Q)				
CHGOPTVOL	Indirizzario root (/) del volume quando si modifica la Descrizione testo [5]	*W	Non applicabili	Non applicabili
	Unità ottica	*USE	*EXECUTE	*CHANGE[3]
	Server CSI	*USE	*EXECUTE	Non applicabili

Comando	Oggetto di riferimento	Autorizzazione necessaria		
		Oggetto	**Libreria**	**Volume unità ottica [1]**
CHKOPTVOL	Unità ottica	*USE	*EXECUTE	*USE
	Indirizzario root (/) del volume	*RWX	Non applicabili	Non applicabili
CPYOPT	Unità ottica	*USE	*EXECUTE	*USE - Volume di origine
				*ALL - Volume di destinazione
	Ciascun indirizzario precedente nel percorso del file di origine	*X	Non applicabili	Non applicabili
	Ciascun indirizzario precedente nel percorso del file di destinazione	*X	Non applicabili	Non applicabili
	File di origine (*DSTMF)[5]	*R	Non applicabili	Non applicabili
	Indirizzario principale del file di destinazione	*WX	Non applicabili	Non applicabili
	Parte principale dell'indirizzario principale se si crea l'indirizzario	*WX	Non applicabili	Non applicabili
CPYOPT	File di destinazione se sostituito a causa di SLTFILE(*ALL)	*W	Non applicabili	Non applicabili
	File di destinazione se sostituito a causa di SLTFILE(*CHANGED)	*RW	Non applicabili	Non applicabili
	Ciascun indirizzario nel percorso che precede l'indirizzario di origine	*X	Non applicabili	Non applicabili
	Ciascun indirizzario nel percorso che precede l'indirizzario di destinazione	*X	Non applicabili	Non applicabili

Comando	Oggetto di riferimento	Autorizzazione necessaria		
		Oggetto	Libreria	Volume unità ottica [1]
CPYOPT	Indirizzario copiato [5]	*R	Non applicabili	Non applicabili
	Indirizzario copiato se contiene voci	*RX	Non applicabili	Non applicabili
	Parte principale dell'indirizzario di destinazione	*WX	Non applicabili	Non applicabili
	Indirizzario di destinazione se sostituito a causa di SLTFILE(*ALL)	*W	Non applicabili	Non applicabili
	Indirizzario di destinazione se sostituito a causa di SLTFILE(*CHANGED)	*RW	Non applicabili	Non applicabili
	Indirizzario di destinazione se è necessario creare le voci	*WX	Non applicabili	Non applicabili
CPYOPT	File di origine	*R	Non applicabili	Non applicabili
	File di destinazione se sostituito a causa di SLTFILE(*ALL)	*W	Non applicabili	Non applicabili
	File di destinazione se sostituito a causa di SLTFILE(*CHANGED)	*RW	Non applicabili	Non applicabili
CRTDEVOPT [4]	Unità ottica		*EXECUTE	
CVTOPTBKU	Unità ottica	*USE	*EXECUTE	*ALL
DSPOPT	Prefisso percorso quando DATA (*SAVRST) [5]	*X	Non applicabili	Non applicabili
	Prefisso file quando (*SAVRST) [2]	*R	Non applicabili	Non applicabili
	Unità ottica	*EXECUTE	*USE	
	Server CSI	*USE	*EXECUTE	
DSPOPTLCK				
DSPOPTSVR	Server CSI	*USE	*EXECUTE	
DUPOPT	Unità ottica	*USE	*EXECUTE	*USE - Volume di origine
				*ALL - Volume di destinazione
INZOPT	Indirizzario root (/) del volume	*RWX	Non applicabili	Non applicabili
	Unità ottica	*USE	*EXECUTE	*ALL
LODOPTFMW	File di flusso	*R	Non applicabili	Non applicabili
	Prefisso percorso	Fare riferimento alle regole generali.		
RCLOPT (Q)	Unità ottica	*USE	*EXECUTE	

Comando	Oggetto di riferimento	Autorizzazione necessaria		
		Oggetto	Libreria	Volume unità ottica [1]
RMVOPTCTG (Q)	Unità ottica	*USE	*EXECUTE	
RMVOPTSVR (Q)	Server CSI	*USE	*EXECUTE	
WRKHLDOPTF[2]	Unità ottica	*USE	*EXECUTE	*USE
	Server CSI	*USE	*EXECUTE	
WRKOPTDIR[2]	Unità ottica	*USE	*EXECUTE	*USE
	Server CSI	*USE	*EXECUTE	
WRKOPTF[2]	Unità ottica	*USE	*EXECUTE	*USE
	Server CSI	*USE	*EXECUTE	
WRKOPTVOL[2]	Unità ottica	*USE	*EXECUTE	

[1] I volumi dell'unità ottica non sono oggetti di sistema effettivi. Il collegamento tra il volume dell'unità ottica e l'elenco di autorizzazioni utilizzato per proteggere il volume viene gestito dalla funzione di supporto dell'unità ottica.

[2] È possibile richiamare sette opzioni dalle funzioni dell'unità ottica che non sono comandi. Tali opzioni e le relative autorizzazioni richieste per il volume unità ottica sono riportate di seguito.

- Cancellazione file: *CHANGE
- Ridenominazione file: *CHANGE
- Cancellazione indirizzario: *CHANGE
- Creazione indirizzario: *CHANGE
- Ridenominazione volume: *ALL
- Rilascio file ottico congelato: *CHANGE
- Salvataggio file ottico congelato: *USE - Volume di origine, *Change - Volume di destinazione

[3] L'autorizzazione gestione elenco di autorizzazioni per l'elenco di autorizzazioni che protegge attualmente il volume unità ottica è necessaria per modificare l'elenco di autorizzazioni utilizzato per proteggere il volume.

[4] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *IOSYSCFG.

[5] Tale verifica dell'autorizzazione viene effettuata solo quando il formato supporto magnetico dell'unità ottica corrisponde all'UDF (Universal Disk Format).

Comandi coda di emissione

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi coda di emissione.

Comando	Oggetto di riferimento	Parametri coda di emissione		Autorizzaz. speciale	Autorizzazione necessaria	
		AUTCHK	OPRCTL		Per oggetto	Per libreria
CHGOUTQ [1]	Coda messaggi				*READ	*EXECUTE
	Coda di emissione	*DTAAUT			*OBJMGT, *READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietario [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Coda messaggi				*OBJOPR *ADD	*EXECUTE
	Oggetto personalizzaz. stazione di lavoro				*USE	*EXECUTE
	Programma trasformazione dati utente				*OBJOPR *EXECUTE	*EXECUTE
	Programma unità di controllo dell'utente				*OBJOPR *EXECUTE	*EXECUTE
CLROUTQ [1]	Coda di emissione	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietario [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CRTOUTQ	Coda messaggi				*READ	*EXECUTE
	Coda di emissione					*READ, *ADD
	Coda messaggi				*OBJOPR *ADD	*EXECUTE
	Oggetto personalizzaz. stazione di lavoro				*USE	*EXECUTE
DLTOUTQ	Coda di emissione				*OBJEXIST	*EXECUTE
HLDOUTQ [1]	Coda di emissione	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietario [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
PRTQAUT [4]						
RLSOUTQ [1]	Coda di emissione	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietario [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKOUTQ [1,3]	Coda di emissione				*READ	*EXECUTE
			*YES	*JOBCTL		*EXECUTE

Comando	Oggetto di riferimento	Parametri coda di emissione		Autorizzaz. speciale	Autorizzazione necessaria	
		AUTCHK	OPRCTL		Per oggetto	Per libreria
WRKOUTQD [1,3]	Coda di emissione				*READ	*EXECUTE
			*YES	*JOBCTL		*EXECUTE

[1] Se si dispone dell'autorizzazione speciale *SPLCTL, non è necessaria l'autorizzazione per la coda di emissione. Tuttavia, è necessario disporre dell'autorizzazione *EXECUTE sulla libreria per la coda di emissione.

[2] È necessario essere il proprietario della coda di emissione.

[3] Se si desidera gestire tutte le code di emissione, l'elenco visualizzerà tutte le code di emissione nelle librerie per cui si dispone dell'autorizzazione *EXECUTE.

[4] È necessario disporre dell'autorizzazione speciale *ALLOBJ per utilizzare questo comando.

Comandi pacchetto

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi pacchetto.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
CRTSQLPKG	Programma	*OBJOPR, *READ	*EXECUTE
	Pacchetto SQL: REPLACE(*NO)		*OBJOPR, *READ, *ADD, *EXECUTE
	Pacchetto SQL: REPLACE(*YES)	*OBJOPR, *OBJMGT, *OBJEXIST, *READ	*OBJOPR, *READ, *ADD, *EXECUTE
DLTSQLPKG	Pacchetto	*OBJEXIST	*EXECUTE
PRTSQLINF	Pacchetto	*OBJOPR, *READ	*EXECUTE
	Programma	*OBJOPR, *READ	*EXECUTE
	Programma di servizio	*OBJOPR, *READ	*EXECUTE
STRSQL			

Comandi prestazioni

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi prestazioni.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri utenti.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ADDDWDFN (Q) [7]			
ADDJWDFN (Q) [7]			
ADDPEXDFN (Q) [5]	Libreria PGM		*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ADDPEXFTR (Q)[5]	Libreria PGMTRG		*EXECUTE
	Libreria PGMFTR		*EXECUTE
	Percorso JVAFTR	*X per l'indirizzario	
	Percorso PATHFTR	*X per l'indirizzario	
ANZBESTMDL (Q)[4]	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Librerie dell'applicazione che contengono i file di database da analizzare		*EXECUTE
	Descrizione lavoro	*USE	*EXECUTE
ANZCMDPFR (Q)	File comando	*USE	*EXECUTE
	File di emissione	*USE	*EXECUTE, *ADD
ANZDBF (Q)[4]	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Descrizione lavoro	*USE	*EXECUTE
ANZDBFKEY (Q)	QPFR/QPTANZKC *PGM	*USE	*EXECUTE
	Librerie dell'applicazione che contengono i programmi da analizzare		*EXECUTE
	Descrizione lavoro	*USE	*EXECUTE
ANZPGM (Q)	QPFR/QPTANZPC *PGM	*USE	*EXECUTE
	Dati delle prestazioni [2]		*ADD, *READ
ANZPFRDTA (Q)[4]	QPFR/QACVPP *PGM	*USE	*EXECUTE
	Dati delle prestazioni [2]		*ADD, *READ
ANZPFRDT2 (Q)[4]	QPFR/QAVCPP *PGM	*USE	*EXECUTE
	QAPTAPGP *FILE	*CHANGE	*EXECUTE
	Comando DLTFCNARA (Q)	*USE	*EXECUTE
	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
CFGPFRCOL (Q)	Libreria raccolte		*EXECUTE
CHGFCNARA (Q)	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE	*CHANGE	*EXECUTE
CHGGPHFMT (Q)	QPFR/QPGCRTFM *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE	*CHANGE	*EXECUTE
	QAPGGPHF *FILE	*USE	*EXECUTE
CHGGPHPKG (Q)	QPFR/QPGCRTPK *PGM	*USE	*EXECUTE
	QAPMDMPT *FILE	*CHANGE	*EXECUTE
CHGJOBTYP (Q)	QPFR/QPTCHGJT *PGM	*USE	*EXECUTE
CHGMGTCOL	MGTCOL	*OBJMGT	
	Libreria utente		*EXECUTE
CHGPEXDFN (Q)[5]	Libreria PGM		*EXECUTE
CHKPFRCOL (Q)			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CPYFCNARA (Q)[4]	QPFR/QPTAGRPR *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE nella libreria di ″provenienza″	*USE	*EXECUTE
	Libreria di ″destinazione″ (se QAPGGPHF *FILE non è presente)		*EXECUTE, *ADD
	QAPGGPHF *FILE nella libreria di ″destinazione″ (se si sta aggiungendo un nuovo formato grafico o se ne sta sostituendo uno esistente)	*CHANGE	*EXECUTE
CPYGPHFMT (Q)[4]	QPFR/QPGCPYGP *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE nella libreria di ″provenienza″	*USE	*EXECUTE
	Libreria di ″destinazione″ (se QAPGPKGF *FILE non è presente)		*EXECUTE, *ADD
	QAPGPKGF *FILE nella libreria di ″destinazione″ (se si sta aggiungendo un nuovo pacchetto grafico o se ne sta sostituendo uno esistente)	*CHANGE	*EXECUTE
	QAPGGPHF *FILE nella libreria di ″destinazione″ (se si sta aggiungendo un nuovo pacchetto grafico o se ne sta sostituendo uno esistente)	*USE	*EXECUTE
CPYGPHPKG (Q)	QPFR/QPGCPYGP *PGM	*USE	*EXECUTE
	Libreria di provenienza		*EXECUTE
	Libreria di destinazione		*EXECUTE, *ADD
	Descrizione lavoro	*USE	*EXECUTE
CPYPFRCOL (Q)	Libreria di provenienza		*EXECUTE
	Libreria di destinazione		*EXECUTE, *ADD
CPYPFRDTA (Q)	QPFR/QITCPYCP *PGM	*USE	*EXECUTE
	Dati delle prestazioni (tutti i file QAPM*)	*USE	*EXECUTE
	Libreria modello		*EXECUTE, *ADD
	Descrizione lavoro	*USE	*EXECUTE
	QPFR/QCYCBMCP *PGM	*USE	*EXECUTE
	QPFR/QCYCBMDL *PGM	*USE	*EXECUTE
	QPFR/QCYOPDBS *PGM	*USE	*EXECUTE
	QPFR/QCYCLIDS *PGM	*USE	*EXECUTE
CRTBESTMDL (Q)	QPFR/QCYCAPT *PGM	*USE	*EXECUTE
	Libreria in cui viene creata l'Area funzionale		*EXECUTE, *ADD
	QAPTAPGP *FILE nella libreria di destinazione (se si sta aggiungendo un nuova area funzionale)	*CHANGE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
CRTFCNARA (Q)	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
	Libreria in cui viene creato il Formato grafico		*EXECUTE, *ADD
	QAPGGPHF *FILE nella libreria di destinazione (se si sta aggiungendo un nuovo formato grafico)	*CHANGE	*EXECUTE
CRTGPHFMT (Q)	QPFR/QPGCRTFM *PGM	*USE	*EXECUTE
	Libreria in cui viene creato il Pacchetto grafico		*EXECUTE, *ADD
	QAPGGPHF *FILE	*CHANGE	*EXECUTE
	QAPGPKGF *FILE nella libreria di destinazione (se si sta aggiungendo un nuovo pacchetto grafico)	*USE	*EXECUTE
CRTGPHPKG (Q)	QPFR/QPGCRTPK *PGM	*USE	*EXECUTE
	Libreria in cui vengono creati i dati cronologici		*ADD, *READ
	Descrizione lavoro	*USE	*EXECUTE
CRTHSTDTA (Q)	QPFR/QPGCRTHS *PGM	*USE	*EXECUTE
	Libreria di destinazione		*ADD, *READ
CRTPEXDTA (Q)[5]	Libreria *MGTCOL		*EXECUTE
	Libreria dati [1]		*READ, *ADD [2]
CRTPFRDTA (Q)	Libreria di provenienza		*EXECUTE
	Libreria di destinazione		*ADD, *READ
	Libreria di provenienza		*USE
CRTPFRSUM (Q)	Libreria utente		*ADD, *READ
CVTPFRCOL (Q)	Libreria di provenienza		*USE
	Libreria di destinazione		*USE, *ADD
CVTPFRDTA (Q)	Descrizione lavoro	*USE	*EXECUTE
CVTPFRTHD (Q)	Dati delle prestazioni [2]		*ADD, *READ
	Libreria modello		*EXECUTE, *ADD
	QPFR/QCYDBMDL *PGM	*USE	*EXECUTE
	QPFR/QCYCVTBD *CMD	*USE	*EXECUTE
DLTBESTMDL (Q)[4]	QPFR/QCYCBTOD *PGM	*USE	*EXECUTE
	QAPTAPGP *FILE nella libreria area funzionale	*CHANGE	*EXECUTE
DLTFCNARA (Q)[4]	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE nella libreria formato grafico	*CHANGE	*EXECUTE
DLTGPHFMT (Q)[4]	QPFR/QPGDLTGP *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE nella libreria pacchetto grafico	*CHANGE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
DLTGPHPKG (Q)[4]	QPFR/QPGDLTGP *PGM	*USE	*EXECUTE
	QAPGHSTD *FILE nella libreria dati cronologici	*CHANGE	*EXECUTE
	QAPGHSTI *FILE nella libreria dati cronologici	*CHANGE	*EXECUTE
	QAPGSUMD *FILE nella libreria dati cronologici	*CHANGE	*EXECUTE
DLTHSTDTA (Q)[4]	QPFR/QPGDLTHS *PGM	*USE	*EXECUTE
DLTPEXDTA (Q)[5]	Libreria dati [1]		*EXECUTE, *DELETE [2]
DLTPFRCOL (Q)	Libreria		*EXECUTE
DLTPFRDTA (Q)[4]	QPFR/QPTDLTCP *PGM	*USE	*EXECUTE
DMPMEMINF	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
DMPTRC (Q)[5]	Libreria in cui verranno memorizzati i dati di traccia		*EXECUTE, *ADD
	File di emissione (QAPTPAGD)	*CHANGE	*EXECUTE, *ADD
DSPHSTGPH (Q)[4]	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Libreria dati cronologici		*EXECUTE
DSPPFRDTA (Q) [4]	QPFR/QAVCPP *PGM	*USE	*EXECUTE
	Libreria pacchetto o formato		*EXECUTE
	Dati delle prestazioni [2]		*EXECUTE
	Libreria file di emissione		*EXECUTE, *ADD
	Coda di emissione	*USE	*EXECUTE
	Descrizione lavoro	*USE	*EXECUTE
DSPPFRGPH (Q)[4]	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Libreria file di emissione		*EXECUTE
	Descrizione lavoro	*USE	*EXECUTE
ENDDW (Q)[7]			
ENDJOBTRC (Q)[4]	QPFR/QPTTRCJ0 *PGM	*USE	*EXECUTE
ENDJW (Q)[7]			
ENDPEX (Q)[5]	Libreria dati [1]		*READ, *ADD [2]
ENDPFRCOL (Q)			
PRTACTRPT (Q)[4]	QPFR/QITPRTAC *PGM	*USE	*EXECUTE
	Dati delle prestazioni [2]	*USE	*ADD, *READ
	Descrizione lavoro	*USE	*EXECUTE
PRTCPTRPT (Q)[4]	QPFR/QPTCPTRP *PGM	*USE	*EXECUTE
	Dati delle prestazioni [2]		*ADD, *READ
	Descrizione lavoro	*USE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
PRTJOBRPT (Q)[4]	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	Dati delle prestazioni [2]		*ADD, *READ
	Descrizione lavoro	*USE	*EXECUTE
PRTJOBTRC (Q)[4]	QPFR/QPTTRCRP *PGM	*USE	*EXECUTE
	Libreria (QAPTTRCJ) file traccia lavoro		*EXECUTE
	Descrizione lavoro	*USE	*EXECUTE
PRTLCKRPT (Q)[4]	QPFR/QPTLCKQ *PGM	*USE	*EXECUTE
PRTPEXRPT[5]	Libreria dati[1]		*EXECUTE[2]
	File di emissione	*USE	*EXECUTE, *ADD
	QPFR/QVPEPRTC *PGM	*USE	*EXECUTE
	QPFR/QVPESVGN *SRVPGM	*USE	*EXECUTE
	QPFR/QYPESVGN *SRVPGM	*USE	*EXECUTE
PRTPOLRPT (Q)[4]	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	Dati delle prestazioni [2]		*ADD, *READ
	Descrizione lavoro	*USE	*EXECUTE
PRTRSCRPT (Q)[4]	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	Dati delle prestazioni [2]		*ADD, *READ
	Descrizione lavoro	*USE	*EXECUTE
PRTSYSRPT (Q)[4]	QPFR/QPTTNSRP *PGM	*USE	*EXECUTE
	QAPMDMPT *FILE		*EXECUTE
	Descrizione lavoro	*USE	*EXECUTE
PRTTNSRPT (Q)[4]	QPFR/QPTTNSRP *PGM	*USE	*EXECUTE
	Libreria (QTRJOBT) file di traccia		*EXECUTE
	Descrizione lavoro	*USE	*EXECUTE
PRTTRCRPT (Q)[4]	QPFR/QPTTRCCP *PGM	*USE	*EXECUTE
RMVDWDFN (Q) [7]			
RMVJWDFN (Q) [7]			
RMVPEXDFN (Q)[5]			
RMVPEXFTR (Q)[5]			
RSTPFRCOL (Q)	Libreria associata alla raccolta di ripristino	*EXECUTE,, *ADD [6]	
	Salvataggio file	*USE	*EXECUTE
SAVPFRCOL (Q)	Libreria contenente la raccolta da salvare	*EXECUTE [6]	
	File di salvataggio, se vuoto	*USE, *ADD	*EXECUTE, *ADD
	File di salvataggio, se contiene i record	*OBJMGT, *USE, *ADD	*EXECUTE
STRBEST (Q)[4]	QPFR/QCYBMAIN *PGM	*USE	*EXECUTE
STRDBMON[3, 4]	File di emissione	*OBJOPR, *ADD	*EXECUTE
STRDW (Q)[7]	Libreria utente		*EXECUTE
STRJOBTRC (Q)	QPFR/QPTTRCJ1 *PGM	*USE	*EXECUTE
STRJW (Q) [7]	Libreria utente		*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
STRPEX (Q)[5]			
STRPFRCOL (Q)			
STRPFRG (Q)[4]	QPFR/QPGSTART *PGM	*USE	*EXECUTE
STRPFRT (Q)[4]	QPFR/QMNMAIN0 *PGM	*USE	*EXECUTE
	QAPTAPGP *FILE nella libreria aree funzionali	*CHANGE	*EXECUTE
	Comando CHGFCNARA (Q)	*USE	*EXECUTE
	Comando CPYFCNARA (Q)	*USE	*EXECUTE
	Comando CRTFCNARA (Q)	*USE	*EXECUTE
	Comando DLTFCNARA (Q)	*USE	*EXECUTE
	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QPFR/QPTAGRPR *PGM	*USE	*EXECUTE
WRKFCNARA (Q)[4]	QPFR/QPTAGRPC *PGM	*USE	*EXECUTE
	File di emissione (QAITMON)	*CHANGE, *ALTER	*EXECUTE, *ADD
WRKPEXDFN (Q)[5]			
WRKPEXFTR (Q)[5]			
WRKSYSACT (Q)[3, 4]	QPFR/QITMONCP *PGM	*USE	*EXECUTE
Questi comandi non richiedono autorizzazioni oggetto: • ENDDBMON[3] • ENDPFRTRC (Q) • STRPFRTRC (Q)			

[1] Se viene specificata la libreria predefinita (QPEXDATA), l'autorizzazione per tale libreria non viene controllata.

[2] È necessario disporre dell'autorizzazione per la libreria che contiene la serie di file di database. L'autorizzazione per la serie di file di database individuali non viene controllata.

[3] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *JOBCTL.

[4] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *SERVICE.

[5] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *SERVICE o essere autorizzati ad utilizzare la funzione Traccia di servizio di i5/OS tramite gestione applicazione in System i Navigator. È inoltre possibile utilizzare il comando CHGFCNUSG (Modifica utilizzo funzione), con un ID funzione di QIBM_SERVICE_TRACE, per modificare l'elenco di utenti a cui è consentita l'esecuzione di operazioni di traccia.

[6] Se si dispone dell'autorizzazione speciale *SAVSYS, non è necessaria l'autorizzazione specificata.

[7] Per usare questo comando, è necessario disporre dell'autorizzazione speciale al servizio (*SERVICE) o essere autorizzati alla funzione Watcher dischi del sistema operativo tramite il supporto di gestione applicazione System i Navigator. Il comando CHGFCNUSG (Modifica utilizzo funzione) con un ID funzione QIBM_SERVICE_DISK_WATCHER, può essere anche utilizzato per modificare l'elenco di utenti a cui è consentito l'utilizzo dello strumento watcher dischi.

Comandi gruppo descrittori di stampa

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi gruppo descrittori di stampa.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
CHGPDGPRF	Profilo utente	*OBJMGT	
CRTPDG	Gruppo descrittori di stampa		*READ, *ADD
DLTPDG	Gruppo descrittori di stampa	*OBJEXIST	*EXECUTE
DSPPDGPRF	Profilo utente	*OBJMGT	
RTVPDGPRF	Profilo utente	*READ	

Comandi di configurazione Print Services Facility

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi Print service facility.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
CHGPSFCFG [1, 2]			
CRTGPSFCFG [1, 2]			*READ, *ADD
DLTPSFCFG [1, 2]	Configurazione PSF	*OBJEXIST	*EXECUTE
DSPPSFCFG [1]	Configurazione PSF	*USE	*EXECUTE
WRKPSFCFG [1]	Configurazione PSF	*READ	*EXECUTE

1 La funzione PSF/400 è necessaria per utilizzare questo comando.

2 È necessario disporre dell'autorizzazione speciale *IOSYSCFG per utilizzare questo comando.

Comandi problema

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi problema.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ADDPRBACNE (Q)	Filtro	*USE, *ADD	*EXECUTE
ADDPRBSLTE (Q)	Filtro	*USE, *ADD	*EXECUTE
ANZPRB (Q)	Comando SNDSRVRQS	*USE	*EXECUTE
CHGPRB (Q)			*EXECUTE
CHGPRBACNE (Q)	Filtro	*USE, *UPD	*EXECUTE
CHGPRBSLTE (Q)	Filtro	*USE, *UPD	*EXECUTE
DLTPRB (Q) [3]	Comando: DLTAPARDTA	*USE	*EXECUTE
DSPPRB	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
PTRINTDTA (Q)			
QRYPRBSTS (Q)			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
VFYCMN (Q)	Descrizione linea [1]	*USE	*EXECUTE
	Descrizione unità di controllo [1]	*USE	*EXECUTE
	ID rete [1]	*USE	*EXECUTE
VFYOPT (Q)	Descrizione unità	*USE	*EXECUTE
VFYTAP[4] (Q)	Descrizione unità	*USE, *OBJMGT	*EXECUTE
VFYPRT (Q)	Descrizione unità	*USE	*EXECUTE
WRKPRB (Q) [2]	Linea, unità di controllo, NWID (ID di rete) e unità basata sull'azione di analisi dei problemi	*USE	*EXECUTE

1 È necessario disporre dell'autorizzazione *USE per l'oggetto comunicazioni che si sta verificando.

2 È necessario disporre dell'autorizzazione *USE per il comando SNDSRVRQS per poter riportare un problema.

3 È necessario disporre dell'autorizzazione per DLTAPARDTA se si desidera che i dati APAR associati al problema vengano cancellati. Consultare DLTAPARDTA nella tabella Autorizzazioni comando necessarie per determinare quali ulteriori autorizzazioni sono necessarie.

4 È necessario disporre dell'autorizzazione speciale *IOSYSCFG quando la descrizione unità è assegnata da un'unità libreria supporti magnetici.

Comandi programma

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi programma.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
Le autorizzazioni oggetto richieste per i comandi CRT*xxx*PGM sono elencate nella tabella Linguaggi nei "Comandi linguaggio" a pagina 451.			
ADDBKP [1]	Programma di gestione punti di interruzione	*USE	*EXECUTE
ADDPGM [1,2]	Programma	*CHANGE	*EXECUTE
ADDTRC [1]	Programma di gestione traccia	*USE	*EXECUTE
CALL	Programma	*OBJOPR, *EXECUTE	*EXECUTE
	Programma di servizio [4]	*EXECUTE	*EXECUTE
CHGDBG	Operazione di debug	*USE, *ADD, *DLT	*EXECUTE
CHGHLLPTR [1]			
CHGPGM	Programma	*OBJMGT, *USE	*USE
	Programma, se è specificata l'opzione per la nuova creazione, il livello di ottimizzazione è cambiato o la raccolta dati delle prestazioni è cambiata	*OBJMGT, *USE	*USE, *ADD, *DLT
	Programma, se il parametro USRPRF o USEADPAUT è stato modificato	Proprietario [7]	*USE, *ADD, *DLT
CHGPGMVAR [1]			
CHGPTR [1]			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGSRVPGM	Programma di servizio	*OBJMGT, *USE	*USE
	Programma di servizio, se è specificata l'opzione per la nuova creazione, il livello di ottimizzazione è cambiato o la raccolta dati delle prestazioni è cambiata	*OBJMGT, *USE	*USE, *ADD, *DLT
	Programma di servizio, se il parametro USRPRF o USEADPAUT è stato modificato.	Proprietario [7], *USE, *OBJMGT	*USE, *ADD, *DLT
CLRTRCDTA [1]			
CRTPGM	Programma, Replace(*NO)	Fare riferimento alle regole generali.	*READ, *ADD
	Programma, Replace(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Programma di servizio specificato nel parametro BNDSRVPGM.	*USE	*EXECUTE
	Modulo	*USE	*EXECUTE
	Indirizzario di collegamento	*USE	*EXECUTE
CRTSRVPGM	Programma di servizio, Replace(*NO)	Fare riferimento alle regole generali.	*READ, *ADD
	Programma di servizio, Replace(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Modulo	*USE	*EXECUTE
	Programma di servizio specificato nel parametro BNDSRVPGM	*USE	*EXECUTE
	File di origine di esportazione	*OBJOPR *READ	*EXECUTE
	Indirizzario di collegamento	*USE	*EXECUTE
CVTCLSRC	Da file	*USE	*EXECUTE
	A file	*OBJOPR, *OBJMGT, *USE, *ADD, *DLT	*READ, *ADD
DLTDFUPGM	Programma	*OBJEXIST	*EXECUTE
	File di visualizzazione	*OBJEXIST	*EXECUTE
DLTPGM	Programma	*OBJEXIST	*EXECUTE
DLTSRVPGM	Programma di servizio	*OBJEXIST	*EXECUTE
DMPCLPGM	Programma CL	*USE	Nessuno [3]
DSPBKP [1]			
DSPDBG [1]			
DSPDBGWCH			
DSPMODSRC[2, 4]	File di origine	*USE	*USE
	Nessun file di inclusione	*USE	*USE
	Programma	*CHANGE	*EXECUTE
DSPPGM	Programma	*READ	*EXECUTE
	Programma, se DETAIL(*MODULE) è specificato	*USE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
DSPPGMREF	Programma	*OBJOPR	*EXECUTE
	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
DSPPGMVAR [1]			
DSPSRVPGM	Programma di servizio	*READ	*EXECUTE
	Programma di servizio, se DETAIL(*MODULE) è specificato	*USE	*EXECUTE
DSPTRC [1]			
DSPTRCDTA [1]			
ENDCBLDBG (programma su licenza COBOL/400 o ambiente S/38)	Programma	*CHANGE	*EXECUTE
ENDDBG [1]	Programma di debug di origine	*USE	*USE
ENDRQS [1]			*EXECUTE
ENTCBLDBG (ambiente S/38)	Programma	*CHANGE	*EXECUTE
EXTPGMINF	File di origine e file di database	*OBJOPR	*EXECUTE
	Informazioni sul programma		*READ, *ADD
PRTCMDUSG	Programma	*USE	*EXECUTE
RMVBKP [1]			
RMVPGM [1]			
RMVTRC [1]			
RSMBKP [1]			
RTVCLSRC	Programma	*OBJMGT, *USE	*EXECUTE
	File di origine database	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
SETATNPGM	Programma di gestione tasto di attenzione	*EXECUTE	*EXECUTE
SETPGMINF	File di database	*OBJOPR	*EXECUTE
	File di origine	*USE	*EXECUTE
	Programma root	*CHANGE	*READ, *ADD
	Sottoprogramma	*USE	*EXECUTE
STRCBLDBG	Programma	*CHANGE	*EXECUTE
STRDBG	Programma [2]	*CHANGE	*EXECUTE
	File di origine [4]	*USE	*EXECUTE
	Qualsiasi file di inclusione [4]	*USE	*EXECUTE
	Programma di debug di origine	*USE	*EXECUTE
	Programma messaggio non controllato	*USE	*EXECUTE
TFRCTL [4]	Programma	*USE o un'autorizzazione dati diversa da *EXECUTE	*EXECUTE
	Alcune funzioni del linguaggio quando si utilizzano linguaggi di alto livello	*READ	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
UPDPGM	Programma	*OBJMGT, *OBJEXIST, *USE	*USE, *ADD
	Programma di servizio specificato nel parametro BNDSRVPGM.	*USE	*EXECUTE
	Modulo	*USE	*EXECUTE
	Indirizzario di collegamento	*USE	*EXECUTE
UPDSRVPGM	Programma di servizio	*OBJMGT, *OBJEXIST, *USE	*USE, *ADD
	Programma di servizio specificato nel parametro BNDSRVPGM	*USE	*EXECUTE
	Modulo	*USE	*EXECUTE
	Indirizzario di collegamento	*USE	*EXECUTE
	File di origine di esportazione	*OBJOPR *READ	*EXECUTE
WRKPGM [6]	Programma	Qualsiasi autorizzazione	*USE
WRKSRVPGM [6]	Programma di servizio	Qualsiasi autorizzazione	*USE

[1] Quando un programma è nella fase di debug, non è necessaria nessuna ulteriore autorizzazione per i comandi di debug.

[2] Se si dispone dell'autorizzazione speciale *SERVICE, è necessario disporre solo dell'autorizzazione *USE per il programma.

[3] È necessario immettere il comando DMPCLPGM dall'interno di un programma CL già in esecuzione. Poiché l'autorizzazione per la libreria contenente il programma viene controllata al momento del richiamo del programma, l'autorizzazione per la libreria non viene controllata nuovamente all'esecuzione del comando DMPCLPGM.

[4] Valido solo per i programmi ILE.

[5] Consultare Authorization, privileges and object ownership per ulteriori informazioni sui requisiti della sicurezza per le istruzioni SQL.

[6] Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

[7] È necessario essere il proprietario del programma o disporre delle autorizzazioni speciali *ALLOBJ e *SECADM.

Comandi QSH shell interpreter

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi QSH shell interpreter.

I comandi elencati in questa tabella non richiedono le autorizzazioni per gli oggetti.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
STRQSH [1, 2]			
QSH [1, 2]			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria

[1] QSH è un nome alternativo per il comando CL STRQSH.

[2] L'utente necessita dell'autorizzazione *RX a tutti gli script e dell'autorizzazione *X a tutti gli indirizzari nel percorso verso lo script.

Comandi query

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi query.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ANZQRY	Definizione query	*USE	*EXECUTE
CHGQRYA[4]			
CRTQMFORM	Modulo del query management: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Modulo del query management: REPLACE(*YES)	*ALL	*READ, *ADD, *EXECUTE
	File di origine	*USE	*EXECUTE
CRTQMQRY	Modulo del query management: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Modulo del query management: REPLACE(*YES)	*ALL	*READ, *ADD, *EXECUTE
	File di origine	*USE	*EXECUTE
	Comando OVRDBF	*USE	*EXECUTE
DLTQMFORM	Modulo del query management	OBJEXIST	*EXECUTE
DLTQMQRY	Query del query management	*OBJEXIST	*EXECUTE
DLTQRY	Definizione query	*OBJEXIST	*EXECUTE
RTVQMFORM	Modulo del query manager	*OBJEXIST	*EXECUTE
	File di origine di destinazione	*ALL	*READ, *ADD, *EXECUTE
	Comandi ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, OVRDBF, RMVM	*USE	*EXECUTE
RTVQMQRY	Query del query manager	*USE	*EXECUTE
	File di origine di destinazione	*ALL	*READ, *ADD
	Comandi ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, OVRDBF, RMVM	*USE	*EXECUTE
RUNQRY	Definizione query	*USE	*USE
	File di immissione	*USE	*EXECUTE
	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
STRQMQRY [1]	Query del query management	*USE	*EXECUTE
	Modulo del query management, se specificato	*USE	*EXECUTE
	Definizione query, se specificata	*USE	*EXECUTE
	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	Comandi ADDPFM, CHGOBJD, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, GRTOBJAUT OVRDBF, OVRPRTF RMVM (se OUTPUT(*OUTFILE) è specificato)	*USE	*EXECUTE
STRQMPRC [1]	File di origine contenente la procedura del query manager	*USE	*EXECUTE
	File di origine contenente il file di origine del comando, se specificato	*USE	*EXECUTE
	Comando OVRPRTF, se le istruzioni risultano in un prospetto stampato o in un oggetto query.	*USE	*EXECUTE
STRQRY			*EXECUTE
WRKQMFORM [3]	Modulo del query management	Qualsiasi autorizzazione	*USE
WRKQMQRY [3]	Query del query management	Qualsiasi autorizzazione	*USE
WRKQRY [3]			

1 Per eseguire STRQM, è necessario disporre dell'autorizzazione richiesta dalle istruzioni nella query. Ad esempio, per inserire una riga in una tabella, è necessario disporre dell'autorizzazione *OBJOPR, *ADD e *EXECUTE per la tabella.

2 È necessario essere proprietario o disporre di un'autorizzazione per l'oggetto.

3 Per utilizzare singole operazioni, è necessario disporre dell'autorizzazione richiesta da tale operazione.

4 Per utilizzare un singolo comando, è necessario disporre dell'autorizzazione speciale *JOBCTL.

Comandi domanda e risposta

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi domanda e risposta.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ANSQST (Q)	File di database QAQA*xx*BQPY [1]	*READ	*READ
ASKQST	File di database QAQA*xx*BBPY [1] o QAQA*xx*BQPY [1]	*READ	*READ
CHGQSTDB (Q)	File di database QAQA*xx*BQPY [1]	*READ	*READ

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTQSTDB [2] (Q)	File di database		*READ, *ADD, *EXECUTE
CRTQSTLOD (Q)	File di database QAQA*xx*BQPY [1]	*READ	*READ
DLTQST (Q)	File di database QAQA*xx*BQPY [1]	*READ	*READ
DLTQSTDB (Q)	File di database QAQA*xx*BQPY [1]	*READ	*READ
EDTQST (Q)	File di database QAQA*xx*BQPY [1]	*READ	*READ
LODQSTDB [2] (Q)	File di database QAQA*xx*BQPY [1,3]	*READ	*READ, *ADD, *EXECUTE
STRQST [4]	File di database QAQA*xx*BBPY [1] o QAQA*xx*BQPY [1]	*READ	*READ
WRKQST	File di database QAQA*xx*BBPY [1] QAQA*xx*BQPY [1]	*READ	*USE
WRKCNTINF			*EXECUTE

[1] La parte "xx" del nome file è l'indice del database Domande e risposte utilizzato dal comando. L'indice è composto da un numero a due cifre, compreso tra 00 e 99. Per ottenere l'indice di un database Domande e risposte particolare, utilizzare il comando WRKCNTINF.

[2] Il profilo utente che esegue il comando diventa il proprietario dei file appena creati, a meno che il parametro OWNER del profilo dell'utente non sia *GRPPRF. L'autorizzazione pubblica per nuovi file, ad eccezione di QAQA*xx*BBPY, è impostata su *EXCLUDE. L'autorizzazione pubblica per QAQA*xx*BBPY è impostata su *READ.

[3] L'autorizzazione al file è richiesta solo se si carica un database Domande e risposte esistente in precedenza.

[4] Il comando visualizza il menu Domande e risposte. Per utilizzare le singole opzioni, è necessario disporre dell'autorizzazione richiesta da tali opzioni.

Comandi programma di lettura

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi programma di lettura.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
STRDBRDR	Coda messaggi	*OBJOPR, *ADD	*EXECUTE
	File di database	*OBJOPR, *USE	*EXECUTE
	Coda lavori	*READ	*EXECUTE
STRDKTRDR	Coda messaggi	*OBJOPR, *ADD	*EXECUTE
	Coda lavori	*READ	*EXECUTE
	Descrizione unità	*OBJOPR, *READ	*EXECUTE
Questi comandi non richiedono l'autorizzazione agli oggetti:			
ENDRDR [1]	HLDRDR [1]	RLSRDR [1]	

[1] L'utente deve aver avviato il programma di lettura oppure deve disporre dell'autorizzazione speciale per tutti gli oggetti (*ALLOBJ) o per il controllo del lavoro (*JOBCTL).

Comandi funzione registrazione

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi funzione registrazione.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ADDEXITPGM (Q)			
RMVEXITPGM (Q)			
WRKREGINF			

Comandi database relazionale

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi database relazionale.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ADDRDBDIRE	File di emissione, se specificato	*EXECUTE	*EXECUTE
CHGRDBDIRE	File di emissione, se specificato	*EXECUTE	*EXECUTE
	Descrizione unità posizione remota[7]	*CHANGE	
DSPRDBDIRE	File di emissione, se specificato	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
Questi comandi non richiedono l'autorizzazione agli oggetti:			
RMVRDBDIRE WRKRDBDIRE			
[1] Autorizzazione verificata quando si utilizza la voce dell'indirizzario.			

Comandi risorse

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi risorse.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
DSPHDWRSC			
DSPSFWRSC	File di emissione, se specificato	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
EDTDEVRSC			
WRKHDWRSC [1]			
[1] Se si desidera utilizzare l'opzione per la creazione di un oggetto di configurazione, è necessario disporre dell'autorizzazione per utilizzare il comando CRT appropriato.			

Comandi RJE (Remote Job Entry)

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi RJE (Remote Job Entry).

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDFCTE	Tabella di controllo moduli	*DELETE, *USE, *ADD	*READ, *EXECUTE
	File unità [1,2]	*USE	*READ, *EXECUTE
	File fisico [1,2] (RJE genera membri)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	File fisico [1,2] (membro specificato)	*USE, *ADD	*READ, *EXECUTE
	Programma [1,2]	*USE	*READ, *EXECUTE
	Coda messaggi [1,2]	*USE, *ADD	*READ, *EXECUTE
	Profilo utente QUSER	*USE	*READ, *EXECUTE
ADDRJECMNE	Descrizione sessione	*USE, *ADD, *DLT	*READ, *EXECUTE
	File BSC/CMN [1,2]	*USE	*READ, *EXECUTE
	Descrizione unità [2]	*USE	*READ, *EXECUTE
	Profilo utente QUSER	*USE	*READ, *EXECUTE
ADDRJERDRE	Descrizione sessione	*READ, *ADD, *DLT	*READ, *EXECUTE
	Coda lavori [2]	*READ	*READ, *EXECUTE
	Coda messaggi [2]	*READ, *ADD	*READ, *EXECUTE
ADDRJEWTRE	Descrizione sessione	*READ, *ADD, *DLT	*READ, *EXECUTE
	File unità [1,2]	*USE	*READ, *EXECUTE
	File fisico [1,2] (RJE genera membri)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	File fisico [1,2] (membro specificato)	*OBJOPR, *ADD	*READ, *EXECUTE
	Programma [1,2]	*USE	*READ, *EXECUTE
	Coda messaggi [1,2]	*USE, *ADD	*READ, *EXECUTE
	Profilo utente QUSER	*USE	*READ, *EXECUTE
CHGFCT	Tabella di controllo moduli	*OBJOPR, *OBJMGT	*READ, *EXECUTE
CHGFCTE	Tabella di controllo moduli	*USE	*READ, *EXECUTE
	File unità [1,2]	*USE	*READ, *EXECUTE
	File fisico [1,2] (RJE genera membri)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	File fisico [1,2] (membro specificato)	*USE, *ADD	*READ, *EXECUTE
	Programma [1,2]	*USE	*READ, *EXECUTE
	Coda messaggi [1,2]	*USE, *ADD	*READ, *EXECUTE
	Profilo utente QUSER	*USE	*READ, *EXECUTE
CHGRJECMNE	Descrizione sessione	*USE	*READ, *EXECUTE
	File BSC/CMN [1,2]	*USE	*READ, *EXECUTE
	Descrizione unità [2]	*USE	*READ, *EXECUTE
	Profilo utente QUSER	*USE	*READ, *EXECUTE
CHGRJERDRE	Descrizione sessione	*USE, *ADD, *DLT	*READ, *EXECUTE
	Coda lavori [2]	*USE	*READ, *EXECUTE
	Coda messaggi [2]	*USE, *ADD	*READ, *EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGRJEWTRE	Descrizione sessione	*USE	*READ, *EXECUTE
	File unità [1,2]	*USE	*READ, *EXECUTE
	File fisico [1,2] (RJE genera membri)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	File fisico [1,2] (membro specificato)	*OBJOPR, *ADD	*READ, *EXECUTE
	Programma [1,2]	*USE	*READ, *EXECUTE
	Coda messaggi [1,2]	*USE, *ADD	*READ, *EXECUTE
	Profilo utente QUSER	*USE	*READ, *EXECUTE
CHGSSND	Descrizione sessione	*OBJMGT, *READ, *UPD, *OBJOPR	*EXECUTE, *READ
	Coda lavori [1,2]	*USE	*EXECUTE
	Coda messaggi [1,2]	*USE, *ADD	*EXECUTE
	Tabella di controllo moduli [1,2]	*USE	*EXECUTE
	Profilo utente QUSER	*USE	*EXECUTE
CNLRJERDR	Descrizione sessione	*USE	*EXECUTE
	Coda messaggi	*USE, *ADD	*EXECUTE
CNLRJEWTR	Descrizione sessione	*USE	*EXECUTE
	Coda messaggi	*USE, *ADD	*EXECUTE
CRTFCT	Tabella di controllo moduli		*READ, *ADD
CRTRJEBSCF	File BSC		*READ, *EXECUTE, *ADD
	File fisico di origine (DDS)	*READ	*EXECUTE
	Descrizione unità	*READ	*EXECUTE
CRTRJECFG	Descrizione sessione		*READ, *ADD, *UPD, *OBJOPR
	Coda lavori		*READ, *ADD
	Descrizione lavoro		*READ, *OBJOPR, *ADD
	Descrizione sottosistema		*READ, *OBJOPR, *ADD
	Coda messaggi		*READ, *ADD
	File CMN		*READ, *EXECUTE, *ADD
	File BSC		*READ, *EXECUTE, *ADD
	File di stampa		*USE, *ADD

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTRJECFG	File fisico		*EXECUTE, *ADD
	Profilo utente QUSER [3]	*USE	*EXECUTE
	Coda di emissione	*READ	*EXECUTE
	Tabella di controllo moduli	*READ	*READ
	Descrizione unità		*EXECUTE
	Descrizione unità di controllo		*EXECUTE
	Descrizione linea		*EXECUTE
CRTRJECMNF	File comunicazioni		*READ, *EXECUTE, *ADD
	File fisico di origine (DDS)	*READ	*EXECUTE
	Descrizione unità	*READ	*EXECUTE
CRTSSND	Descrizione sessione		*READ, *ADD, *UPD, *OBJOPR
	Coda lavori [1,2]	*USE	*EXECUTE
	Coda messaggi [1,2]	*USE, *ADD	*EXECUTE
	Tabella di controllo moduli [1,2]	*USE	*EXECUTE
	Profilo utente QUSER	*USE	*EXECUTE
CVTRJEDTA	Tabella di controllo moduli	*USE	*EXECUTE
	File di immissione	*USE, *UPD	*EXECUTE
	File di emissione (RJE genera il membro)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	File di emissione (membro specificato)	*USE, *ADD	*EXECUTE
DLTFCT	Tabella di controllo moduli	*OBJEXIST	*EXECUTE
DLTRJECFG	Descrizione sessione	*OBJEXIST	*EXECUTE
	Coda lavori	*OBJEXIST	*EXECUTE
	File BSC/CMN	*OBJEXIST, *OBJOPR	*EXECUTE
	File fisico	*OBJEXIST, *OBJOPR	*EXECUTE
	File di stampa	*OBJEXIST, OBJOPR	*EXECUTE
	Coda messaggi	*OBJEXIST, *USE, *DLT	*EXECUTE
	Descrizione lavoro	*OBJEXIST	*EXECUTE
	Descrizione sottosistema	*OBJEXIST, *USE	*EXECUTE
	Descrizione unità [4]	*OBJEXIST	*EXECUTE
	Descrizione unità di controllo [4]	*OBJEXIST	*EXECUTE
	Descrizione linea [4]	*OBJEXIST	*EXECUTE
DLTSSND	Descrizione sessione	*OBJEXIST	*EXECUTE
DSPRJECFG	Descrizione sessione	*READ	*EXECUTE
ENDRJESSN [5]	Descrizione sessione	*USE	*EXECUTE
RMVFCTE	Tabella di controllo moduli	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
RMVRJECMNE	Descrizione sessione	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJERDRE	Descrizione sessione	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJEWTRE	Descrizione sessione	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
SNDRJECMD	Descrizione sessione	*USE	*EXECUTE
SBMRJEJOB	Descrizione sessione	*USE	*EXECUTE
	File di immissione [6]	*USE	*EXECUTE
	Coda messaggi	*USE, *ADD	*EXECUTE
	Oggetti relativi al lavoro [7]		
SNDRJECMD	Descrizione sessione	*USE	*EXECUTE
STRRJECSL	Descrizione sessione	*USE	*EXECUTE
	Coda messaggi	*USE	*EXECUTE
STRRJERDR	Descrizione sessione	*USE	*USE
STRRJESSN [5]	Descrizione sessione	*USE	*USE, *ADD
	Programma	*USE	*EXECUTE
	Profilo utente QUSER	*USE	*EXECUTE
	Oggetti relativi al lavoro [7]		*EXECUTE
STRRJEWTR	Descrizione sessione	*USE	*USE
	Programma [1]	*USE	*READ, *EXECUTE
	File unità [1]	*USE, *ADD	*READ, *EXECUTE
	File fisico [1] (RJE genera membri)	*OBJMGT, *USE, *ADD	*OBJOPR, *ADD
	File fisico [1] (membro specificato)	*READ, *ADD	*READ, *EXECUTE
	Coda messaggi [1]	*USE, *ADD	*READ, *EXECUTE
	Profilo utente QUSER	*USE	*READ, *EXECUTE
WRKFCT [8]	Tabella di controllo moduli	*USE	*EXECUTE
WRKRJESSN [8]	Descrizione sessione	*USE	*EXECUTE
WRKSSND [8]	Descrizione sessione	*CHANGE	*EXECUTE

1 Il profilo utente QUSER richiede l'autorizzazione a questo oggetto.

2 Se l'oggetto non viene trovato o se l'autorizzazione richiesta non è disponibile, viene inviato un messaggio informativo e la funzione del comando viene ancora eseguita.

3 Questa autorizzazione è necessaria per creare la descrizione del lavoro QRJESSN.

4 Questa autorizzazione è richiesta solo quando si specifica DLTCMN(*YES).

5 È necessario disporre dell'autorizzazione speciale *JOBCTL.

6 I file di immissione includono quelli incorporati mediante l'istruzione di controllo .. READFILE.

7 Verificare le autorizzazioni richieste per il comando SBMJOB.

8 Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.

Comandi attributi sicurezza

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi attributi sicurezza.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
CHGSECA [1]			
CHGSECAUD [2,3]			
CFGSYSSEC [1,2,3]			
DSPSECA			
DSPSECAUD [3]			
PRTSYSSECA [4]			

[1] È necessario disporre dell'autorizzazione speciale *SECADM per utilizzare questo comando.

[2] È necessario disporre dell'autorizzazione speciale *ALLOBJ per utilizzare questo comando.

[3] È necessario disporre dell'autorizzazione speciale *AUDIT per utilizzare questo comando.

[4] È necessario disporre dell'autorizzazione speciale *ALLOBJ o *AUDIT per utilizzare questo comando.

Comandi voce di autenticazione server

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi voce di autenticazione server.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ADDSVRAUTE[1]			
CHGSVRAUTE[1]			
DSPSVRAUTE	Profilo utente	*READ	*EXECUTE
RMVSVRAUTE[1]			

[1] Se il profilo utente per questa operazione non è *CURRENT o l'utente corrente per il lavoro, è necessario disporre dell'autorizzazione speciale *SECADM e delle autorizzazioni *OBJMGT e *USE sul profilo.

Comandi servizi

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi servizi.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ADDTRCFTR[11]			
APYPTF (Q)	Libreria prodotto	*OBJMGT	
CHGSRVA [3] (Q)			
CHKCMNTRC [3] (Q)			*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHKPRDOPT (Q)	Tutti gli oggetti nell'opzione prodotto [4]		
CPYPTF[2](Q)	Da file	*USE	*EXECUTE
	File-di-destinazione[8]	Stessi requisiti del comando SAVOBJ	Stessi requisiti del comando SAVOBJ
	Descrizione unità	*USE	*EXECUTE
	Programma su licenza		*USE
	Comandi: CHKTAP, CPYFRMTAP, CPYTOTAP, CRTLIB, CRTSAVF, CRTTAPF e OVRTAPF	*USE	*EXECUTE
	Libreria QSRV	*USE	*EXECUTE
CPYPTFGRP[2] (Q)	Descrizione unità	*USE	*EXECUTE
	A file	*Stessi requisiti del comando SAVOBJ	*Stessi requisiti del comando SAVOBJ
	Da file	*USE	*EXECUTE
	Comandi: CHKTAP, CRTLIB, CRTSAVF	*USE	*EXECUTE
DLTAPARDTA (Q)			
DLTCMNTRC [3] (Q)	NWID (ID di rete) o descrizione linea	*USE	*EXECUTE
DLTPTF (Q)	File lettera di accompagnamento [4]		*EXECUTE
	File di salvataggio PTF [4]		*EXECUTE
DLTTRC (Q)	Comando RMVM	*USE	
	Libreria QSYS	*EXECUTE	
	File di database	*OBJEXIST, *OBJOPR	
DMPJOB (Q)			*EXECUTE
DMPJOBINT (Q)			
DSPPTF (Q)	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
DSPSRVA (Q)			
DSPSRVSTS (Q)			
DSPSSTUSR [20]			
ENDCMNTRC [3] (Q)	NWID o descrizione linea	*USE	*EXECUTE
ENDCPYSCN (Q)	Descrizione unità	*USE	*EXECUTE
ENDSRVJOB (Q)			
ENDTRC (Q)	Libreria QSYS	*ADD, *EXECUTE	
	File di database	*OBJOPR, *OBJMGMT, *ADD, *DLT	
	Comandi: PTRTRC, DLTTRC	*USE	
EDNWCH[16] (Q)	Sessioni di controllo che ricercano un messaggio nella registrazione lavori[18]		
INSPTF[9] (Q)			
LODPTF (Q)	Descrizione unità	*USE	*EXECUTE
LODRUN [2]	Comando RSTOBJ	*USE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
PRTCMNTRC [3] (Q)	NWID (ID di rete) o descrizione linea	*USE	*EXECUTE
	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
PRTERRLOG (Q)	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
PRTINTDTA[12,13] (Q)			
PRTTRC[11](Q)	Libreria QSYS	*EXECUTE	
	File di database	*USE	
	Comando DLTTRC	*USE	
RMVPTF (Q)	Libreria prodotto	*OBJMGT	
RMVTRCFTR[11]			
RUNLPDA (Q)	Descrizione linea	*READ	*EXECUTE
SAVAPARDTA [6] (Q)	Comandi: CRTDUPOBJ, CRTLIB, CRTOUTQ, CRTSAVF, DLTF, DMPOBJ, DMPSYSOBJ, DSPCTLD, DSPDEVD, DSPHDWRSC, DSPJOB, DSPLIND, DSPLOG, DSPNWID, DSPPTF, DSPSFWRSC, OVRPRTF, PRTERRLOG, PRTINTDTA, SAV, SAVDLO, SAVLIB, SAVOJB, WRKACTJOB e WRKSYSVAL	*USE	*EXECUTE
	Problema esistente [7]	*CHANGE	*EXECUTE
SNDPTFORD [10] (Q)	CRTIMGCLG	*USE	
	QUSRSYS		*ADD, *READ
SNDSRVRQS (Q)			
STRCMNTRC [11] (Q)	NWID (ID di rete) o descrizione linea	*USE	*EXECUTE
	Lavoro controllato[17]		
	Programma di traccia	*OBJOPR e *EXECUTE	*EXECUTE
	Coda messaggi	*USE	*USE
STRCPYSCN	Coda lavori	*USE	*EXECUTE
	Descrizione unità	*USE	*EXECUTE
	File di emissione, se specificato	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
STRSRVJOB (Q)	Profilo utente del lavoro	*USE	*EXECUTE
STRSST [3] (Q)			
STRTRC (Q)[11, 15]	Lavoro controllato[17]		
	Programma di traccia	*OBJOPR e *EXECUTE	*EXECUTE
	Coda messaggi	*USE	*USE
STRWCH[16] (Q)	Lavoro controllato[17]		
	Programma di controllo	*OBJOPR e *EXECUTE	*EXECUTE
	Coda messaggi	*USE	*USE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
TRCCNN[11](Q)	Lavoro controllato[17]		
	Programma di traccia	*OBJOPR e *EXECUTE	*EXECUTE
	Coda messaggi	*USE	*USE
TRCCPIC (Q)			
TRCICF (Q)			
TRCINT[11] (Q)	Lavoro controllato[17]		
	Programma di traccia	*OBJOPR e *EXECUTE	*EXECUTE
	Coda messaggi	*USE	*USE
TRCJOB (Q)	File di emissione, se specificato	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
	Programma di uscita, se specificato	*USE	*EXECUTE
TRCTCPAPP[11] (Q)	Descrizione linea	*USE	
	Interfaccia di rete	*USE	
	Interfaccia di rete	*USE	
	Lavoro controllato[17]		
	Programma di traccia	*OBJOPR e *EXECUTE	*EXECUTE
	Coda messaggi	*USE	*USE
VFYCMN (Q)	Descrizione linea [5]	*USE	*EXECUTE
	Descrizione unità di controllo [5]	*USE	*EXECUTE
	ID di rete [5]	*USE	*EXECUTE
VFYLNKLPDA (Q)	Descrizione linea	*READ	*EXECUTE
VFYPRT (Q)	Descrizione unità	*USE	*EXECUTE
VFYOPT (Q)	Descrizione unità	*USE	*EXECUTE
VFYTAP[14] (Q)	Descrizione unità	*USE, *OBJMGT	*EXECUTE
WRKCNTINF (Q)			
WRKFSTAF (Q)	QUSRSYS/QPVINDEX *USRIDX	*CHANGE	*USE
WRKFSTPCT (Q)	QUSRSYS/QPVPCTABLE *USRIDX	*CHANGE	*USE
WRKPRB [1, 10] (Q)	Linea, unità di controllo, NWID (ID di rete) e unità basata sull'azione di analisi dei problemi	*USE, *ADD	*EXECUTE
WRKPTFGRP (Q)			
WRKPTFORD (Q)	QESCPTFO e SNDPTFORD	*USE	
WRKSRVPVD (Q)			
WRKTRC[11] (Q)			
WRKWCH[19] (Q)			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
[1]	È necessaria l'autorizzazione al comando PRTERRLOG per alcune procedure di analisi o se i record delle registrazioni errori vengono salvati.		
[2]	Si applicano anche tutte le restrizioni per il comando RSTOBJ.		
[3]	È necessario disporre dell'autorizzazione speciale al servizio (*SERVICE) per utilizzare questo comando.		
[4]	Gli oggetti elencati vengono utilizzati dal comando, ma l'autorizzazione sugli oggetti non viene controllata. L'autorizzazione per l'utilizzo del comando è sufficiente per utilizzare gli oggetti.		
[5]	È necessaria l'autorizzazione *USE sull'oggetto delle comunicazioni che si sta verificando.		
[6]	È necessario disporre dell'autorizzazione speciale *SPLCTL per salvare un file di spool.		
[7]	Quando si esegue il comando SAVAPARDTA per un nuovo problema, viene creata una libreria APAR univoca per tale problema. Se, per lo stesso problema, si esegue nuovamente il comando SAVAPARDTA per raccogliere un numero maggiore di informazioni, è necessario disporre dell'autorizzazione all'utilizzo sulla libreria APAR per il problema.		
[8]	L'opzione per aggiungere un nuovo membro ad un file di emissione esistente non è valida per questo comando.		
[9]	Questo comando dispone delle stesse autorizzazioni e limitazioni dei comandi APYPTF e LODPTF.		
[10]	Per accedere alle opzioni 1 e 3 sul pannello "Selezione opzione di documentazione", è necessario disporre dell'autorizzazione *USE sul comando SNDSRVRQS. Le seguenti restrizioni si applicano al parametro IMGDIR: • È necessario disporre dell'autorizzazione *X a ogni indirizzario nel percorso. • È necessario disporre dell'autorizzazione *WX all'indirizzario che contiene l'immagine ottica.		
[11]	Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *SERVICE o essere autorizzati ad utilizzare la funzione Traccia di servizio di i5/OS tramite Gestione applicazione in System i Navigator. Il comando Modifica utilizzo funzione (CHGFCNUSG), con un ID funzione dei QIBM_SERVICE_TRACE, può essere utilizzato anche per modificare l'elenco di utenti autorizzati all'esecuzione delle operazioni di traccia.		
[12]	Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *SERVICE o essere autorizzati ad utilizzare la funzione Dump di servizio di i5/OS tramite Gestione applicazione in System i Navigator. Il comando Modifica utilizzo funzione (CHGFCNUSG), con un ID funzione ID di QIBM_SERVICE_DUMP, può essere utilizzato anche per modificare l'elenco di utenti autorizzati all'esecuzione delle operazioni di dump.		
[13]	Questo comando deve essere emesso dal lavoro con dati interni da stampare oppure chi emette il comando deve lavorare nel profilo utente che è lo stesso dell'identità utente del lavoro di un lavoro con dati interni in fase di stampa oppure chi emette il comando deve lavorare in un profilo utente con autorizzazione speciale al controllo del lavoro (*JOBCTL).		
[14]	È necessario disporre dell'autorizzazione speciale *IOSYSCFG quando la descrizione unità è assegnata da un'unità libreria supporti magnetici.		
[15]	Se si specifica un nome utente generico per il parametro Nome lavoro (JOB), è necessario disporre dell'autorizzazione speciale a tutti gli oggetti (*ALLOBJ) o essere autorizzati alla funzione traccia di qualsiasi utente di i5/OS tramite Gestione applicazione in System i Navigator. È inoltre possibile utilizzare il comando CHGFCNUSG (Modifica utilizzo funzione), con un ID funzione di QIBM_ALLOBJ_TRACE, per modificare l'elenco di utenti a cui è consentita l'esecuzione di operazioni di traccia.		

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**

[16] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale al servizio (*SERVICE) o essere autorizzati alla funzione controllo di servizio i5/OS tramite Gestione applicazione in System i Navigator. È inoltre possibile utilizzare il comando CHGFCNUSG (Modifica utilizzo funzione), con un ID funzione di QIBM_SERVICE_WATCH, per modificare l'elenco di utenti a cui è consentita l'avvio e l'arresto delle operazioni di controllo.

[17] L'autorizzazione speciale di controllo lavoro (*JOBCTL) è necessaria se il lavoro è in esecuzione per un utente differente rispetto all'identità utente del lavoro per il lavoro controllato. L'autorizzazione speciale all'oggetto (*ALLOBJ) è necessaria se si specifica *ALL per il nome del lavoro controllato o un nome utente generico. Un utente che non dispone dell'autorizzazione speciale *ALLOBJ può eseguire la funzione se è autorizzato alla funzione di controllo di qualsiasi lavoro di i5/OS tramite Gestione applicazione in System i Navigator. È inoltre possibile utilizzare il comando CHGFCNUSG (Modifica utilizzo funzione), con un ID funzione di QIBM_WATCH_ANY_JOB, per modificare l'elenco di utenti a cui è consentito l'avvio e l'arresto delle operazioni di controllo.

[18] Stessa autorizzazione richiesta sul comando STRWCH.

[19] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale al servizio (*SERVICE) o essere autorizzati alla funzione traccia di servizio e alla funzione controllo di servizio di i5/OS tramite Gestione applicazione in System i Navigator. È inoltre possibile utilizzare il comando CHGFCNUSG (Modifica utilizzo funzione), con un ID funzione di QIBM_SERVICE_TRACE e QIBM_SERVICE_WATCH, per modificare l'elenco di utenti a cui è consentita l'esecuzione di operazioni di traccia.

[20] È necessario disporre delle autorizzazioni speciali al controllo (*AUDIT) e amministratore della riservatezza (*SECADM) per utilizzare questo comando.

Comandi Dizionario di ausilio ortografico

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi dizionario ausilio ortografico.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTSPADCT	Dizionario di ausilio ortografico	*OBJEXIST	*EXECUTE
	Dizionario - REPLACE(*NO)		*READ, *ADD
	Dizionario - REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
DLTSPADCT	Dizionario di ausilio ortografico	*OBJEXIST	*EXECUTE
WRKSPADCT [1]	Dizionario di ausilio ortografico	Qualsiasi autorizzazione	*USE

[1] Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.

Comandi sfera di controllo

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi sfera di controllo.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDSOCE	Sfera di controllo [1]	*USE, *ADD	*EXECUTE
DSPSOCSTS			
RMVSOCE	Sfera di controllo [1]	*USE, *DLT	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
WRKSOC	Sfera di controllo [1]	*USE	*EXECUTE
[1] La sfera di controllo è il file fisico QUSRSYS/QAALSOC.			

Comandi file di spool

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi file di spool.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Parametri coda di emissione			Autorizzaz. speciale	Autorizzazione necessaria	
		DSPDTA	AUTCHK	OPRCTL		Per oggetto	Per libreria
CHGSPLFA [1,2]	Coda di emissione [3]		*DTAAUT			*READ, *DLT, *ADD	
			*OWNER			Propriet.[4]	
				*YES	*JOBCTL		
CHGSPLFA [1], se si sposta il file di spool	Coda di emissione originale [3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Propriet.[4]	
				*YES	*JOBCTL		
	File di spool	*OWNER				Propriet.[6]	
	Coda di emissione di destinazione[7]					*READ	*EXECUTE
				*YES	*JOBCTL		*EXECUTE
	Unità di destinazione					*USE	
CPYSPLF [1]	File di database					Fare riferimento alle regole generali per la Visualizzazione (DSP) o altre operazioni utilizzando il file di emissione (OUTPUT (*OUTFILE))	Fare riferimento alle regole generali per la Visualizzazione (DSP) o altre operazioni utilizzando il file di emissione (OUTPUT (*OUTFILE))
	File di spool	*OWNER				Propriet.[6]	
	Coda di emissione [3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Propriet.[4]	
		*YES o *NO		*YES	*JOBCTL		

Comando	Oggetto di riferimento	Parametri coda di emissione			Autorizzaz. speciale	Autorizzazione necessaria	
		DSPDTA	AUTCHK	OPRCTL		Per oggetto	Per libreria
DLTEXPSPLF (Q) [10]	Lotto dischi indipendente[9]					*USE	
DLTSPLF [1]	Coda di emissione [3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Propriet.[4]	
				*YES	*JOBCTL		
DSPSPLF [1]	Coda di emissione [3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Propriet.[4]	
		*YES o *NO		*YES	*JOBCTL		
	File di spool	*OWNER				Propriet.[6]	
HLDSPLF [1]	Coda di emissione [3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Propriet.[4]	
				*YES	*JOBCTL		
RCLSPLSTG (Q) [10]	Lotto dischi indipendente[9]					*USE	
RLSSPLF [1, 8]	Coda di emissione [3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Propriet.[4]	
				*YES	*JOBCTL		
SNDNETSPLF [1,5]	Coda di emissione [3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Propriet.[4]	
		*YES o *NO		*YES	*JOBCTL		
	File di spool	*OWNER				Propriet.[6]	
SNDTCPSPLF [1,5]	Coda di emissione [3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Propriet.[4]	
		*YES o *NO		*YES	*JOBCTL		
	File di spool	*OWNER				Propriet.[6]	
STRSPLRCL (Q)[9, 10]	Lotto dischi indipendente[9]					*USE	
WRKSPLF							

Comando	Oggetto di riferimento	Parametri coda di emissione			Autorizzaz. speciale	Autorizzazione necessaria	
		DSPDTA	AUTCHK	OPRCTL		Per oggetto	Per libreria

[1] Gli utenti sono sempre autorizzati al controllo dei propri file di spool.

[2] Per spostare un file di spool davanti ad una coda di emissione (PRTSEQ(*NEXT)) o modificarne la priorità in un valore maggiore rispetto al limite specificato nel profilo utente, è necessario disporre di una delle autorizzazioni visualizzate per la coda di emissione o dell'autorizzazione speciale *SPLCTL.

[3] Se si dispone dell'autorizzazione speciale *SPLCTL, non è necessario disporre di un'autorizzazione sulla coda di emissione.

[4] È necessario essere il proprietario della coda di emissione.

[5] È necessario disporre dell'autorizzazione *USE sulla coda di emissione e sulla libreria della coda di emissione del destinatario quando si invia un file ad un utente sullo stesso sistema.

[6] L'utente deve essere il proprietario del file di spool.

[7] Nel caso in cui l'utente disponesse dell'autorizzazione speciale *SPLCTL, l'autorizzazione sulla coda di emissione di destinazione non è necessaria, mentre invece è necessario disporre dell'autorizzazione *EXECUTE sulla relativa libreria.

[8] Quando il file di spool viene conservato con HLDJOB SPLFILE(*YES) e il file di spool è stato separato dal lavoro, l'utente dovrà disporre dell'autorizzazione *USE sul comando RLSJOB e disporre dell'autorizzazione speciale *JOBCTL o essere il proprietario del file di spool.

[9] È necessario disporre dell'autorizzazione *USE a tutti i lotti disco indipendenti in un lotto dischi indipendente.

[10] È necessario disporre dell'autorizzazione speciale *SPLCTL per eseguire questo comando.

Comandi descrizione sottosistema

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi descrizione sottosistema.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ADDAJE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descrizione lavoro[9]	*OBJOPR, *READ	*EXECUTE
ADDCMNE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descrizione lavoro[9]	*OBJOPR, *READ	*EXECUTE
	Profilo utente	*USE	
ADDJOBQE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE
ADDPJE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Profilo utente	*USE	
	Descrizione lavoro[9]	*OBJOPR, *READ	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ADDRTGE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE
ADDWSE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descrizione lavoro[9]	*OBJOPR, *READ	*EXECUTE
CHGAJE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descrizione lavoro[9]	*OBJOPR, *READ	*EXECUTE
CHGCMNE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descrizione lavoro[9]	*OBJOPR, *READ	*EXECUTE
	Profilo utente	*USE	
CHGJOBQE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE
CHGPJE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Profilo utente	*USE	
	Descrizione lavoro[9]	*OBJOPR, *READ	*EXECUTE
CHGRTGE	Descrizione sottosistema	*OJBOPR, *OBJMGT, *READ	*EXECUTE
CHGSBSD [5, 7]	Descrizione sottosistema	*OJBOPR, *OBJMGT, *READ	*EXECUTE
	file di visualizzazione accesso[4]	*USE	*EXECUTE
CHGWSE	Descrizione sottosistema	*OJBOPR, *OBJMGT, *READ	*EXECUTE
	Descrizione lavoro[9]	*OBJOPR, *READ	*EXECUTE
CRTSBSD [5] (Q)	Descrizione sottosistema		*READ, *ADD
	file di visualizzazione accesso[4]	*USE	*EXECUTE
	Descrizione unità ASP (auxiliary storage pool [8]	*USE	
DLTSBSD	Descrizione sottosistema	*OBJEXIST, *USE	*EXECUTE
DSPSBSD	Descrizione sottosistema	*OBJOPR, *READ	*EXECUTE
ENDSBS [1]			
PRTSBSDAUT [6]			
RMVAJE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVCMNE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVJOBQE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVPJE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVRTGE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
RMVWSE	Descrizione sottosistema	*OBJOPR, *OBJMGT, *READ	*EXECUTE
STRSBS [1]	Descrizione sottosistema	*USE	*EXECUTE
	Descrizione unità ASP (auxiliary storage pool)	*USE	
WRKSBS [2, 3]	Descrizione sottosistema	Qualsiasi autorizzazione	*USE
WRKSBSD [3]	Descrizione sottosistema	Qualsiasi autorizzazione	*USE

[1] È necessario disporre dell'autorizzazione speciale sul controllo del lavoro (*JOBCTL) per poter utilizzare questo comando.

[2] Richiede alcune autorizzazioni (tutte tranne *EXCLUDE)

[3] Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.

[4] L'autorizzazione è necessaria per completare i controlli dei formati del file di visualizzazione. Ciò consente di prevedere se il pannello funzionerà correttamente all'avvio del sottosistema. Se non si è autorizzati al file di visualizzazione o alla relativa libreria, tali controlli dei formati non verranno eseguiti.

[5] È necessario disporre dell'autorizzazione speciale *SECADM o *ALLOBJ per specificare una libreria specifica per la libreria del sottosistema.

[6] È necessario disporre dell'autorizzazione speciale *ALLOBJ o *AUDIT per utilizzare questo comando.

[7] È necessario disporre delle autorizzazioni speciali *ALLOBJ e *SECADM per modificare il nome gruppo ASP (auxiliary storage pool).

[8] Per specificare una descrizione dell'unità ASP che non esiste, è necessario disporre dell'autorizzazione speciale a tutti gli oggetti (*ALLOBJ).

[9] Per specificare una descrizione lavoro che non esiste, è necessario disporre dell'autorizzazione speciale a tutti gli oggetti (*ALLOBJ).

Comandi di sistema

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi di sistema.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. L'argomento Comandi forniti con autorizzazione pubblica *EXCLUDE mostra i profili utente forniti da IBM autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
PWRDWNSYS[1]	Catalogo immagini (se specificato)	*USE	
RTVSYSINF (Q)[2]	Libreria	*READ, *ADD, *EXECUTE	
Questi comandi non richiedono le autorizzazioni agli oggetti:			
CHGSHRPOOL DSPSYSSTS ENDSYS[1] PRTSYSINF (Q)	RCLACTGRP[1] RCLRSC RETURN RTVGRPA	SIGNOFF UPDSYSINF (Q)[3] WRKSHRPOOL	WRKSYSSTS

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**

[1] È necessario disporre dell'autorizzazione speciale sul controllo del lavoro (*JOBCTL) per poter utilizzare questo comando.

[2] È necessario disporre dell'autorizzazione speciale *SAVSYS per utilizzare questo comando.

[3] È necessario disporre delle autorizzazioni speciali *SECADM, *ALLOBJ, *AUDIT, *JOBCTL e *SAVSYS per utilizzare questo comando.

Comandi elenco di risposte sistema

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi elenco di risposte sistema.

Questi comandi non richiedono le autorizzazioni oggetto:			
ADDRPYLE (Q)	CHGRPYLE (Q)	RMVRPYLE (Q)	WRKRPYLE

Comandi valori di sistema

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi valori di sistema.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Questi comandi non richiedono l'autorizzazione agli oggetti:			
CHGSYSVAL (Q) [1,2]	DSPSYSVAL[3]	RTVSYSVAL[3]	WRKSYSVAL [1,2, 3]

[1] Per modificare alcuni valori di sistema, è necessario disporre delle autorizzazioni speciali *ALLOBJ, *ALLOBJ e *SECADM, *AUDIT, *IOSYSCFG o *JOBCTL.

[2] Per utilizzare questi comandi nel modo indicato da IBM, è necessario essere collegati come QPGMR, QSYSOPR o QSRV oppure disporre dell'autorizzazione speciale *ALLOBJ.

[3] Per visualizzare o richiamare valori di sistema relativi al controllo, è necessario disporre dell'autorizzazione speciale *AUDIT o *ALLOBJ.

Comandi ambiente System/36

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi ambiente System/36.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGS36	Oggetto configurazione S/36 QS36ENV	*UPD	*EXECUTE
CHGS36A	Oggetto configurazione S/36 QS36ENV	*UPD	*EXECUTE
CHGS36PGMA	Programma	*OBJMGT, *USE	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CHGS36PRCA	File QS36PRC	*OBJMGT, *USE	*EXECUTE
CHGS36SRCA	Origine	*OBJMGT, *USE	*EXECUTE
CRTMSGFMNU	Menu: REPLACE(*NO)		*READ, *ADD
	Menu: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD
	Visualizzazione file se esiste	*ALL	*EXECUTE
	File di messaggi	*USE	*CHANGE
	File di origine QS36SRC	*ALL	*EXECUTE
CRTS36DSPF	File di visualizzazione: REPLACE(*NO)		*READ, *ADD
	File di visualizzazione: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD, *CHANGE
	File di origine a file quando TOMBR non è *NONE	*ALL	*CHANGE
	File di origine QS36SRC	*USE	*EXECUTE
	Comando CRTDSPF (Creazione file di visualizzazione)	*OBJOPR	*EXECUTE
CRTS36MNU	Menu: REPLACE(*NO)		*READ, *ADD, *CHANGE
	Menu: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD, *CHANGE
	File di origine a file quando TOMBR non è *NONE	*ALL	*CHANGE
	File di origine QS36SRC	*USE	*EXECUTE
	File di visualizzazione quando si specifica REPLACE(*YES)	*ALL	*EXECUTE
	File di messaggi denominati nell'origine	*ALL	*EXECUTE
	File di visualizzazione		*CHANGE
	Comando CRTMSGF	*OBJOPR, *OBJEXIST	*EXECUTE
	Comando ADDMSGD	*OBJOPR	*EXECUTE
	Comando CRTDSPF	*OBJOPR	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTS36MSGF	File dei messaggi: REPLACE(*NO)		*READ, *ADD, *CHANGE
	File dei messaggi: REPLACE(*YES)	Fare riferimento alle regole generali.	*READ, *ADD, *CHANGE
	File di origine a file quando TOMBR non è *NONE	*ALL	*CHANGE
	File di origine QS36SRC	*USE	*EXECUTE
	File di visualizzazione quando si specifica REPLACE(*YES)	*ALL	*EXECUTE
	File di messaggi denominati nell'origine	*ALL	*EXECUTE
	File dei messaggi denominati nell'origine quando OPTION è *ADD o *CHANGE	*CHANGE	*EXECUTE
	File dei messaggi denominati nell'origine quando si specifica OPTION(*CREATE)	*ALL	*EXECUTE
	Comando CRTMSGF	*OBJOPR, *OBJEXIST	*EXECUTE
	Comando ADDMSGD	*OBJOPR	*EXECUTE
	Comando CHGMSGD quando si specifica OPTION(*CHANGE)	*OBJOPR	*EXECUTE
DSPS36	Oggetto configurazione S/36 QS36ENV	*READ	*EXECUTE
EDTS36PGMA	Programma, per modificare gli attributi	*OBJMGT, *USE	*EXECUTE
	Programma, per visualizzare gli attributi	*USE	*EXECUTE
EDTS36PRCA	File QS36PRC, per modificare gli attributi	*OBJMGT, *USE	*EXECUTE
	File QS36PRC, per visualizzare gli attributi	*USE	*EXECUTE
EDTS36SRCA	File di origine QS36SRC, per modificare gli attributi	*OBJMGT, *USE	*EXECUTE
	File di origine QS36SRC, per visualizzare gli attributi	*USE	*EXECUTE
RSTS36F (Q)	Da file	*USE	*EXECUTE
	A file	*ALL	Fare riferimento alle regole generali.
	Basato su file fisici, se il file ripristinato è un file logico (alternativo)	*CHANGE	*EXECUTE
	File unità o descrizione unità	*USE	*EXECUTE
RSTS36FLR [1,2,3] (Q)	Cartella S/36	*USE	*EXECUTE
	Cartella di destinazione	*CHANGE	*EXECUTE
	File unità o descrizione unità	*USE	*EXECUTE
RSTS36LIBM (Q)	Da file	*USE	*EXECUTE
	A file	*ALL	Fare riferimento alle regole generali.
	File unità o descrizione unità	*USE	*EXECUTE
RTVS36A	Oggetto configurazione S/36 QS36ENV	*UPD	*EXECUTE

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
SAVS36F	Da file	*USE	*EXECUTE
	File di destinazione, quando si tratta di un file fisico	*ALL	Fare riferimento alle regole generali.
	File unità o descrizione unità	*USE	*EXECUTE
SAVS36LIBM	Da file	*USE	*EXECUTE
	File di destinazione, quando si tratta di un file fisico	*ALL	Fare riferimento alle regole generali.
	File unità o descrizione unità	*USE	*EXECUTE
WRKS36	Oggetto configurazione S/36 QS36ENV	*READ	*EXECUTE
WRKS36PGMA	Programma, per modificare gli attributi	*OBJMGT, *USE	*EXECUTE
	Programma, per visualizzare gli attributi	*USE	*EXECUTE
WRKS36PRCA	File QS36PRC, per modificare gli attributi	*OBJMGT, *USE	*EXECUTE
	File QS36PRC, per visualizzare gli attributi	*USE	*EXECUTE
WRKS36SRCA	File di origine QS36SRC, per modificare gli attributi	*OBJMGT, *USE	*EXECUTE
	File di origine QS36SRC, per visualizzare gli attributi	*USE	*EXECUTE

[1] È necessario disporre dell'autorizzazione *ALL sul comando, se lo si sta sostituendo. È necessaria l'autorizzazione operativa o su tutti i dati per la cartella se si stanno ripristinando le nuove informazioni sulle cartelle oppure è necessaria l'autorizzazione speciale *ALLOBJ.

[2] Se utilizzata per un dizionario dati, viene richiesta solo l'autorizzazione sul comando.

[3] È necessario essere iscritti nell'indirizzario della distribuzione del sistema se la cartella di origine è una cartella di documenti.

Comandi tabella

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi tabella.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTTBL	Tabella		*READ, *ADD, *EXECUTE
	File di origine	*USE	*EXECUTE
DLTTBL	Tabella	*OBJEXIST	*EXECUTE
WRKTBL [1]	Tabella	Qualsiasi autorizzazione	*USE

[1] Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione.

Comandi TCP/IP

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi TCP/IP.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ADDTCPSVR[1]	Programma da richiamare	*EXECUTE	*EXECUTE
CHGTCPSVR[1]	Programma da richiamare	*EXECUTE	*EXECUTE
CPYTCPHT [6]	Oggetti file		
CVTTCPCL (Q)	Oggetti file	*USE	*EXECUTE
ENDTCPPTP	Descrizione linea [4]	*USE	*EXECUTE
	Descrizione unità di controllo [4]	*USE	*EXECUTE
	Descrizione unità [4]	*USE	*EXECUTE
	Oggetti file	*USE	*EXECUTE
ENDTCPSRV (Q)	Oggetti file	*USE	*EXECUTE
FTP	Oggetti file	*USE	*EXECUTE
	Oggetti tabella	*USE	*EXECUTE
LPR [2]	Oggetto personalizzaz. stazione di lavoro	*USE	*EXECUTE
SETVTTBL	Oggetti tabella	*USE	*EXECUTE
SNDTCPSPLF [2]	Oggetto personalizzaz. stazione di lavoro	*USE	*EXECUTE
STRTCPFTP	Oggetti tabella	*USE	*EXECUTE
	Oggetti file	*USE	*EXECUTE
STRTCPPTP	Descrizione linea [4]	*USE	*EXECUTE
	Descrizione unità di controllo [4]	*USE	*EXECUTE
	Descrizione unità [4]	*USE	*EXECUTE
	Oggetti file	*USE	*EXECUTE
STRTCPSVR (Q)	Oggetti tabella	*USE	*EXECUTE
	Oggetti file	*USE	*EXECUTE
STRTCPTELN	Oggetti tabella	*USE	*EXECUTE
	Oggetti file	*USE	*EXECUTE
	Unità stazione di lavoro virtuale[5]	*USE	*EXECUTE
TELNET	Oggetti tabella	*USE	*EXECUTE
	Oggetti file	*USE	*EXECUTE
	Unità stazione di lavoro virtuale[5]	*USE	*EXECUTE
Questi comandi non richiedono le autorizzazioni agli oggetti:			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
ADDCOMSNMP [1]	CFGRTG	CHGVTMAP	RMVTCPRSI [1]
ADDNETTBLE [1]	CFGTCPSMTP	DSPVTMAP	RMVTCPRTE [1]
ADDOSPFARA[1]	CFGTCPSNMP	ENDTCP (Q)	RMVTCPSVR [1]
ADDOSPFLNK[1]	CFGTCPTELN	ENDTCPCNN	RNMTCPHTE [1]
ADDOSPFIFC[1]	CHGCOMSNMP [1]	ENDTCPIFC (Q)	SETVTMAP
ADDOSPFRNG[1]	CHGFTPA [1]	MGRTCPHT [1]	STRTCP (Q)
ADDPCLTBLE [1]	CHGLPDA [1]	NETSTAT	STRTCPIFC (Q)
ADDRIPACP[1]	CHGOSPFA[1]	PING	VFYTCPCNN
ADDRIPFLT[1]	CHGOSPFARA[1]	RMVCOMSNMP [1]	WRKNAMSMTP [3]
ADDRIPIFC[1]	CHGOSPFIFC[1]	RMVNETTBLE [1]	WRKNETTBLE[1]
ADDRIPIGN[1]	CHGOSPFLNK[1]	RMVOSPFARA[1]	WRKPCLTBLE[1]
ADDSRVTBLE [1]	CHGOSPFRNG[1]	RMVOSPFIFC[1]	WRKSRVTBLE[1]
ADDTCPHTE [1]	CHGRIPA[1]	RMVOSPFLNK[1]	WRKTCPSTS
ADDTCPIFC [1]	CHGRIPFLT[1]	RMVOSPFRNG[1]	
ADDTCPPORT [1]	CHGRIPIFC[1]	RMVPCLTBLE [1]	
ADDTCPRSI [1]	CHGSMTPA [1]	RMVRIPACP[1]	
ADDTCPRTE [1]	CHGSNMPA [1]	RMVRIPFLT[1]	
CFGTCP	CHGTCPA [1]	RMVRIPIFC[1]	
CFGTCPAPP	CHGTCPHTE[1]	RMVRIPIGN[1]	
CFGTCPFTP [1]	CHGTCPIFC[1]	RMVSRVTBLE [1]	
CFGTCPLPD [1]	CHGTCPRTE [1]	RMVTCPHTE[1]	
	CHGTELNA [1]	RMVTCPIFC[1]	
		RMVTCPPORT [1]	

1 È necessario disporre dell'autorizzazione speciale *IOSYSCFG per utilizzare questo comando.

2 Il comando SNDTCPSPLF e il comando LPR utilizzano le stesse combinazioni di autorizzazioni oggetto di riferimento del comando SNDNETSPLF.

3 L'utente deve disporre dell'autorizzazione speciale *SECADM per modificare la tabella alias di sistema o la tabella alias di un altro profilo utente.

4 Se si dispone dell'autorizzazione speciale *JOBCTL, non è necessaria l'autorizzazione specificata sull'oggetto.

5 Se si dispone dell'autorizzazione speciale *JOBCTL, non è necessaria l'autorizzazione specificata sull'oggetto sul sistema remoto.

6 Per le autorizzazioni richieste, fare riferimento alla descrizione della sezione Visualizzazione (DSP) o altre operazioni utilizzando il file di emissione (OUTPUT(*OUTFILE)) nell'argomento Regole generali per le autorizzazioni oggetto sui comandi.

Comandi descrizione fuso orario

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi descrizione fuso orario.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
CHGTIMZON	Descrizione fuso orario	*CHANGE	*EXECUTE
CRTTIMZON	Descrizione fuso orario		*READ, *ADD

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
DLTTIMZON[1]	Descrizione fuso orario	*OBJEXIST	*EXECUTE
WRKTIMZON[2]	Descrizione fuso orario	*USE	*USE

[1] La descrizione del fuso orario specificato nel valore di sistema QTIMZON non può essere cancellato.

[2] Se viene utilizzato un messaggio per specificare i nomi abbreviati o quelli completi della descrizione del fuso orario, è necessario disporre dell'autorizzazione *USE sul file dei messaggi e dell'autorizzazione *EXECUTE sulla libreria del file dei messaggi per visualizzare i nomi completi e abbreviati.

Comandi aggiornamento dati informazioni ordine

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi aggiornamento dati informazione ordine.

Questi comandi vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
WRKORDINF	File QGPL/QMAHFILE	*CHANGE, *OBJALTER	*EXECUTE

Comandi indice utente, coda utente e spazio utente

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi indice utente, coda utente e spazio utente.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	Per libreria
DLTUSRIDX	Indice utente	*OBJEXIST	*EXECUTE
DLTUSRQ	Coda utente	*OBJEXIST	*EXECUTE
DLTUSRSPC	Spazio utente	*OBJEXIST	*EXECUTE

Comandi UDFS

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi UDFS (user-defined file system).

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto
ADDMFS [1,2,3]	dir_to_be_mounted_over	*DIR	"root" (/)	*W
	Prefisso percorso	Fare riferimento alle regole generali.		
CRTUDFS [1,2,6,7] (Q)	/dev/QASP*xx* o /dev/IASPname	*DIR	"root" (/)	*RWX

Comando	Oggetto di riferimento	Tipo oggetto	File system	Autorizzaz. necessaria per l'oggetto
DLTUDFS [1,2,4,5,8,9,10] (Q)	/dev/QASP*xx* o /dev/IASPname	*DIR	″root″ (/)	*RWX
	qualsiasi oggetto IFS (integrated file system) in UDFS		″root″ (/)	*OBJEXIST
	Qualsiasi oggetto indirizzario non vuoto	*DIR	″root″ (/)	*WX
DSPUDFS	some_dirsxx	*DIR	″root″ (/)	*RX
MOUNT [1,2,3]	dir_to_be_ mounted_over	*DIR	″root″ (/)	*W
	Prefisso percorso	Fare riferimento alle regole generali.		
RMVMFS [1]				
UNMOUNT [1]				

[1] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *IOSYSCFG.

[2] Esistono due convenzioni di denominazione indirizzario a seconda dell'ubicazione dell'UDFS (user-defined file system). Utilizzare una delle seguenti convenzioni:

- - /dev/QASPxx dove *xx* è 01 per l'asp di sistema o 02-32 per gli asp dell'utente di base.
- - /dev/IASPname dove *IASPname* è il nome dell'ASP indipendente.

Questo è l'indirizzario contenente il *BLKSF caricato.

[3] L'indirizzario caricato (dir_to_be_mounted_over) è un qualsiasi indirizzario file system integrato che può essere caricato.

[4] Un UDFS può contenere un sottoalbero intero di oggetti, in questo modo quando si cancella un UDFS si cancellano gli oggetti di tutti i tipi che possono essere memorizzati nell'UDFS (user-defined file system).

[5] Quando si utilizzando i comandi DLTUDFS, è necessario disporre dell'autorizzazione *OBJEXIST su ciascun oggetto nell'UDFS oppure nessun oggetto viene cancellato.

[6] L'utente deve disporre delle autorizzazioni speciali a tutti gli oggetti (*ALLOBJ) e amministratore della riservatezza (*SECADM) per specificare un valore per il parametro Scansione opzione per oggetti (CRTOBJSCAN) diverso da *PARENT.

[7] L'autorizzazione speciale di controllo (*AUDIT) è necessaria quando si specifica un valore diverso da *SYSVAL sul parametro del valore di controllo per gli oggetti (CRTOBJAUD).

[8] È necessario disporre dell'autorizzazione alla scrittura (*W) e all'esecuzione (*X) per tutti gli oggetti indirizzario non vuoti nell'UDFS.

[9] Se un oggetto indirizzario non vuoto nell'UDFS dispone dell'attributo ″Ridenominazione e scollegamento limitati″ impostato su sì (questo attributo equivale al bit della modalità S_ISVTX), devono verificarsi una o più delle seguenti condizioni:

- È necessario essere il proprietario di tutti gli oggetti contenuti nell'indirizzario.
- È necessario essere il proprietario dell'indirizzario.
- È necessario disporre dell'autorizzazione speciale a tutti gli oggetti (*ALLOBJ).

[10] Non è possibile cancellare UDFS se contiene un oggetto che dispone dell'attributo *sola lettura* impostato su *sì* o se contiene un oggetto sottoposto a check out.

Comandi profilo utente

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi profilo utente.

I comandi identificati da (Q) vengono forniti con l'autorizzazione pubblica *EXCLUDE. Appendice C, "Comandi forniti con autorizzazione pubblica *EXCLUDE", a pagina 349 mostra quali profili utente forniti da IBM sono autorizzati sul comando. Il responsabile della riservatezza può concedere l'autorizzazione *USE ad altri.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
ANZDFTPWD [3, 14, 15](Q)			
ANZPRFACT [3, 14, 15](Q)			
CHGACTPRFL [14](Q)			
CHGACTSCDE [3, 14, 15](Q)			
CHGDSTPWD [1]			
CHGEXPSCDE [3, 14, 15](Q)			
CHGPRF	Profilo utente	*OBJMGT, *USE	
	Programma iniziale [2]	*USE	*EXECUTE
	Menu iniziale [2]	*USE	*EXECUTE
	Descrizione lavoro [2]	*USE	*EXECUTE
	Coda messaggi [2]	*USE	*EXECUTE
	Coda di emissione [2]	*USE	*EXECUTE
	Programma di gestione tasto di attenzione [2]	*USE	*EXECUTE
	Libreria corrente [2]	*USE	*EXECUTE
CHGPWD			
CHGUSRAUD [11](Q)			
CHGUSRPRF [3]	Profilo utente	*OBJMGT, *USE	*EXECUTE
	Programma iniziale [2]	*USE	*EXECUTE
	Menu iniziale [2]	*USE	*EXECUTE
	Descrizione lavoro [2]	*USE	*EXECUTE
	Coda messaggi [2]	*USE	*EXECUTE
	Coda di emissione [2]	*USE	*EXECUTE
	Programma di gestione tasto di attenzione [2]	*USE	*EXECUTE
	Libreria corrente [2]	*USE	*EXECUTE
	Profilo gruppo (GRPPRF o SUPGRPPRF)[2,4]	*OBJMGT, *OBJOPR, *READ, *ADD, *UPD, *DLT	*EXECUTE
CHGUSRPRTI	Profilo utente	*CHANGE	
CHKPWD			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTUSRPRF [3, 12, 17]	Programma iniziale	*USE	*EXECUTE
	Menu iniziale	*USE	*EXECUTE
	Descrizione lavoro	*USE	*EXECUTE
	Coda messaggi	*USE	*EXECUTE
	Coda di emissione	*USE	*EXECUTE
	Programma di gestione tasto di attenzione	*USE	*EXECUTE
	Libreria corrente	*USE	*EXECUTE
	Profilo gruppo (GRPPRF o SUPGRPPRF)[4]	*OBJMGT, *OBJOPR, *READ, *ADD, *UPD, *DLT	*EXECUTE
CVTUSRCERT[3, 14]			
DLTUSRPRF [3,9]	Profilo utente	*OBJEXIST, *USE	*EXECUTE
	Coda messaggi [5]	*OBJEXIST, *USE, *DLT	*EXECUTE
DMPUSRPRF [22](Q)	Profilo utente		
DSPACTPRFL [14](Q)			
DSPACTSCD [14](Q)			
DSPAUTUSR [6]	Profilo utente	*READ	
DSPEXPSCD [14](Q)			
DSPPGMADP	Profilo utente	*OBJMGT	
	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
DSPSSTUSR [23]			
DSPUSRPRF[19]	Profilo utente	*READ	*EXECUTE
	File di emissione	Fare riferimento alle regole generali.	Fare riferimento alle regole generali.
DSPUSRPRTI	Profilo utente	*USE	
GRTUSRAUT [7]	Profilo utente di riferimento	*READ	
	Oggetti a cui si sta concedendo l'autorizzazione	*OBJMGT	*EXECUTE
PRTPRFINT [14](Q)			
PRTUSRPRF [18]			
RSTAUT (Q) [8]			
RSTUSRPRF (Q) [8,10, 16]			
RTVUSRPRF[20]	Profilo utente	*READ	
RTVUSRPRTI	Profilo utente	*USE	
SAVSECDTA [8]	File di salvataggio, se vuoto	*USE, *ADD	*EXECUTE
	File di salvataggio, se i record esistono	*OBJMGT, *USE, *ADD	*EXECUTE
WRKUSRPRF [13]	Profilo utente	Qualsiasi autorizzazione	

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
[1] Questo comando può essere eseguito solo se si è collegati come QSECOFR. [2] È necessaria l'autorizzazione solo sugli oggetti per i campi che che si stanno modificando nel profilo utente. [3] È richiesta l'autorizzazione speciale *SECADM. [4] L'autorizzazione *OBJMGT sul profilo gruppo non può provenire dall'autorizzazione adottata. [5] La coda dei messaggi associata al profilo utente viene cancellata se di proprietà del profilo utente. Per cancellare la coda messaggi, l'utente che esegue il comando DLTUSRPRF deve disporre delle autorizzazioni specificati.			
[6] La visualizzazione comprende solo i profili utente su cui l'utente che esegue il comando dispone dell'autorizzazione. [7] Verificare le autorizzazioni richieste per il comando GRTOBJAUT. [8] È richiesta l'autorizzazione speciale *SAVSYS. [9] Se si seleziona l'opzione per cancellare gli oggetti di proprietà del profilo utente, è necessario disporre dell'autorizzazione necessaria per le operazioni di cancellazione. Se si seleziona l'opzione per il trasferimento della proprietà ad un altro profilo utente, è necessario disporre dell'autorizzazione necessaria sugli oggetti e sul profilo utente di destinazione. Consultare le informazioni per il comando CHGOBJOWN. [10] È necessario disporre dell'autorizzazione speciale *ALLOBJ per specificare un valore diverso da *NONE per il parametro ALWOBJDIF (Consenso differenze oggetto).			
[11] È necessario disporre dell'autorizzazione speciale *AUDIT. [12] All'utente per il quale viene creato il profilo vengono concesse le autorizzazioni su tale profilo: *OBJMGT, *OBJOPR, *READ, *ADD, *DLT, *UPD, *EXECUTE. [13] Per utilizzare una singola operazione, è necessario disporre dell'autorizzazione richiesta dall'operazione. [14] È necessario disporre dell'autorizzazione speciale *ALLOBJ per utilizzare questo comando. [15] È necessario disporre dell'autorizzazione speciale *JOBCTL per utilizzare questo comando.			
[16] L'utente deve disporre delle autorizzazioni speciali *ALLOBJ e *SECADM per specificare SECDTA(*PWDGRP), USRPRF(*ALL) o OMITUSRPRF. [17] Quando si esegue CRTUSRPRF, non è possibile creare un profilo utente (*USRPRF) in un lotto dischi indipendente. Tuttavia, quando un utente dispone di un'autorizzazione privata per un oggetto nel lotto dischi indipendente, è il proprietario di un oggetto in un lotto dischi indipendente o è il gruppo principale di un oggetto in un lotto dischi indipendente, il nome del profilo viene memorizzato nel lotto dischi indipendente. Se il lotto dischi indipendente viene spostato su un altro sistema, l'autorizzazione privata, la proprietà dell'oggetto e le voci del gruppo principali verranno collegate al profilo con lo stesso nome sul sistema di destinazione. Se un profilo non esiste sul sistema di destinazione, verrà creato un profilo. L'utente non disporrà di alcuna autorizzazione speciale e la parola d'ordine verrà impostata su *NONE. [18] È necessario disporre dell'autorizzazione speciale *ALLOBJ o *AUDIT per utilizzare questo comando. [19] È necessario disporre dell'autorizzazione speciale *ALLOBJ o *AUDIT per visualizzare il valore di controllo oggetto e di controllo operazione correnti. Altrimenti, verrà visualizzato il valore *NOTAVL ad indicare che i valori non sono disponibili per la visualizzazione. [20] È necessario disporre dell'autorizzazione speciale *ALLOBJ o *AUDIT per richiamare i valori OBJAUD e AUDLVL correnti. Altrimenti, viene restituito il valore *NOTAVL ad indicare che i valori non sono disponibili per il richiamo.			

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**

[21] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale al servizio (*SERVICE) o essere autorizzati alla funzione Dump di servizio di i5/OS tramite il supporto di Gestione applicazione di System i Navigator. Il comando CHGFCNUSG (Modifica utilizzo funzione) con un ID funzione di QIBM_SERVICE_DUMP può essere utilizzato anche per modificare l'elenco di utenti a cui è consentita l'esecuzione di operazioni di dump.

[22] Per utilizzare questo comando, è necessario disporre dell'autorizzazione speciale *SERVICE o dell'autorizzazione all'elenco di utilizzo della funzione QIBM_SERVICE_DUMP.

[23] È necessario disporre dell'autorizzazione speciale dell'amministratore della riservatezza (*SECADM) o al controllo (*AUDIT) per utilizzare questo comando.

Comandi elenco di convalida

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi elenco di convalida.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTVLDL	Elenco di convalida		*ADD, *READ
DLTVLDL	Elenco di convalida	*OBJEXIST	*EXECUTE

Comandi personalizzazione stazione di lavoro

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi personalizzazione stazione di lavoro.

Comando	Oggetto di riferimento	Autorizzazione necessaria	
		Per oggetto	**Per libreria**
CRTWSCST	File di origine	*USE	*EXECUTE
	Oggetto personalizzazione stazione di lavoro, se REPLACE(*NO)		*READ, *ADD
	Oggetto di personalizzazione stazione di lavoro, se REPLACE(*YES)	*OBJMGT, *OBJEXIST	*READ, *ADD
DLTWSCST	Oggetto personalizzaz. stazione di lavoro	*OBJEXIST	*EXECUTE
RTVWSCST	File di destinazione, se esiste e viene aggiunto un nuovo membro	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	File di destinazione, se il file e il membro esistono	*OBJOPR, *ADD, *DLT	*EXECUTE
	File di destinazione, se il file non esiste		*READ, *ADD

Comandi programma di scrittura

Questa tabella elenca le autorizzazioni specifiche richieste per i comandi programma di scrittura.

Comando	Oggetto di riferimento	Parametri coda di emissione		Autorizzaz. speciale	Autorizzazione necessaria	
		AUTCHK	OPRCTL		Per oggetto	Per libreria
CHGWTR [2, 4]	Coda di emissione corrente[1]	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Proprietario [3]	
			*YES	*JOBCTL		
	Nuova coda di emissione	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietario	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
ENDWTR [1]	Coda di emissione	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Proprietario [3]	
			*YES	*JOBCTL		
HLDWTR [1]	Coda di emissione	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Proprietario [3]	
			*YES	*JOBCTL		
RLSWTR [1]	Coda di emissione	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Proprietario [3]	
			*YES	*JOBCTL		
STRDKTWTR [1]	Coda di emissione	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietario [3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Coda messaggi				*OBJOPR, *ADD	*EXECUTE
	Descrizione unità				*OBJOPR, *READ	

Comando	Oggetto di riferimento	Parametri coda di emissione		Autorizzaz. speciale	Autorizzazione necessaria	
		AUTCHK	OPRCTL		Per oggetto	Per libreria
STRPRTWTR [1]	Coda di emissione	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietario [3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Coda messaggi				*OBJOPR, *ADD	*EXECUTE
	Oggetto personalizzaz. stazione di lavoro				*USE	*EXECUTE
	Programma unità di controllo dell'utente				*OBJOPR *EXECUTE	*EXECUTE
	Programma trasformazione dati utente				*OBJOPR *EXECUTE	*EXECUTE
	Programma separatore utente				*OBJOPR *EXECUTE	*EXECUTE
	Descrizione unità				*OBJOPR, *READ	
STRRMTWTR [1]	Coda di emissione	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietario [3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Coda messaggi				*OBJOPR, *ADD	*EXECUTE
	Oggetto personalizzaz. stazione di lavoro				*USE	*EXECUTE
	Programma unità di controllo dell'utente				*OBJOPR *EXECUTE	*EXECUTE
	Programma trasformazione dati utente				*OBJOPR *EXECUTE	*EXECUTE
WRKWTR						

[1] Se si dispone dell'autorizzazione speciale *SPLCTL, non è necessario disporre di un'autorizzazione sulla coda di emissione.

[2] Per modificare la coda di emissione per il programma di scrittura, è necessaria una delle autorizzazioni specificate per la nuova coda di emissione.

[3] È necessario essere il proprietario della coda di emissione.

[4] È necessario disporre dell'autorizzazione *EXECUTE sulla nuova libreria della coda di emissione anche se l'utente dispone dell'autorizzazione *SPLCTL.

Appendice E. Controllo e operazioni oggetto

Questa raccolta di argomenti elenca le operazioni che possono essere effettuate rispetto ad oggetti sul sistema e se tali operazioni sono sottoposte a controllo.

Gli elenchi sono organizzati per tipo di oggetto. Le operazioni sono raggruppate in base al fatto che siano sottoposte al controllo quando si specifica *ALL o *CHANGE per il valore OBJAUD del comando CHGOBJAUD o CHGDLOAUD.

Il fatto che si scriva un record di controllo per un'azione dipende da una combinazione di valori di sistema, un valore nel profilo utente dell'utente che esegue l'azione e un valore definito per l'oggetto. "Pianificazione del controllo dell'accesso agli oggetti" a pagina 308 descrive come impostare il controllo per gli oggetti.

Le operazioni riportate nelle tabelle in lettere maiuscole, come ad esempio CPYF, fanno riferimento a comandi CL, a meno che non siano etichettate come API (application programming interface).

Operazioni comuni a tutti i tipi di oggetti

Questo elenco descrive le operazioni che è possibile effettuare rispetto a tutti i tipi di oggetti e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  CRTDUPOBJ
  Creazione oggetto duplicato (se è specificato *ALL per *"da-oggetto"*).

  DMPOBJ
  Dump oggetto

  DMPSYSOBJ
  Dump oggetto di sistema

  QSRSAVO
  API oggetto di salvataggio

  QsrSave
  API Salvataggio oggetto nell'indirizzario

  SAV Salvataggio oggetto nell'indirizzario

  SAVCHGOBJ
  Salvataggio oggetto modificato

  SAVLIB
  Salvataggio libreria

  SAVOBJ
  Salvataggio oggetto

  SAVSAVFDTA
  Salvataggio dati file di salvataggio

  SAVDLO
  Salvataggio oggetto DLO

  SAVLICPGM
  Salvataggio programma su licenza

SAVSHF
Salvataggio scaffale

Nota: il record di controllo per l'operazione di salvataggio stabilirà se il salvataggio è avvenuto con STG(*FREE).

- Operazione di modifica

APYJRNCHG
Applicazione modifiche giornale

CHGJRNOBJ
Modifica oggetto su giornale

CHGOBJD
Modifica descrizione oggetto

CHGOBJOWN
Modifica proprietario oggetto

CRTxxxxxx
Creazione oggetto

Note:

1. Se si specifica *ALL o *CHANGE per la libreria di destinazione, viene scritta una voce ZC quando si crea un oggetto.
2. Se è attivo *CREATE per il controllo dell'operazione, viene scritta una voce CO quando si crea un oggetto.

DLTxxxxxx
Cancellazione oggetto

Note:

1. Se si specifica *ALL o *CHANGE per la libreria che contiene l'oggetto, si scrive una voce ZC quando si cancella un oggetto.
2. Se si specifica *ALL o *CHANGE per l'oggetto, si scrive una voce ZC quando viene cancellato.
3. Se *DELETE è attivo per il controllo dell'operazione, si scrive una voce DO un oggetto viene cancellato.

ENDJRNxxx
Fine registrazione su giornale

GRTOBJAUT
Concessione autorizzazione oggetto

Nota: se si concede un'autorizzazione in base ad un oggetto a cui si fa riferimento, non si scrive un record di controllo per l'oggetto a cui si fa riferimento.

MOVOBJ
Spostamento oggetto

QjoEndJournal
Fine registrazione su giornale

QjoStartJournal
Avvio registrazione su giornale

QSRRSTO
API ripristino oggetto

QsrRestore
API ripristino oggetto in indirizzario

RCLSTG
Riacquisizione memoria:
- Se un oggetto viene protetto da un *AUTL danneggiato, si scrive un record di controllo quando l'oggetto viene protetto dall'elenco di autorizzazioni QRCLAUTL.
- Si scrive un record di controllo se un oggetto viene spostato nella libreria QRCL.

RMVJRNCHG
Eliminazione modifiche giornale

RNMOBJ
Ridenominazione oggetto

RST Ripristino oggetto in indirizzario

RSTCFG
Ripristino oggetti configurazione

RSTLIB
Ripristino libreria

RSTLICPGM
Ripristino programma su licenza

RSTOBJ
Ripristino oggetto

RVKOBJAUT
Revoca autorizzazione oggetto

STRJRNxxx
Avvio registrazione su giornale

- Operazioni che non sono controllate

Richiesta [1]
Programma di sostituzione richiesta per un comando di modifica (se ne esiste uno)

CHKOBJ
Controllo oggetto

ALCOBJ
Assegnazione oggetto

CPROBJ
Compressione oggetto

DCPOBJ
Decompressione oggetto

DLCOBJ
Rilascio oggetto

DSPOBJD
Visualizzazione descrizione oggetto

DSPOBJAUT
Visualizzazione autorizzazione oggetto

---

1. Un programma di sostituzione richiesta visualizza i valori correnti quando è necessaria la richiesta per un comando. Ad esempio, se si immette CHGURSPRF USERA e si preme F4 (richiesta), il pannello Modifica pannello utente mostra i valori correnti per il profilo utente USERA.

EDTOBJAUT
Editazione autorizzazione oggetto

Nota: se si modifica l'autorizzazione all'oggetto ed il controllo dell'operazione include *SECURITY o si sta controllando l'oggetto, viene scritto un record di controllo.

QSYCUSRA
Controllo dell'autorizzazione utente ad un'API Oggetto

QSYLUSRA
Elenco degli utenti autorizzati ad un API Oggetto. Non viene scritto un record di controllo per l'oggetto la cui autorizzazione viene elencata. Si scrive un record di controllo per lo spazio utente utilizzato per contenere informazioni.

QSYRUSRA
Richiamo dell'autorizzazione utente ad un'API Oggetto

RCLTMPSTG
Riacquisizione memoria temporanea

RMVDFRID
Rimozione ID differimento

RSTDFROBJ
Ripristino oggetto differito

RTVOBJD
Richiamo descrizione oggetto

SAVSTG
Salvataggio memoria (controllo solo del comando SAVSTG)

WRKOBJLCK
Gestione vincoli su oggetto

WRKOBJOWN
Gestione oggetti per proprietario

WRKxxx
Gestione comandi oggetto

Operazioni per tempi di ripristino percorso accesso

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'oggetto tempi di ripristino percorso accesso e se tali operazioni vengono controllate o meno.

Nota: modifiche ai tempi di ripristino percorso accesso vengono controllate se il valore di sistema (QAUDLVL) controllo operazione o il parametro controllo operazione (AUDLVL) nel profilo utente include *SYSMGT.

- Operazioni che sono controllate

  CHGRCYAP
  Modifica ripristino per percorsi accesso

  EDTRCYAP
  Editazione ripristino per percorsi accesso
- Operazioni che non sono controllate

  DSPRCYAP
  Visualizzazione ripristino per percorsi accesso

Operazioni per tabella avvisi (*ALRTBL)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla tabella avvisi (*ALRTBL) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Nessuna

- Operazione di modifica

  ADDALRD
  Aggiunta descrizione avviso

  CHGALRD
  Modifica descrizione avviso

  CHGALRTBL
  Modifica tabella avvisi

  RMVALRD
  Rimozione descrizione avviso

- Operazioni che non sono controllate

  Stampa
  Stampa descrizione avviso

  WRKALRD
  Gestione descrizione avviso

  WRKALRTBL
  Gestione tabella avvisi

Operazioni per l'Elenco autorizzazioni (*AUTL)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'elenco autorizzazioni (*AUTL), e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Nessuna

- Operazione di modifica

  ADDAUTLE
  Aggiunta voce elenco di autorizzazioni

  CHGAUTLE
  Modifica voce elenco autorizzazioni

  EDTAUTL
  Editazione elenco autorizzazioni

  RMVAUTLE
  Eliminazione voce elenco autorizzazioni

- Operazioni che non sono controllate

  DSPAUTL
  Visualizzazione elenco autorizzazioni

  DSPAUTLOBJ
  Visualizzazione oggetti elenco autorizzazioni

  DSPAUTLDLO
  Visualizzazione DLO elenco autorizzazioni

RTVAUTLE
Richiamo voce elenco autorizzazioni

QSYLATLO
Elenco oggetti protetti dall'API *AUTL

WRKAUTL
Gestione elenco autorizzazioni

Operazioni per l'archivio autorizzazioni (*AUTHLR)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'archivio autorizzazioni (*AUTHLR) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Nessuna
- Operazione di modifica

  Associata
  Quando viene utilizzata per proteggere un oggetto.
- Operazioni che non sono controllate

  DSPAUTHLR
  Visualizzazione titolare autorizzazione

Operazioni per indirizzario di collegamento (*BNDDIR)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'indirizzario di collegamento (*BNDDIR) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  CRTPGM
  Creazione programma

  CRTSRVPGM
  Creazione programma servizio

  RTVBNDSRC
  Richiamo origine binder

  UPDPGM
  Aggiornamento programma

  UPDSRVPGM
  Aggiornamento programma servizio
- Operazione di modifica

  ADDBNDDIRE
  Aggiunta di voci all'indirizzario di collegamento

  RMVBNDDIRE
  Rimozione di voci dall'indirizzario di collegamento
- Operazioni che non sono controllate

  DSPBNDDIR
  Visualizzazione del contenuto di un indirizzario di collegamento

  WRKBNDDIR
  Gestione indirizzario di collegamento

  WRKBNDDIRE
  Gestione voce indirizzario binding

Operazioni per l'elenco di configurazioni (*CFGL)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'elenco configurazioni (*CFGL) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  CPYCFGL
  Copia dell'elenco di configurazioni. Viene scritta una voce per l'*elenco-configurazioni-origine*.

- Operazione di modifica

  ADDCFGLE
  Aggiunta voci elenco configurazioni

  CHGCFGL
  Modifica elenco configurazioni

  CHGCFGLE
  Modifica voce elenco configurazioni

  RMVCFGLE
  Eliminazione voce elenco configurazioni

- Operazioni che non sono controllate

  DSPCFGL
  Visualizzazione elenco configurazioni

  WRKCFGL
  Gestione elenco configurazioni

Operazioni per file speciali (*CHRSF)

Questo elenco descrive le operazioni che è possibile effettuare rispetto file speciali (*CHRSF) e se tali operazioni vengono controllate o meno.

Consultare Operazioni per file di flusso (*STMF) per il controllo *CHRSF.

Operazioni per il formato grafico (*CHTFMT)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al formato grafico (*CHTFMT) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Visualizzazione
  Comando DSPCHT oppure opzione F10 dal menu BGU

  Stampa/Tracciato
  Comando DSPCHT oppure opzione F15 dal menu BGU

  Salvataggio/Creazione
  Salvataggio o creazione di GDF (graphics data file) utilizzando il comando CRTGDF oppure l'opzione F13 dal menu BGU

- Operazione di modifica

  Nessuna

- Operazioni che non sono controllate

  Nessuna

Operazioni per *CLD (descrizione locale C)

Questo elenco descrive le operazioni che è possibile effettuare rispetto a *CLD (descrizione locale C) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  RTVCLDSRC
  Richiamo origine locale C

  Setlocale
  Utilizzo dell'oggetto locale C durante il tempo di esecuzione del programma C tramite la funzione Impostazione locale.

- Operazione di modifica

  Nessuna

- Operazioni che non sono controllate

  Nessuna

Operazioni per *CRQD (descrizione richiesta di modifica)

Questo elenco descrive le operazioni che è possibile effettuare rispetto a *CRQD (descrizione richiesta di modifica e se tali operazioni vengono controllate.

- Operazione di lettura

  QFVLSTA
  API Elenco attività descrizione richiesta di modifica

  QFVRTVCD
  API Richiamo descrizione richiesta di modifica

  SBMCRQ
  Inoltro richiesta di modifica

- Operazione di modifica

  ADDCMDCRQA
  Aggiunta attività richiesta di modifica comando

  ADDOBJCRQA
  Aggiunta attività richiesta di modifica oggetto

  ADDPRDCRQA
  Aggiunta attività richiesta di modifica prodotto

  ADDPTFCRQA
  Aggiunta attività richiesta di modifica PTF

  ADDRSCCRQA
  Aggiunta attività richiesta di modifica risorsa

  CHGCMDCRQA
  Modifica attività richiesta di modifica comando

  CHGCRQD
  Modifica descrizione richiesta di modifica

  CHGOBJCRQA
  Modifica attività richiesta di modifica oggetto

  CHGPRDCRQA
  Modifica attività richiesta di modifica prodotto

CHGPTFCRQA
Modifica attività richiesta di modifica PTF

CHGRSCCRQA
Modifica attività richiesta di modifica risorsa

QFVADDA
API Aggiunta attività descrizione richiesta di modifica

QFVRMVA
API Rimozione attività descrizione richiesta di modifica

RMVCRQDA
Rimozione attività descrizione richiesta di modifica

- Operazioni che non sono controllate

WRKCRQD
Gestione descrizioni richiesta di modifica

Operazioni per la classe (*CLS)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla Classe (*CLS) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

Nessuna

- Operazione di modifica

CHGCLS
Modifica classe

- Operazioni che non sono controllate

Avvio lavoro
Quando viene utilizzata da gestione lavoro per avviare un lavoro

DSPCLS
Visualizzazione classe

WRKCLS
Gestione classe

Operazioni per il Comando (*CMD)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al Comando (*CMD) e se tali operazioni vengono controllate.

- Operazione di lettura

Esecuzione
Quando si esegue il comando

- Operazione di modifica

CHGCMD
Modifica comando

CHGCMDDFT
Modifica valore predefinito comando

- Operazioni che non sono controllate

DSPCMD
Visualizzazione comando

PRTCMDUSG
Stampa utilizzo comando

QCDRCMDI
API Richiamo informazioni comando

WRKCMD
Gestione comando

I seguenti comandi sono utilizzati nei programmi CL per controllare l'elaborazione e operare sui dati nel programma. L'utilizzo di questi comandi non è controllato.

CALL [1]
CALLPRC
CHGVAR
COPYRIGHT
DCL
DCLF
DO
ELSE
ENDDO
	ENDPGM
	ENDRCV
	GOTO
	IF
	MONMSG
	PGM
		RCVF
		RETURN
		SNDF
		SNDRCVF
		TFRCTL
		WAIT

[1] CALL viene controllato se viene eseguito in modo interattivo. Non è controllato se viene eseguito nell'ambito di un programma CL.		

Operazioni per l'elenco di collegamenti (*CNNL)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'elenco di collegamenti (*CNNL) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Nessuna

- Operazione di modifica

  ADDCNNLE
  Aggiunta voce elenco collegamenti

  CHGCNNL
  Modifica elenco collegamenti

  CHGCNNLE
  Modifica voce elenco collegamenti

  RMVCNNLE
  Rimozione voce elenco collegamenti

  RNMCNNLE
  Ridenominazione voce elenco collegamenti

- Operazioni che non sono controllate

  Copia Opzione 3 di WRKCNNL

  DSPCNNL
  Visualizzazione elenco collegamenti

  RTVCFGSRC
  Richiamo dell'origine dell'elenco di collegamenti

  WRKCNNL
  Gestione elenco collegamenti

WRKCNNLE
Gestione voce elenco collegamenti

Operazioni per la per la descrizione classe di servizio (*COSD)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla descrizione classe di servizio (*COSD) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Nessuna
- Operazione di modifica

  CHGCOSD
  Modifica descrizione classe di servizio
- Operazioni che non sono controllate

  DSPCOSD
  Visualizzazione descrizione classe di servizio

  RTVCFGSRC
  Richiamo dell'origine della descrizione classe di servizio

  WRKCOSD
  Copia descrizione classe di servizio

  WRKCOSD
  Gestione descrizione classe di servizio

Operazioni per informazioni lato comunicazioni (*CSI)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alle informazioni lato comunicazioni (*CSI) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  DSPCSI
  Visualizzazione informazioni lato comunicazioni

  Inizializzazione
  Inizializzazione conversazione
- Operazione di modifica

  CHGCSI
  Modifica informazioni lato comunicazioni
- Operazioni che non sono controllate

  WRKCSI
  Gestione informazioni lato comunicazioni

Operazioni per la definizione prodotto tra sistemi (*CSPMAP)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla definizione prodotto tra sistemi (*CSPMAP) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Riferimento
  Quando vi si fa riferimento in un'applicazione CSP
- Operazione di modifica

  Nessuna

- Operazioni che non sono controllate

  DSPCSPOBJ
  Visualizzazione oggetto CSP

  WRKOBJCSP
  Gestione degli oggetti per CSP

Operazioni per la tabella prodotti tra sistemi (*CSPTBL)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla tabella prodotti tra sistemi (*CSPTBL) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Riferimento
  Quando vi si fa riferimento in un'applicazione CSP

- Operazione di modifica

  Nessuna

- Operazioni che non sono controllate

  DSPCSPOBJ
  Visualizzazione oggetto CSP

  WRKOBJCSP
  Gestione degli oggetti per CSP

Operazioni per la descrizione unità di controllo (*CTLD)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla descrizione unità di controllo (*CTLD) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  SAVCFG
  Salvataggio configurazione

  VFYCMN
  Verifica collegamento

- Operazione di modifica

  CHGCTL*xxx*
  Modifica descrizione unità di controllo

  VRYCFG
  Attivazione o disattivazione della descrizione dell'unità di controllo

- Operazioni che non sono controllate

  DSPCTLD
  Visualizzazione descrizione unità di controllo

  ENDCTLRCY
  Fine ripristino unità di controllo

  PRTDEVADR
  Stampa indirizzi unità

  RSMCTLRCY
  Ripresa ripristino unità di controllo

  RTVCFGSRC
  Richiamo dell'origine della descrizione dell'unità di controllo

RTVCFGSTS
Richiamo stato descrizione unità di controllo

WRKCTLD
Copia descrizione unità di controllo

WRKCTLD
Gestione descrizione unità di controllo

Operazioni per descrizione unità (*DEVD)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla descrizione unità (*DEVD) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Acquisizione
  Prima acquisizione dell'unità durante un'operazione di apertura o un'operazione di acquisizione esplicita

  Assegnazione
  Assegnazione di conversazione

  SAVCFG
  Salvataggio configurazione

  STRPASTHR
  Avvio sessione pass-through

  Avvio della seconda sessione per pass-through intermedio

  VFYCMN
  Verifica collegamento
- Operazione di modifica

  CHGDEV*xxx*
  Modifica descrizione unità

  HLDDEV*xxx*
  Congelamento descrizione unità

  RLSDEV*xxx*
  Rilascio descrizione unità

  QWSSETWS
  Modifica impostazione type-ahead per un'unità

  VRYCFG
  Attivazione o disattivazione della descrizione unità
- Operazioni che non sono controllate

  DSPDEVD
  Visualizzazione descrizione unità

  DSPMODSTS
  Visualizzazione stato modalità

  ENDDEVRCY
  Fine ripristino unità

  HLDCMNDEV
  Congelamento unità comunicazioni

  RLSCMNDEV
  Rilascio unità comunicazioni

RSMDEVRCY
Ripresa ripristino unità

RTVCFGSRC
Richiamo dell'origine della descrizione unità

RTVCFGSTS
Richiamo stato descrizione unità

WRKCFGSTS
Gestione stato configurazione

WRKDEVD
Copia descrizione unità

WRKDEVD
Gestione descrizione unità

Operazioni per indirizzario (*DIR)

Questo elenco descrive le operazioni che è possibile effettuare rispetto agli oggetti Indirizzario (*DIR) e se tali operazioni vengono controllate o meno.

- Operazioni lettura/ricerca

access, accessx, QlgAccess, QlgAccessx
Determinazione accessibilità file

CHGATR
Modifica attributo

CPY Copia oggetto

DSPCURDIR
Visualizzazione indirizzario corrente

DSPLNK
Visualizzazione collegamenti oggetto

faccessx
Determinazione accessibilità file per una classe di utenti per descrittore

getcwd, qlgGetcwd
API richiamo nome percorso dell'indirizzario corrente

Qp0lGetAttr, QlgGetAttr
API Richiamo attributi

Qp0lGetPathFromFileID, QlgGetPathFromFileID
API Richiamo percorso da identificativo file

Qp0lProcessSubtree, QlgProcessSubtree
API Elaborazione di un nome percorso

open, open64, QlgOpen, QlgOpen64, Qp0lOpen
API Apertura file

Qp0lSetAttr, QlgSetAttr
API Impostazione attributi

opendir, QlgOpendir
API Apertura indirizzario

RTVCURDIR
Richiamo indirizzario corrente

SAV Salvataggio oggetto

WRKLNK
Gestione collegamenti

- Operazione di modifica

CHGATR
Modifica attributi

CHGAUD
Modifica valore di controllo

CHGAUT
Modifica autorizzazione

CHGOWN
Modifica proprietario

CHGPGP
Modifica gruppo principale

chmod, QlgChmod
API Modifica autorizzazioni file

chown, QlgChown
API Modifica proprietario e gruppo

CPY Copia oggetto

CRTDIR
Creazione indirizzario

fchmod
API Modifica autorizzazioni file per descrittore

fchown
API Modifica proprietario e gruppo del file per descrittore

mkdir, QlgMkdir
API Preparazione indirizzario

MOV Spostamento oggetto

Qp0lRenameKeep, QlgRenameKeep
API Ridenominazione file o indirizzario, Conservazione nuovo

Qp0lRenameUnlink, QlgRenameUnlink
API Ridenominazione file o indirizzario, Scollegamento nuovo

Qp0lSetAttr, QlgSetAttr
API Impostazione attributo

rmdir, QlgRmdir
API Rimozione indirizzario

RMVDIR
Rimozione indirizzario

RNM Ridenominazione oggetto

RST Ripristino oggetto

utime, QlgUtime
API Impostazione ore di accesso e modifica file

WRKAUT
Gestione autorizzazione

WRKLNK
Gestione collegamenti oggetto

- Operazioni che non sono controllate

chdir, QlgChdir
API Modifica indirizzario

CHGCURDIR
Modifica indirizzario corrente

close API Chiusura descrittore file

closedir
API Chiusura indirizzario

DSPAUT
Visualizzazione autorizzazione

dup API Duplicazione descrittore file aperto

dup2 API Duplicazione descrittore file aperto in un altro descrittore

faccessx
Determinazione accessibilità file per una classe di utenti per descrittore

fchdir Modifica indirizzario corrente per descrittore

fcntl API Esecuzione comando controllo file

fpathconf
API Richiamo variabili nome percorso configurabili per descrittore

fstat, fstat64
API Richiamo informazioni file per descrittore

givedescriptor
API Concessione accesso file

ioctl API Esecuzione richiesta controllo I/E

lseek, lseek64
API Impostazione scostamento lettura/scrittura file

lstat, lstat64, QlgLstat, QlgLstat64
API Richiamo informazioni file o collegamento

pathconf, QlgPathconf
API Richiamo variabili nome percorso configurabili

readdir
API Lettura voce indirizzario

rewinddir
API Reimpostazione flusso indirizzario

select API Controllo stato I/E di più descrittori file

stat, QlgStat
API Richiamo informazioni file

takedescriptor
API Acquisizione accesso file

Operazioni per il Server indirizzario

Questo elenco descrive le operazioni che è possibile effettuare rispetto al Server indirizzario e se tali operazioni vengono controllate o meno.

Nota: le operazioni relative al Server indirizzario vengono controllate se il valore di sistema del controllo operazione (QAUDLVL) o il parametro del controllo operazione (AUDLVL) nel profilo utente include *OFCSRV.

- Operazioni che sono controllate

  Aggiunta
  Aggiunta di nuove voci indirizzario

  Modifica
  Modifica dei dettagli della voce indirizzario

  Cancellazione
  Cancellazione delle voci indirizzario

  Ridenominazione
  Ridenominazione voci indirizzario

  Stampa
  Visualizzazione o stampa dei dettagli della voce indirizzario

  Visualizzazione o stampa dei dettagli reparto

  Visualizzazione o stampa delle voci indirizzario come risultato di una ricerca

  RTVDIRE
  Richiamo voce indirizzario

  Raccolta
  Raccolta dei dati sulle voci indirizzario tramite lo shadow dell'indirizzario

  Fornitura
  Fornitura dei dati sulle voci indirizzario tramite lo shadow dell'indirizzario

- Operazioni che non sono controllate

  Comandi CL
  I comandi CL che operano sull'indirizzario possono essere controllati separatamente utilizzando la funzione di controllo oggetto.

  Nota: alcuni comandi indirizzario CL danno origine ad un record di controllo poiché eseguono una funzione che viene controllata dal controllo operazione *OFCSRV, come ad esempio l'aggiunta di una voce indirizzario.

  CHGSYSDIRA
  Modifica attributi indirizzario di sistema

  Reparti
  Aggiunta, modifica, cancellazione o visualizzazione dei dati reparto indirizzario

  Descrizioni
  Assegnazione di una descrizione ad una voce indirizzario differente tramite l'opzione 8 dal pannello WRKDIR.

  Aggiunta, modifica o cancellazione di descrizioni voci indirizzario

  Elenchi di distribuzione
  Aggiunta, modifica, ridenominazione o cancellazione degli elenchi di distribuzione

  ENDDIRSHD
  Fine copia indirizzario

  Elenco
  Visualizzazione o stampa di un elenco di voci indirizzario che non include i dettagli delle voci indirizzario, come ad esempio l'utilizzo del comando WRKDIRE o l'utilizzo di F4 selezionare voci per l'invio di una nota.

Ubicazioni
Aggiunta, modifica, cancellazione o visualizzazione dei dati sull'ubicazione dell'indirizzario

Nome alternativo
Aggiunta, modifica, ridenominazione o cancellazione dei nomi alternativi

Ricerca
Ricerca delle voci indirizzario

STRDIRSHD
Avvio copia indirizzario

Operazioni per DLO (*DOC or *FLR)

Questo elenco descrive le operazioni che è possibile effettuare rispetto a DLO (*DOC o *FLR) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

CHKDOC
Controllo ortografia documento

CPYDOC
Copia documento

DMPDLO
Dump del DLO

DSPDLOAUD
Visualizzazione controllo DLO

Nota: se si visualizzano le informazioni sul controllo per tutti i documenti contenuti in una cartella ed è stato specificato il controllo oggetto per la cartella, viene scritto un record di controllo. La visualizzazione del controllo oggetto per singoli documenti non dà come risultato un record di controllo.

DSPDLOAUT
Visualizzazione autorizzazione DLO

DSPDOC
Visualizzazione documento

DSPHLPDOC
Visualizzazione documento di aiuto

EDTDLOAUT
Editazione autorizzazione DLO

MRGDOC
Integrazione documento

PRTDOC
Stampa documento

QHFCPYSF
API Copia file di flusso

QHFGETSZ
API Richiamo dimensione file di flusso

QHFRDDR
API Lettura voce indirizzario

QHFRDSF
API Lettura file di flusso

RTVDOC
Richiamo documento

SAVDLO
Salvataggio DLO

SAVSHF
Salvataggio scaffale

SNDDOC
Invio documento

SNDDST
Invio distribuzione

WRKDOC
Gestione documento

Nota: viene scritta una voce di lettura per la cartella che contiene i documenti.

- Operazione di modifica

ADDDLOAUT
Aggiunta autorizzazione DLO

ADDOFCENR
Aggiunta iscrizione Office

CHGDLOAUD
Modifica controllo DLO

CHGDLOAUT
Modifica autorizzazione DLO

CHGDLOOWN
Modifica della proprietà del DLO

CHGDLOPGP
Modifica gruppo principale DLO

CHGDOCD
Modifica descrizione documento

CHGDSTD
Modifica descrizione distribuzione

CPYDOC [2]
Copia documento

Nota: viene scritta una voce di modifica se esiste già il documento di destinazione.

CRTFLR
Creazione cartella

CVTTOFLR [2]
Conversione in cartella

DLTDLO [2]
Cancellazione DLO

DLTSHF
Cancellazione scaffale

---

2. Viene scritta una voce di modifica sia per il documento che per la cartella se la destinazione dell'operazione si trova in una cartella.

DTLDOCL [2]
Cancellazione elenco documenti

DLTDST [2]
Cancellazione distribuzione

EDTDLOAUT
Editazione autorizzazione DLO

EDTDOC
Editazione documento

FILDOC [2]
Archiviazione documento

GRTACCAUT
Concessione autorizzazione codice di accesso

GRTUSRPMN
Concessione permesso utente

MOVDOC [2]
Spostamento documento

MRGDOC [2]
Integrazione documento

PAGDOC
Paginazione documento

QHFCHGAT
API Modifica attributi voce indirizzario

QHFSETSZ
API Impostazione dimensione file di flusso

QHFWRTSF
API Scrittura file di flusso

QRYDOCLIB [2]
Query sulla libreria documenti

Nota: viene scritta una voce di modifica se si sostituisce un documento esistente che risulta da una ricerca.

RCVDST [2]
Ricezione distribuzione

RGZDLO
Riorganizzazione DLO

RMVACC
Eliminazione del codice di accesso, per qualsiasi DLO a cui il codice di accesso è associato

RMVDLOAUT
Rimozione autorizzazione DLO

RNMDLO [2]
Ridenominazione DLO

RPLDOC
Sostituzione documento

RSTDLO [2]
Ripristino DLO

RSTSHF
Ripristino scaffale

RTVDOC
Richiamo documento (controllo in uscita)

RVKACCAUT
Revoca autorizzazione codice di accesso

RVKUSRPMN
Revoca permesso utente

SAVDLO [2]
Salvataggio DLO

- Operazioni che non sono controllate

ADDACC
Aggiunta codice di accesso

DSPACC
Visualizzazione codice di accesso

DSPUSRPMN
Visualizzazione permesso utente

QHFCHGFP
API Modifica puntatore file

QHFCLODR
API Chiusura indirizzario

QHFCLOSF
API Chiusura file di flusso

QHFFRCSF
API Forzatura dati memorizzati in buffer

QHFLULSF
API Blocco/Sblocco intervallo file di flusso

QHFRTVAT
API Richiamo attributi voce indirizzario

RCLDLO
Riacquisizione DLO (*ALL o *INT)

WRKDOCLIB
Gestione libreria documenti

WRKDOCPRTQ
Gestione coda stampa documenti

Operazioni per Area dati (*DTAARA)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'Area dati (*DTAARA) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

DSPDTAARA
Visualizzazione area dati

RCVDTAARA
Ricezione area dati (comando S/38)

RTVDTAARA
Richiamo area dati

QWCRDTAA
API Richiamo area dati

- Operazione di modifica

CHGDTAARA
Modifica area dati

SNDDTAARA
Invio area dati

- Operazioni che non sono controllate

Aree dati
Area dati locale, Area dati gruppo, Area dati PIP (Program Initialization Parameter)

WRKDTAARA
Gestione area dati

Operazioni per IDDU (Programma di utilità per la definizione dei dati interattivi) (*DTADCT)

Questo elenco descrive le operazioni che è possibile effettuare rispetto a IDDU (Programma di utilità definizione dati interattivi) (*DTADCT), e se tali operazioni vengono controllate o meno.

- Operazione di lettura

Nessuna

- Operazione di modifica

Creazione
Dizionario dati e definizioni dati

Modifica
Dizionario dati e definizioni dati

Copia Definizioni dati (registrati come sono stati creati)

Cancellazione
Dizionario dati e definizioni dati

Ridenominazione
Definizioni dati

- Operazioni che non sono controllate

Visualizzazione
Dizionario dati e definizioni dati

LNKDTADFN
Collegamento e scollegamento di definizioni file

Stampa
Dizionario dati, definizioni dati ed eventuali informazioni relative alle definizioni dati

Operazioni per la coda dati (*DTAQ)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla coda dati (*DTAQ) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

QMHRDQM
API Richiamo messaggio coda dati

- Operazione di modifica

QRCVDTAQ
API Ricezione coda dati

QSNDDTAQ
API Invio coda dati

QCLRDTAQ
API Eliminazione contenuto coda dati

- Operazioni che non sono controllate

WRKDTAQ
Gestione coda dati

QMHQRDQD
API Richiamo descrizione coda dati

Operazioni per la descrizione editazione (*EDTD)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla descrizione editazione (*EDTD) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

DSPEDTD
Visualizzazione descrizione editazione

QECCVTEC
API Editazione espansione coda (tramite routine QECEDITU)

- Operazione di modifica

Nessuna

- Operazioni che non sono controllate

WRKEDTD
Gestione descrizioni editazione

QECEDT
API Editazione

QECCVTEW
API per la conversione del Lavoro editazione nella Maschera editazione

Operazioni per la registrazione uscita (*EXITRG)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla registrazione uscita (*EXITRG) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

QUSRTVEI
API Richiamo informazioni uscita

QusRetrieveExitInformation
API Richiamo informazioni uscita

- Operazione di modifica

ADDEXITPGM
Aggiunta programma di uscita

QUSADDEP
API Aggiunta programma di uscita

QusAddExitProgram
API Aggiunta programma di uscita

QUSDRGPT
API Annullamento registrazione punto di uscita

QusDeregisterExitPoint
API Annullamento registrazione punto di uscita

QUSRGPT
API Registrazione punto di uscita

QusRegisterExitPoint
API Registrazione punto di uscita

QUSRMVEP
API Rimozione programma di uscita

QusRemoveExitProgram
API Rimozione programma di uscita

RMVEXITPGM
Rimozione programma di uscita

WRKREGINF
Gestione informazioni registrazione

- Operazioni che non sono controllate

  Nessuna

Operazioni per la tabella controllo formati (*FCT)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla tabella controllo formati (*FCT) e se tali operazioni vengono controllate o meno.

- Nessuna operazione di Lettura o Modifica è sottoposta a controllo per il tipo di oggetto *FCT .

Operazioni per il file (*FILE)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al File (*FILE) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  CPYF Copia file (utilizza operazione di apertura)

  Apertura
  Apertura d un file per la lettura

  DSPPFM
  Visualizzazione membro file fisico (utilizza operazione di apertura)

  Apertura
  Apertura di MRT dopo l'apertura iniziale

  CRTBSCF
  Creazione file BSC (utilizza operazione di apertura)

  CRTCMNF
  Creazione file delle comunicazioni (utilizza operazione di apertura)

  CRTDSPF
  Creazione file di visualizzazione (utilizza operazione di apertura)

CRTICFF
Creazione file ICF (utilizza operazione di apertura)

CRTMXDF
Creazione file MXD (utilizza operazione di apertura)

CRTPRTF
Creazione file di stampa (utilizza operazione di apertura)

CRTPF
Creazione file fisico (utilizza operazione di apertura)

CRTLF
Creazione file logico (utilizza operazione di apertura)

DSPMODSRC
Visualizzazione origine formato (utilizza operazione di apertura)

STRDBG
Avvio debug (utilizza operazione di apertura)

QTEDBGS
API Richiamo testo visualizzazione

- Operazione di modifica

Apertura
Apertura di un file per la modifica

ADDBSCDEVE
(S/38E) Aggiunta voce unità BSC ad un file unità mista (MXD)

ADDCMNDEVE
(S/38E) Aggiunta voce unità comunicazioni ad un file unità mista (MXD)

ADDDSPDEVE
(S/38E) Aggiunta voce unità di visualizzazione ad un file unità mista (MXD)

ADDICFDEVE
(S/38E) Aggiunta voce unità ICF ad un file unità mista (MXD)

ADDLFM
Aggiunta membro file logico

ADDPFCST
Aggiunta restrizione file fisico

ADDPFM
Aggiunta membro file fisico

ADDPFTRG
Aggiunta trigger file fisico

ADDPFVLM
Aggiunta membro file fisico a lunghezza variabile

APYJRNCHGX
Applicazione estensione modifiche giornale

CHGBSCF
Modifica funzione BSC

CHGCMNF
(S/38E) Modifica file delle comunicazioni

CHGDDMF
Modifica file DDM

CHGDKTF
Modifica file minidisco

CHGDSPF
Modifica file di visualizzazione

CHGICFDEVE
Modifica voce file unità ICF

CHGICFF
Modifica file ICF

CHGMXDF
(S/38E) Modifica file MXD

CHGLF
Modifica file logico

CHGLFM
Modifica membro file logico

CHGPF
Modifica file fisico

CHGPFCST
Modifica restrizione file fisico

CHGPFM
Modifica membro file fisico

CHGPRTF
Modifica unità di stampa GQle

CHGSAVF
Modifica file di salvataggio

CHGS36PRCA
Modifica attributi procedura S/36

CHGS36SRCA
Modifica attributi origine S/36

CHGTAPF
Modifica file unità nastro

CLRPFM
Cancellazione del contenuto del membro file fisico

CPYF Copia file (file aperto per la modifica, come ad esempio aggiunta di record, cancellazione del contenuto di un membro o salvataggio di un membro)

EDTS36PRCA
Editazione attributi procedura S/36

EDTS36SRCA
Editazione attributi origine S/36

INZPFM
Inizializzazione membro file fisico

JRNAP
(S/38E) Avvio percorso accesso giornale (voce per file)

JRNPF
(S/38E) Avvio file fisico giornale (voce per file)

RGZPFM
Riorganizzazione membro file fisico

RMVBSCDEVE
(S/38E) Rimozione voce unità BSC da un file MXD

RMVCMNDEVE
(S/38E) Rimozione voce unità CMN da un file MXD

RMVDSPDEVE
(S/38E) Rimozione voce unità DSP da un file MXD

RMVICFDEVE
(S/38E) Rimozione voce unità ICF da un file unità ICM

RMVM
Rimozione membro

RMVPFCST
Rimozione restrizione file fisico

RMVPFTGR
Rimozione trigger file fisico

RNMM
Ridenominazione membro

WRKS36PRCA
Gestione attributi procedura S/36

WRKS36SRCA
Gestione attributi origine S/36

- Operazioni che non sono controllate

CHGPFTRG
Modifica trigger file fisico

DSPCPCST
Visualizzazione restrizioni sospensione controllo

DSPFD
Visualizzazione descrizione file

DSPFFD
Visualizzazione descrizione campo file

DSPDBR
Visualizzazione relazioni database

DSPPGMREF
Visualizzazione riferimenti file programma

EDTCPCST
Editazione restrizioni sospensione controllo

OVR*xxx*
Sostituzione file

RTVMBRD
Richiamo descrizione membro

WRKPFCST
Gestione restrizioni file fisico

WRKF
Gestione file

Operazioni per i file First-in First-out (*FIFO)

Questo elenco descrive le operazioni che è possibile effettuare rispetto agli oggetti first-in first-out (*FIFO)e se tali operazioni vengono controllate o meno.

Consultare Operazioni per il file di flusso (*STMF) per il controllo di *FIFO.

Operazioni per la cartella (*FLR)

Questo elenco descrive le operazioni che è possibile effettuare rispetto agli oggetti cartella (*FLR) e se tali operazioni vengono controllate o meno.

consultare le operazioni per "Operazioni per DLO (*DOC or *FLR)" a pagina 546

Operazioni per la risorsa font (*FNTRSC)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla risorsa font (*FNTRSC) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Stampa
  Stampa di un file di spool che fa riferimento alla risorsa font
- Operazione di modifica

  Nessuna

- Operazioni che non sono controllate

  WRKFNTRSC
  Gestione risorsa font

  Stampa
  Riferimento alla risorsa font durante la creazione di un file di spool

Operazioni per la definizione formato (*FORMDF)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla definizione formato (*FORMDF) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Stampa
  Stampa di un file di spool che fa riferimento alla definizione formato
- Operazione di modifica

  Nessuna

- Operazioni che non sono controllate

  WRKFORMDF
  Gestione definizione formato

  Stampa
  Riferimento alla definizione formato durante la creazione di un file di spool

Operazioni per oggetto filtro (*FTR)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'oggetto filtro (*FTR) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Nessuna

- Operazione di modifica

  ADDALRACNE
  Aggiunta voce operazione avviso

  ADDALRSLTE
  Aggiunta voce selezione avviso

  ADDPRBACNE
  Aggiunta voce operazione problema

  ADDPRBSLTE
  Aggiunta voce selezione problema

  CHGALRACNE
  Modifica voce operazione avviso

  CHGALRSLTE
  Modifica voce selezione avviso

  CHGPRBACNE
  Modifica voce operazione problema

  CHGPRBSLTE
  Modifica voce selezione problema

  CHGFTR
  Modifica filtro

  RMVFTRACNE
  Rimozione voce operazione avviso

  RMVFTRSLTE
  Rimozione voce selezione avviso

  WRKFTRACNE
  Gestione voce operazione avviso

  WRKFTRSLTE
  Gestione voce selezione avviso

- Operazioni che non sono controllate

  WRKFTR
  Gestione filtro

  WRKFTRACNE
  Gestione voci operazione filtro

  WRKFTRSLTE
  Gestione voci selezione filtro

Operazioni per la serie di simboli grafici (*GSS)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla serie di simboli grafici (*GSS) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Caricato
  Quando viene caricato

  Font Quando viene utilizzato come font in un file di stampa descritto esternamente
- Operazione di modifica

  Nessuna.

- Operazioni che non sono controllate

  WRKGSS
  Gestione serie di simboli grafici

Operazioni per il dizionario DBCS (*IGCDCT)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al dizionario DBCS (*IGCDCT) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  DSPIGCDCT
  Visualizzazione dizionario IGC
- Operazione di modifica

  EDTIGCDCT
  Editazione dizionario IGC

Operazioni per ordinamento DBCS (*IGCSRT)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'ordinamento DBCS (*IGCSRT) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  CPYIGCSRT
  Copia oggetto ordinamento IGC (*da-oggetto-*ICGSRT*)

  Conversione
  Conversione nel formato V3R1, se necessario

  Stampa
  Stampa carattere da registrare in tabella di ordinamento (opzione 1 dal menu CGU)

  Stampa prima di cancellare il carattere dalla tabella di ordinamento (opzione 2 dal menu CGU)
- Operazione di modifica

  CPYIGCSRT
  Copia ordinamento IGC (*ad-oggetto-*ICGSRT*)

  Conversione
  Conversione nel formato V3R1, se necessario

  Creazione
  Creazione di un carattere definito dall'utente (opzione 1 dal menu CGU)

  Cancellazione
  Cancellazione di un carattere definito dall'utente (opzione 2 dal menu CGU)

Aggiornam.
Aggiornamento della tabella di ordinamento attiva (opzione 5 dal menu CGU)

- Operazioni che non sono controllate

FMTDTA
Ordinamento dei record o dei campi in un file

Operazioni per la tabella DBCS (*IGCTBL)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla tabella DBCS (*IGCTBL), e se tali operazioni vengono controllate o meno.

- Operazione di lettura

CPYIGCTBL
Copia tabella IGC

STRFMA
Avvio di Font Management Aid

- Operazione di modifica

STRFMA
Avvio di Font Management Aid

- Operazioni che non sono controllate

CHKIGCTBL
Controllo tabella IGC

Operazioni per la descrizione lavoro (*JOBD)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla descrizione lavoro (*JOBD) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

Nessuna

- Operazione di modifica

CHGJOBD
Modifica descrizione lavoro

- Operazioni che non sono controllate

DSPJOBD
Visualizzazione descrizione lavoro

WRKJOBD
Gestione descrizione lavoro

QWDRJOBD
API Richiamo descrizione lavoro

Lavoro batch
Quando viene utilizzato per stabilire un lavoro

Operazioni per coda lavori (*JOBQ)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla coda lavori (*JOBQ) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

Nessuna

- Operazione di modifica

  Voce Quando una voce è collocata nella coda o rimossa da essa

  CHGJOBQ
  Modifica coda lavori

  CLRJOBQ
  Cancellazione contenuto coda lavori

  HLDJOBQ
  Congelamento coda lavori

  RLSJOBQ
  Rilascio coda lavori
- Operazioni che non sono controllate

  ADDJOBQE "Descrizioni sottosistema" a pagina 220
  Aggiunta voce coda lavori

  CHGJOB
  Modifica del lavoro da una JOBQ ad un'altra JOBQ

  CHGJOBQE "Descrizioni sottosistema" a pagina 220
  Modifica voce coda lavori

  QSPRJOBQ
  Richiamo informazioni coda lavori

  RMVJOBQE "Descrizioni sottosistema" a pagina 220
  Rimozione voce coda lavori

  TFRJOB
  Trasferimento lavoro

  TFRBCHJOB
  Trasferimento lavoro batch

  WRKJOBQ
  Gestione coda lavori per una specifica coda lavori

  WRKJOBQ
  Gestione coda lavori per tutte le code lavori

  WRKJOBQD
  Gestione descrizione coda lavori

Operazioni per l'oggetto Job Scheduler (*JOBSCD)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'oggetto Job Scheduler (*JOBSCD) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Nessuna
- Operazione di modifica

  ADDJOBSCDE
  Aggiunta specifica schedulazione lavori

  CHGJOBSCDE
  Modifica specifica schedulazione lavori

3. Viene scritto un record di controllo se è specificato il controllo oggetto per la descrizione sottosistema (*SBSD).

RMVJOBSCDE
Rimozione specifica schedulazione lavori

HLDJOBSCDE
Congelamento specifica schedulazione lavori

RLSJOBSCDE
Rilascio specifica schedulazione lavori

- Operazioni che non sono controllate

Visualizzazione
Visualizzazione dei dettagli della voce lavoro pianificata

WRKJOBSCDE
Gestione specifiche schedulazione lavori

Gestione ...
Gestione di lavori precedentemente inoltrati dalla specifica di schedulazione lavori

QWCLSCDE
API Elenco specifiche schedulazione lavori

Operazioni per il giornale (*JRN)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al Giornale (*JRN) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

CMPJRNIMG
Confronto immagini giornale

DSPJRN
Visualizzazione voce di giornale per giornali utente

QJORJIDI
Richiamo informazioni JID (Journal Identifier)

QjoRetrieveJournalEntries
Richiamo voci giornale

RCVJRNE
Ricezione voce di giornale

RTVJRNE
Richiamo voce di giornale

- Operazione di modifica

ADDRMTJRN
Aggiunta giornale remoto

APYJRNCHG
Applicazione modifiche giornale

APYJRNCHGX
Applicazione estensione modifiche giornale

CHGJRN
Modifica giornale

CHGRMTJRN
Modifica giornale remoto

ENDJRN*xxx*
Fine registrazione su giornale

JRNAP
(S/38E) Avvio percorso d'accesso al giornale

JRNPF
(S/38E) Avvio file fisico giornale

QjoAddRemoteJournal
API Aggiunta giornale remoto

QjoChangeJournalState
API Modifica stato giornale

QjoEndJournal
API Fine registrazione su giornale

QjoRemoveRemoteJournal
API Rimozione giornale remoto

QJOSJRNE
API Invio voce di giornale (voci utente solo tramite API QJOSJRNE)

QjoStartJournal
API Avvio registrazione su giornale

RMVJRNCHG
Eliminazione modifiche giornale

RMVRMTJRN
Rimozione giornale remoto

SNDJRNE
Invio voce di giornale (voci utente solo tramite il comando SNDJRNE)

STRJRN*xxx*
Avvio registrazione su giornale

- Operazioni che non sono controllate

DSPJRN
Visualizzazione voce di giornale per giornali interni di sistema, JRN(*INTSYSJRN)

DSPJRNA
(S/38E) Gestione attributi giornale

DSPJRNMNU
(S/38E) Gestione giornale

QjoRetrieveJournalInformation
API Richiamo informazioni giornale

WRKJRN
Gestione giornale (DSPJRNMNU in ambiente S/38)

WRKJRNA
Gestione attributi giornale (DSPJRNA in ambiente S/38)

Operazioni per il ricevitore di giornale (*JRNRCV)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al ricevitore di giornale (*JRNRCV) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Nessuna

- Operazione di modifica

CHGJRN
Modifica giornale (quando si associano nuovi ricevitori)

- Operazioni che non sono controllate

DSPJRNRCVA
Visualizzazione attributi ricevitore di giornale

QjoRtvJrnReceiverInformation
API Richiamo informazioni ricevitore giornale

WRKJRNRCV
Gestione ricevitore di giornale

Operazioni per libreria (*LIB)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla Libreria (*LIB) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

DSPLIB
Visualizzazione libreria (quando non è vuota. Se la libreria è vuota, non si esegue alcun controllo.)

Localizzazione
Quando si accede ad una libreria per reperire un oggetto

Nota:

1. È possibile scrivere diverse voci di controllo per una libreria per un singolo comando. Ad esempio, quando si apre un file, viene scritta una voce del giornale di controllo ZR per la libreria quando il sistema individua il file ed ogni membro in esso contenuto.
2. Non si scrive alcuna voce di controllo se la funzione di localizzazione non ha avuto esito positivo. Ad esempio, si esegue un comando utilizzando un parametro generico, come ad esempio:

   ```
   DSPOBJD OBJ(AR/WRK*) OBJTYPE(*FILE)
   ```

   Se una libreria denominata “AR” non contiene alcun nome file che inizi con “WRK”, non viene scritto alcun record di modifica per tale libreria.

Elenco librerie
Aggiunta di una voce ad un elenco librerie

- Operazione di modifica

CHGLIB
Modifica libreria

CLRLIB
Cancellazione contenuto libreria

MOVOBJ
Spostamento oggetto

RNMOBJ
Ridenominazione oggetto

Aggiunta
Aggiunta di un oggetto alla libreria

Cancellazione
Cancellazione di un oggetto dalla libreria

- Operazioni che non sono controllate

Nessuna

Operazioni per la descrizione linea (*LIND)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla descrizione linea (*LIND) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  SAVCFG
  Salvataggio configurazione

  RUNLPDA
  Esecuzione comandi operativi LPDA-2

  VFYCMN
  Verifica collegamento

  VFYLNKLPDA
  Verifica collegamento LPDA-2
- Operazione di modifica

  CHGLIN*xxx*
  Modifica descrizione linea

  VRYCFG
  Attivazione/Disattivazione descrizione linea
- Operazioni che non sono controllate

  ANSLIN
  Risposta a linea

  Copia Opzione 3 da WRKLIND

  DSPLIND
  Visualizzazione descrizione linea

  ENDLINRCY
  Fine ripristino linea

  RLSCMNDEV
  Rilascio unità comunicazioni

  RSMLINRCY
  Ripresa ripristino linea

  RTVCFGSRC
  Richiamo dell'origine della descrizione linea

  RTVCFGSTS
  Richiamo stato descrizione linea

  WRKLIND
  Gestione descrizione linea

  WRKCFGSTS
  Gestione stato descrizione linea

Operazioni per i servizi di posta

Questo elenco descrive le operazioni che è possibile effettuare rispetto ai servizi di posta e se tali operazioni vengono controllate o meno.

Nota: le operazioni relative ai servizi di posta vengono controllate se il valore di sistema del controllo operazione (QAUDLVL) o il parametro del controllo operazione (AUDLVL) nel profilo utente include *OFCSRV.

- Operazioni che sono controllate

  Modifica
  Modifiche all'indirizzario di distribuzione del sistema

  Per conto di
  Lavoro per conto di un altro utente

  Nota: il lavoro per conto di un altro utente viene controllato se AUDLVL nel profilo utente o il valore di sistema QAUDLVL include *SECURITY.

  Apertura
  Viene scritto un record di controllo quando si apre la registrazione di posta

- Operazioni che non sono controllate

  Modifica
  Modifica dei dettagli di una voce di posta

  Cancellazione
  Cancellazione di una voce di posta

  File Archiviazione di una voce di posta in un documento o in una cartella

  Nota: quando viene archiviata una voce di posta, questa diventa un DLO (document library object). È possibile specificare il controllo oggetto per un DLO.

  Inoltro
  Inoltro di una voce di posta

  Stampa
  Stampa di una voce di posta

  Nota: è possibile controllare la stampa delle voci di posta utilizzando il livello di controllo *SPLFDTA o *PRTDTA.

  Ricezione
  Ricezione di una voce di posta

  Risposta
  Risposta ad una voce di posta

  Invio Invio di una voce di posta

  Visualizzazione
  Visualizzazione di una voce di posta

Operazioni per il menu (*MENU)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al Menu (*MENU) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Visualizzazione
  Visualizzazione di un menu tramite il comando GO MENU o il comando della casella di dialogo UIM

- Operazione di modifica

  CHGMNU
  Modifica menu

- Operazioni che non sono controllate

  Ritorno
  Ritorno ad un menu nello stack di menu che è già stato visualizzato

  DSPMNUA
  Visualizzazione attributi menu

  WRKMNU
  Gestione menu

Operazioni per la descrizione modalità (*MODD)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla descrizione modalità (*MODD) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Nessuna
- Operazione di modifica

  CHGMODD
  Modifica descrizione modalità
- Operazioni che non sono controllate

  CHGSSNMAX
  Modifica numero massimo di sessioni

  DSPMODD
  Visualizzazione descrizione modalità

  ENDMOD
  Fine modalità

  STRMOD
  Avvio modalità

  WRKMODD
  Gestione descrizioni modalità

Operazioni per l'oggetto modulo (*MODULE)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'oggetto modulo (*MODULE) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  CRTPGM
  Una voce di controllo per ogni oggetto modulo utilizzato durante un CRTPGM.

  CRTSRVPGM
  Una voce di controllo per ogni oggetto modulo utilizzato durante un CRTSRVPGM

  UPDPGM
  Una voce di controllo per ogni oggetto modulo utilizzato durante un UPDPGM

  UPDSRVPGM
  Una voce di controllo per ogni oggetto modulo utilizzato durante un UPDSRVPGM
- Operazione di modifica

  CHGMOD
  Modifica modulo
- Operazioni che non sono controllate

DSPMOD
Visualizzazione modulo

RTVBNDSRC
Richiamo origine binder

WRKMOD
Gestione modulo

Operazioni per file messaggi (*MSGF)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al file messaggi (*MSGF) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  DSPMSGD
  Visualizzazione descrizioni messaggi

  MRGMSGF
  Integrazione file messaggi da file

  Stampa
  Stampa descrizione messaggio

  RTVMSG
  Richiamo delle informazioni da un file di messaggi

  QMHRTVM
  API Richiamo messaggio

  WRKMSGD
  Gestione descrizione messaggio

- Operazione di modifica

  ADDMSGD
  Aggiunta descrizione messaggio

  CHGMSGD
  Modifica descrizione messaggio

  CHGMSGF
  Modifica file messaggi

  MRGMSGF
  Integrazione file messaggi (nel file e sostituzione di MSGF)

  RMVMSGD
  Rimozione descrizione messaggio

- Operazioni che non sono controllate

  OVRMSGF
  Sostituzione con file messaggi

  WRKMSGF
  Gestione file messaggi

  QMHRMFAT
  API Richiamo attributi file messaggi

Operazioni per la coda messaggi (*MSGQ)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla coda messaggi (*MSGQ) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  QMHLSTM
  API Elenco messaggi Nonprogram

  QMHRMQAT
  API Richiama attributi coda messaggi Nonprogram

  DSPLOG
  Visualizzazione registrazione

  DSPMSG
  Visualizzazione messaggi

  Stampa
  Stampa messaggi

  RCVMSG
  Ricezione messaggio RMV(*NO)

  QMHRCVM
  API Ricezione messaggi Nonprogram quando l'operazione messaggio non è *REMOVE.
- Operazione di modifica

  CHGMSGQ
  Modifica coda messaggi

  CLRMSGQ
  Cancellazione contenuto coda messaggi

  RCVMSG
  Ricezione messaggio RMV(*YES)

  QMHRCVM
  API Ricezione messaggi Nonprogram quando l'operazione messaggio è *REMOVE.

  RMVMSG
  Rimozione messaggio

  QMHRMVM
  API Rimozione messaggi Nonprogram

  SNDxxxMSG
  Invio di un messaggio ad una coda messaggi

  QMHSNDBM
  API Invio messaggio di interruzione

  QMHSNDM
  API Invio messaggio Nonprogram

  QMHSNDRM
  API Invio messaggio di risposta

  SNDRPY
  Invio risposta

  WRKMSG
  Gestione messaggio
- Operazioni che non sono controllate

WRKMSGQ
Gestione coda messaggi

Programma
Programmazione operazioni coda messaggi

Operazioni per gruppo nodi (*NODGRP)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al gruppo nodi(*NODGRP) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  DSPNODGRP
  Visualizzazione gruppo nodi
- Operazione di modifica

  CHGNODGRPA
  Modifica gruppo nodi

Operazioni per elenco nodi (*NODL)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'elenco nodi (*NODL) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  QFVLSTNL
  Elenco voci elenco nodi
- Operazione di modifica

  ADDNODLE
  Aggiunta voce elenco nodi

  RMVNODLE
  Rimozione voce elenco nodi
- Operazioni che non sono controllate

  WRKNODL
  Gestione elenco nodi

  WRKNODLE
  Gestione voci elenco nodi

Operazioni per la descrizione NetBIOS (*NTBD)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla descrizione NetBIOS (*NTBD) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  SAVCFG
  Salvataggio configurazione
- Operazione di modifica

  CHGNTBD
  Modifica descrizione NetBIOS
- Operazioni che non sono controllate

  Copia Opzione 3 di WRKNTBD

  DSPNTBD
  Visualizzazione descrizione NetBIOS

RTVCFGSRC
Richiamo dell'origine della configurazione della descrizione NetBIOS

WRKNTBD
Gestione descrizione NetBIOS

Operazioni per l'interfaccia di rete (*NWID)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'interfaccia di rete (*NWID) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  SAVCFG
  Salvataggio configurazione
- Operazione di modifica

  CHGNWIISDN
  Modifica descrizione interfaccia di rete

  VRYCFG
  Attivazione o disattivazione della descrizione interfaccia di rete
- Operazioni che non sono controllate

  Copia Opzione 3 di WRKNWID

  DSPNWID
  Visualizzazione descrizione interfaccia di rete

  ENDNWIRCY
  Fine ripristino interfaccia di rete

  RSMNWIRCY
  Ripresa ripristino interfaccia di rete

  RTVCFGSRC
  Richiamo dell'origine della descrizione interfaccia di rete

  RTVCFGSTS
  Richiamo stato descrizione interfaccia di rete

  WRKNWID
  Gestione descrizione interfaccia di rete

  WRKCFGSTS
  Gestione stato descrizione interfaccia di rete

Operazioni per la descrizione server di rete (*NWSD)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla descrizione server di rete (*NWSD) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  SAVCFG
  Salvataggio configurazione
- Operazione di modifica

  CHGNWSD
  Modifica descrizione server di rete

  VRYCFG
  Modifica configurazione
- Operazioni che non sono controllate

Copia Opzione 3 di WRKNWSD

DSPNWSD
Visualizzazione descrizione server di rete

RTVCFGSRC
Richiamo origine configurazione per *NWSD

RTVCFGSTS
Richiamo stato configurazione per *NWSD

WRKNWSD
Gestione descrizione server di rete

Operazioni per la coda di emissione (*OUTQ)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla coda di emissione (*OUTQ) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  STRPRTWTR
  Avvio di un programma di stampa in una OUTQ

  STRRMTWTR
  Avvio di un programma di scrittura remoto in una OUTQ

- Operazione di modifica

  Posizionamento
  Quando una voce è collocata nella coda o rimossa da essa

  CHGOUTQ
  Modifica coda emissione

  CHGSPLFA [4]
  Modifica attributi file di spool, se viene spostato in un'altra coda di emissione e una o l'altra coda di emissione viene controllata

  CLROUTQ
  Cancellazione contenuto coda emissione

  DLTSPLF [4]
  Cancellazione file di spool

  HLDOUTQ
  Congelamento coda emissione

  RLSOUTQ
  Rilascio coda emissione

- Operazioni che non sono controllate

  CHGSPLFA [4]
  Modifica attributi file di spool

  CPYSPLF [4]
  Copia file di spool

  Creazione [4]
  Creazione di un file di spool

  DSPSPLF [4]
  Visualizzazione file di spool

  HLDSPLF [4]
  Congelamento file di spool

QSPROUTQ
Richiamo informazioni coda emissione

RLSSPLF [4]
Rilascio file di spool

SNDNETSPLF [4]
Invio file di spool di rete

WRKOUTQ
Gestione coda emissione

WRKOUTQD
Gestione descrizione coda emissione

WRKSPLF
Gestione file di spool

WRKSPLFA
Gestione attributi file di spool

Operazioni per la sovrapposizione (*OVL)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla sovrapposizione (*OVL) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Stampa
  Stampa di un file di spool che fa riferimento alla sovrapposizione
- Operazione di modifica

  Nessuna
- Operazioni che non sono controllate

  WRKOVL
  Gestione sovrapposizione

  Stampa
  Riferimento alla sovrapposizione durante la creazione di un file di spool

Operazioni per la definizione pagina (*PAGDFN)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla definizione pagina (*PAGDFN) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Stampa
  Stampa di un file di spool che fa riferimento alla definizione pagina
- Operazione di modifica

  Nessuna
- Operazioni che non sono controllate

  WRKPAGDFN
  Gestione definizione pagina

  Stampa
  Riferimento alla definizione formato durante la creazione di un file di spool

4. Questo viene controllato anche se il controllo operazione (valore di sistema QAUDLVL o valore profilo utente AUDLVL) include *SPLFDTA.

Operazioni per il segmento pagina (*PAGSEG)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al segmento pagina (*PAGSEG) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Stampa
  Stampa di un file di spool che fa riferimento al segmento pagina

- Operazione di modifica

  Nessuna

- Operazioni che non sono controllate

  WRKPAGSEG
  Gestione segmento pagina

  Stampa
  Riferimento al segmento pagina durante la creazione di un file di spool

Operazioni per il gruppo descrittori di stampa (*PDG)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al gruppo descrittori di stampa (*PDG) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Apertura
  Quando il gruppo descrittori di pagina viene aperto per accesso di lettura da un'API PrintManager o da un verbo CPI.

- Operazione di modifica

  Apertura
  Quando il gruppo descrittori di pagina viene aperto per accesso di modifica da un API PrintManager* o da un verbo CPI.

- Operazioni che non sono controllate

  CHGPDGPRF
  Modifica profilo gruppo descrittori di stampa

  WRKPDG
  Gestione gruppo descrittori di stampa

Operazioni per il programma (*PGM)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al programma (*PGM) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Attivazione
  Attivazione programma

  Chiamata
  Programma che non è stato già attivato

  ADDPGM
  Aggiunta del programma al debug

  QTEDBGS
  API Qte Registrazione vista debug

QTEDBGS
API Qte Richiamo viste modulo

// RUN
Esecuzione programma in un ambiente S/36

RTVCLSRC
Richiamo sorgente CL

STRDBG
Avvio debug

- Operazione di creazione

CRTPGM
Creazione programma

UPDPGM
Aggiornamento programma

- Operazione di modifica

CHGCSPPGM
Modifica programma CSP/AE

CHGPGM
Modifica programma

CHGS36PGMA
Modifica attributi programma S/36

EDTS36PGMA
Editazione attributi programma S/36

WRKS36PGMA
Gestione attributi programma S/36

- Operazioni che non sono controllate

ANZPGM
Analisi programma

DMPCLPGM
Dump programma CL

DSPCSPOBJ
Visualizzazione oggetto CSP

DSPPGM
Visualizzazione programma

PRTCMDUSG
Stampa utilizzo comando

PRTCSPAPP
Stampa applicazione CSP

PRTSQLINF
Stampa informazioni SQL

QBNLPGMI
API Elenco informazioni programma ILE

QCLRPGMI
API Richiamo informazioni programma

STRCSP
Avvio programmi di utilità CSP

TRCCSP
Traccia applicazione CSP

WRKOBJCSP
Gestione degli oggetti per CSP

WRKPGM
Gestione programma

Operazioni per il gruppo di pannelli (*PNLGRP)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al gruppo di pannelli (*PNLGRP) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  ADDSCHIDXE
  Aggiunta voce indice ricerca

  QUIOPNDA
  API Apertura gruppo pannelli per la visualizzazione

  QUIOPNPA
  API Apertura gruppo pannelli per la stampa

  QUHDSPH
  API Visualizzazione aiuto
- Operazione di modifica

  Nessuna

- Operazioni che non sono controllate

  WRKPNLGRP
  Gestione gruppo di pannelli

Operazioni per la disponibilità prodotto (*PRDAVL)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla disponibilità prodotto (*PRDAVL) e se tali operazioni vengono controllate o meno.

- Operazione di modifica

  WRKSPTPRD
  Gestione prodotti supportati, quando il supporto è aggiunto o rimosso
- Operazioni che non sono controllate

  Lettura
  Non viene controllata alcuna operazione di lettura

Operazioni per la definizione prodotto (*PRDDFN)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla definizione prodotto (*PRDDFN) e se tali operazioni vengono controllate o meno.

- Operazione di modifica

  ADDPRDLICI
  Aggiunta informazioni prodotto su licenza

  WRKSPTPRD
  Gestione prodotti supportati, quando il supporto è aggiunto o rimosso
- Operazioni che non sono controllate

Lettura
Non viene controllata alcuna operazione di lettura

Operazioni per il caricamento prodotto (*PRDLOD)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al caricamento prodotto (*PRDLOD) e se tali operazioni vengono controllate o meno.

- Operazione di modifica

  Modifica
  Stato caricamento prodotto, elenco librerie caricamento prodotto, elenco cartelle caricamento prodotto, lingua principale

- Operazioni che non sono controllate

  Lettura
  Non viene controllata alcuna operazione di lettura

Operazioni per modulo Query Manager (*QMFORM)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al modulo Query Manager (*QMFORM) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  STRQMQRY
  Avvio query Query Management

  RTVQMFORM
  Richiamo modulo Query Management

  Esecuzione
  Esecuzione di una query

  Esportare
  Esportazione modulo Query Management

  Stampa
  Stampa modulo Query Management

  Stampa di un prospetto Query Management utilizzando il modulo

  Utilizzo di
  Accesso al modulo utilizzando l'opzione 2, 5, 6 o 9 oppure la funzione F13 da DB2 Query Manager e SQL Development Kit per i5/OS.

- Operazione di modifica

  CRTQMFORM
  Creazione modulo Query Management

  IMPORT
  Importazione modulo Query Management

  Salvataggio
  Salvataggio del modulo utilizzando un'opzione di menu o di un comando

  Copia Opzione 3 dalla funzione Gestione moduli Query Management

- Operazioni che non sono controllate

  Gestione
  Quando vengono elencati *QMFORM in un pannello Gestione

  Attiva Qualsiasi operazione relativa al modulo eseguita nei confronti del modulo 'attivo'.

Operazioni per la query Query Manager (*QMQRY)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla query Query Manager (*QMQRY) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  RTVQMQRY
  Richiamo query Query Manager

  Esecuzione
  Esecuzione query Query Manager

  STRQMQRY
  Avvio query Query Manager

  Esportare
  Esportazione query Query Manager

  Stampa
  Stampa query Query Manager

  Utilizzo di
  Accesso alla query tramite la funzione F13 o l'opzione 2, 5, 6 o 9 dalla funzione Gestione query Query Manager
- Operazione di modifica

  CRTQMQRY
  Creazione query Query Management

  Conversione
  Opzione 10 (Conversione in SQL) dalla funzione Gestione query Query Manager

  Copia Opzione 3 dalla funzione Gestione query Query Manager

  Salvataggio
  Salvataggio della query utilizzando un menu o un comando
- Operazioni che non sono controllate

  Gestione
  Quando vengono elencate *QMQRY in un pannello Gestione

  Attiva Qualsiasi operazione relativa alla query eseguita nei confronti della query 'attiva'.

Operazioni per la definizione query (*QRYDFN)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla definizione query (*QRYDFN) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  ANZQRY
  Analisi query

  Modifica
  Modifica di una query utilizzando un pannello di richiesta presentato da WRKQRY o QRY.

  Visualizzazione
  Visualizzazione di una query utilizzando il pannello di richiesta WRKQRY

  Esportare
  Esportazione del modulo utilizzando Query Manager

  Esportare
  Esportazione della query utilizzando Query Manager

Stampa
Stampa di una definizione query utilizzando il pannello di richiesta WRKQRY

Stampa del modulo Query Management

Stampa della query Query Management

Stampa del prospetto Query Management

QRYRUN
Esecuzione della query

RTVQMFORM
Richiamo modulo Query Management

RTVQMQRY
Richiamo query Query Management

Esecuzione
Esecuzione della query utilizzando il pannello di richiesta WRKQRY

Esecuzione (comando Query Management)

RUNQRY
Esecuzione della query

STRQMQRY
Avvio query Query Management

Inoltro
Inoltro di una query (esecuzione di una richiesta) in batch utilizzando il pannello di richiesta WRKQRY o il pannello di richiesta Fine query

- Operazione di modifica

  Modifica
  Salvataggio di una query modificata utilizzando il programma su licenza Query/400
- Operazioni che non sono controllate

  Copia Copia di una query utilizzando l'opzione 3 sul pannello "Gestione query"

  Creazione
  Creazione di una query utilizzando l'opzione 1 sul pannello "Gestione query"

  Cancellazione
  Cancellazione di una query utilizzando l'opzione 4 sul pannello "Gestione query"

  Esecuzione
  Esecuzione di una query utilizzando l'opzione 1 sul pannello "Fine query" quando si crea o si modifica una query utilizzando il programma su licenza Query/400; Esecuzione interattiva di una query utilizzando PF5 mentre si crea, si visualizza o si modifica una query utilizzando il programma su licenza Query/400

  DLTQRY
  Cancellazione di una query

Operazioni per la tabella conversione codice di riferimento (*RCT)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla tabella conversione codice di riferimento (*RCT) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Nessuna

- Operazione di modifica

Nessuna

- Operazioni che non sono controllate

  Nessuna

Operazioni per l'elenco di risposte

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'elenco di risposte e se tali operazioni vengono controllate o meno.

Nota: le operazioni relative all'elenco di risposte sono controllate se il valore di sistema controllo operazione (QAUDLVL) o il parametro del controllo operazione (AUDLVL) nel profilo utente include *SYSMGT.

- Operazioni che sono controllate

  ADDRPYLE
  Aggiunta di una voce dell'elenco risposte

  CHGRPYLE
  Modifica di una voce dell'elenco risposte

  RMVRPYLE
  Eliminazione di una voce dell'elenco risposte

  WRKRPYLE
  Gestione voce elenco risposte

- Operazioni che non sono controllate

  Nessuna

Operazioni per la descrizione sottosistema (*SBSD)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla descrizione sottosistema (*SBSD) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  ENDSBS
  Arresto sottosistema

  STRSBS
  Avvio sottosistema

- Operazione di modifica

  ADDAJE
  Aggiunta voce lavoro di avvio automatico

  ADDCMNE
  Aggiunta voce di comunicazioni

  ADDJOBQE
  Aggiunta voce coda lavori

  ADDPJE
  Aggiunta voce lavoro di preavvio

  ADDRTGE
  Aggiunta voce instradamento

ADDWSE
Aggiunta voce stazione di lavoro

CHGAJE
Modifica voce lavoro di avvio automatico

CHGCMNE
Modifica voce di comunicazioni

CHGJOBQE
Modifica voce coda lavori

CHGPJE
Modifica voce lavoro di preavvio

CHGRTGE
Modifica voce instradamento

CHGSBSD
Modifica descrizione sottosistema

CHGWSE
Modifica voce stazione di lavoro

RMVAJE
Rimozione voce lavoro di avvio automatico

RMVCMNE
Rimozione voce di comunicazioni

RMVJOBQE
Rimozione voce coda lavori

RMVPJE
Rimozione voce lavoro di preavvio

RMVRTGE
Rimozione voce instradamento

RMVWSE
Rimozione voce stazione di lavoro

- Operazioni che non sono controllate

DSPSBSD
Visualizzazione descrizione sottosistema

QWCLASBS
API Elenco sottosistema attivo

QWDLSJBQ
API Elenco coda lavori sottosistema

QWDRSBSD
API Richiamo descrizione sottosistema

WRKSBSD
Gestione descrizione sottosistema

WRKSBS
Gestione sottosistema

WRKSBSJOB
Gestione lavoro sottosistema

Operazioni per l'indice ricerca informazioni (*SCHIDX)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'indice ricerca informazioni (*SCHIDX) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  STRSCHIDX
  Avvio indice ricerca

  WRKSCHIDXE
  Gestione voce indice ricerca
- Operazione di modifica (controllata se OBJAUD è *CHANGE o *ALL)

  ADDSCHIDXE
  Aggiunta voce indice ricerca

  CHGSCHIDX
  Modifica indice ricerca

  RMVSCHIDXE
  Modifica voce indice ricerca
- Operazioni che non sono controllate

  WRKSCHIDX
  Gestione indice di ricerca

Operazioni per socket locale (*SOCKET)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al socket locale (*SOCKET) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  collegamento
  Associazione di una destinazione permanente ad un socket ed attuazione di un collegamento.

  DSPLNK
  Visualizzazione collegamenti

  givedescriptor
  API Concessione accesso file

  Qp0lGetPathFromFileID
  API Richiamo nome percorso dell'oggetto da ID file

  Qp0lRenameKeep
  API Ridenominazione file o indirizzario, Conservazione nuovo

  Qp0lRenameUnlink
  API Ridenominazione file o indirizzario, Scollegamento nuovo

  sendmsg
  Invio di un datagramma in modalità senza collegamento. È possibile utilizzare più buffer.

  sendto
  Invio di un datagramma in modalità senza collegamento.

  WRKLNK
  Gestione collegamenti
- Operazione di modifica

  ADDLNK
  Aggiunta collegamento

collegamento
Definizione di un indirizzo locale per un socket.

CHGAUD
Modifica controllo

CHGAUT
Modifica autorizzazione

CHGOWN
Modifica proprietario

CHGPGP
Modifica gruppo principale

CHKIN
Controllo in entrata

CHKOUT
Controllo in uscita

chmod
API Modifica autorizzazioni file

chown
API Modifica proprietario e gruppo

givedescriptor
API Concessione accesso file

collegamento
API Creazione di un collegamento al file

Qp0lRenameKeep
API Ridenominazione file o indirizzario, Conservazione nuovo

Qp0lRenameUnlink
API Ridenominazione file o indirizzario, Scollegamento nuovo

RMVLNK
Rimozione collegamento

RNM Ridenominazione

RST Ripristino

scollegamento
API Rimozione di un collegamento al file

utime API Impostazione ore di accesso e modifica file

WRKAUT
Gestione autorizzazione

WRKLNK
Gestione collegamenti

- Operazioni che non sono controllate

  close API Chiusura file

  Nota: la chiusura non è controllata, ma se vi fosse un errore o una modifica in un programma di uscita di chiusura basato sulla scansione, viene tagliato un record di controllo.

  DSPAUT
  Visualizzazione autorizzazione

  dup API Duplicazione descrittore file aperto

dup2 API Duplicazione descrittore file aperto in un altro descrittore

fcntl API Esecuzione comando controllo file

fstat API Richiamo informazioni file per descrittore

fsync API Sincronizzazione modifiche file

ioctl API Esecuzione richiesta controllo I/E

lstat API Richiamo informazioni su file o collegamento

pathconf
API Richiamo variabili nome percorso configurabili

lettura API Lettura da file

readv API Lettura da file (Vettore)

select API Controllo stato I/E di più descrittori file

stat API Richiamo informazioni file

takedescriptor
API Acquisizione accesso file

scrittura
API Scrittura nel file

writev API Scrittura nel file (Vettore)

Operazioni per il dizionario di ausilio ortografico (*SPADCT)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al dizionario di ausilio ortografico (*SPADCT) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Verifica
  Funzione di verifica ortografica

  Ausilio
  Funzione ausilio ortografico

  Tratteggiatura
  Funzione tratteggiatura

  Eliminazione tratteggiatura
  Funzione eliminazione tratteggiatura

  Sinonimi
  Funzione sinonimi

  Base Utilizzo del dizionario come base quando si crea un altro dizionario

  Verifica
  Utilizzo come dizionario di verifica quando si crea un altro dizionario

  Richiamo
  Richiamo origine elenco parole d'arresto

  Stampa
  Stampa origine elenco parole d'arresto
- Operazione di modifica

  CRTSPADCT
  Creazione dizionario di ausilio ortografico con REPLACE(*YES)
- Operazioni che non sono controllate

Nessuna

Operazioni per i file di spool

Questo elenco descrive le operazioni che è possibile effettuare rispetto ai file di spool e se tali operazioni vengono controllate o meno.

Nota: le operazioni sui file di spool sono controllate se il valore di sistema del controllo operazione (QAUDLVL) o il parametro del controllo operazione (AUDLVL) nel profilo utente include *SPLFDTA.

- Operazioni che sono controllate

  Accesso

  Ogni accesso da parte di qualsiasi utente che non sia il proprietario del file di spool, incluso:

  – CPYSPLF
  – DSPSPLF
  – SNDNETSPLF
  – SNDTCPSPLF
  – STRRMTWTR
  – API QSPOPNSP

  Modifica

  Modifica di uno qualsiasi dei seguenti attributi del file di spool con CHGSPLFA:

  – COPIES
  – DEV
  – FORMTYPE
  – RESTART
  – PAGERANGE
  – OUTQ
  – DRAWER
  – PAGDFN
  – FORMDF
  – USRDFNOPT
  – USRDFNOBJ
  – USRDFNDTA
  – EXPDATE
  – SAVE

  Modifica di uno qualsiasi dei seguenti attributi del file di spool con CHGSPLFA:

  Creazione

  Creazione di un file di spool tramite operazioni di stampa

  Creazione di un file di spool tramite l'API QSPCRTSP

  Cancellazione

  Cancellazione di un file di spool per mezzo di una qualsiasi delle seguenti operazioni:

  – Stampa di un file di spool per mezzo di un programma di scrittura della stampante o del minidisco
  – Cancellazione coda emissione (CLROUTQ)
  – Cancellazione del file di spool tramite il comando DLTSPLF o l'opzione di cancellazione da un pannello dei file di spool

– Cancellazione dei file di spool al termine di un lavoro (ENDJOB SPLFILE(*YES))
– Cancellazione dei file spool al termine di un lavoro di stampa (ENDPJ SPLFILE(*YES))
– Invio di un file di spool ad un sistema remoto da parte di un programma di scrittura remoto
– Eliminazione dei file di spool scaduti, utilizzando il comando DLTEXPSPLF
– Eliminazione dei file di spool tramite la funzione di ripulitura di operational assist

Congelamento
Congelamento di un file di spool tramite una delle seguenti operazioni:
– Utilizzo del comando HLDSPLF
– Utilizzo dell'opzione congelamento da un pannello dei file di spool
– Stampa di un file di spool che specifica SAVE(*YES)
– Invio di un file di spool ad un sistema remoto da parte di un programma di scrittura remoto quando il file di spool specifica SAVE(*YES)
– Il congelamento di un file di spool da parte di un programma di scrittura dopo che si è verificato un errore durante l'elaborazione del file di spool

Lettura
Lettura di un file di spool da parte di un programma di scrittura della stampante o del minidisco

Rilascio
Rilascio di un file di spool

Ripristino
Ripristino di un file di spool

Salvataggio
Salvataggio di un file di spool

Operazioni per il pacchetto SQL (*SQLPKG)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al pacchetto SQL (*SQLPKG) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Esecuzione
  Quando si esegue l'oggetto *SQLPKG

- Operazione di modifica

  Nessuna

- Operazioni che non sono controllate

  PRTSQLINF
  Stampa informazioni SQL

Operazioni per il programma di servizio (*SRVPGM)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al programma di servizio (*SRVPGM) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  CRTPGM
  Una voce di controllo per ogni programma di servizio utilizzato durante un comando CRTPGM

CRTSRVPGM
Una voce di controllo per ogni programma di servizio utilizzato durante un comando CRTSRVPGM

QTEDBGS
API Registrazione vista debug

QTEDBGS
API Richiamo viste modulo

RTVBNDSRC
Richiamo origine binder

UPDPGM
Una voce di controllo per ogni programma di servizio utilizzato durante un comando UPDPGM.

UPDSRVPGM
Una voce di controllo per ogni programma di servizio utilizzato durante un comando UPDSRVPGM.

- Operazione di creazione

  CRTSRVPGM
  Creazione programma servizio

  UPDSRVPGM
  Aggiornamento programma servizio
- Operazione di modifica

  CHGSRVPGM
  Modifica programma servizio
- Operazioni che non sono controllate

  DSPSRVPGM
  Visualizzazione programma servizio

  PRTSQLINF
  Stampa informazioni SQL

  QBNLSPGM
  API Elenco informazioni programma servizio

  QBNRSPGM
  API Richiamo informazioni programma servizio

  WRKSRVPGM
  Gestione programma servizio

Operazioni per la descrizione sessione (*SSND)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla descrizione sessione (*SSND) e se tali operazioni vengono controllate o meno.

Non viene controllata alcuna operazione di Lettura o Modifica per il tipo di oggetto *SSND.

Operazioni per lo spazio memoria server (*SVRSTG)

Questo elenco descrive le operazioni che è possibile effettuare rispetto allo spazio memoria server (*SVRSTG) e se tali operazioni vengono controllate o meno.

Non viene controllata alcuna operazione di Lettura o Modifica per il tipo di oggetto *SVRSTG.

Operazioni per il file di flusso (*STMF)

Questo elenco descrive le operazioni che è possibile effettuare rispetto agli oggetti file di flusso (*STMF) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  CPY Copia oggetto

  DSPLNK
  Visualizzazione collegamenti oggetto

  givedescriptor
  API Concessione accesso file

  MOV Spostamento oggetto

  open, open64, QlgOpen, QlgOpen64, Qp0lOpen
  API Apertura file

  SAV Salvataggio oggetto

  WRKLNK
  Gestione collegamenti oggetto

- Operazione di modifica

  ADDLNK
  Aggiunta collegamento

  CHGAUD
  Modifica controllo

  CHGAUT
  Modifica autorizzazione

  CHGOWN
  Modifica proprietario

  CHGPGP
  Modifica gruppo principale

  CHKIN
  Controllo in entrata oggetto

  CHKOUT
  Controllo in uscita oggetto

  chmod, QlgChmod
  API Modifica autorizzazioni file

  chown, QlgChown
  API Modifica proprietario e gruppo

  CPY Copia oggetto

  creat, creat64, QlgCreat, QlgCreat64
  API Creazione nuovo file o Riscrittura file esistente

  fchmod
  API Modifica autorizzazioni file per descrittore

  fchown
  API Modifica proprietario e gruppo del file per descrittore

  givedescriptor
  API Concessione accesso file

collegamento
API Creazione di un collegamento al file

MOV Spostamento oggetto

open, open64, QlgOpen, QlgOpen64, Qp0lOpen
API di apertura per la scrittura

Qp0lGetPathFromFileID, QlgGetPathFromFileID
API Richiamo nome percorso dell'oggetto da ID file

Qp0lRenameKeep, QlgRenameKeep
API Ridenominazione file o indirizzario, Conservazione nuovo

Qp0lRenameUnlink, QlgRenameUnlink
API Ridenominazione file o indirizzario, Scollegamento nuovo

RMVLNK
Rimozione collegamento

RNM Ridenominazione oggetto

RST Ripristino oggetto

unlink, QlgUnlink
API Rimozione di un collegamento al file

utime, QlgUtime
API Impostazione ore di accesso e modifica file

WRKAUT
Gestione autorizzazione

WRKLNK
Gestione collegamenti

- Operazioni che non sono controllate

close API Chiusura file

DSPAUT
Visualizzazione autorizzazione

dup API Duplicazione descrittore file aperto

dup2 API Duplicazione descrittore file aperto in un altro descrittore

faccessx
Determinazione accessibilità file

fclear, fclear64
Eliminazione del contenuto di un file

fcntl API Esecuzione comando controllo file

fpathconf
API Richiamo variabili nome percorso configurabili per descrittore

fstat, fstat64
API Richiamo informazioni file per descrittore

fsync API Sincronizzazione modifiche file

ftruncate, ftruncate64
API Troncamento file

ioctl API Esecuzione richiesta controllo I/E

lseek, lseek64
API Impostazione scostamento lettura/scrittura file

lstat, lstat64
API Richiamo informazioni file o collegamento

pathconf, QlgPathconf
API Richiamo variabili nome percorso configurabili

pread, pread64
API Lettura da identificativo con scostamento

pwrite, pwrite64
API Scrittura in identificativo con scostamento

lettura API Lettura da file

readv API Lettura da file (Vettore)

select API Controllo stato I/E di più descrittori file

stat, stat64, QlgStat, QlgStat64
API Richiamo informazioni file

takedescriptor
API Acquisizione accesso file

scrittura
API Scrittura nel file

writev API Scrittura nel file (Vettore)

Operazioni per il collegamento simbolico (*SYMLNK)

Questo elenco descrive le operazioni che è possibile effettuare rispetto agli oggetti collegamento simbolico (*SYMLNK) e se tali operazioni vengono controllate.

- Operazione di lettura

  CPY Copia oggetto

  DSPLNK
  Visualizzazione collegamenti oggetto

  MOV Spostamento oggetto

  readlink
  API Lettura valore di collegamento simbolico

  SAV Salvataggio oggetto

  WRKLNK
  Gestione collegamenti oggetto
- Operazione di modifica

  CHGOWN
  Modifica proprietario

  CHGPGP
  Modifica gruppo principale

  CPY Copia oggetto

  MOV Spostamento oggetto

  Qp0lRenameKeep, QlgRenameKeep
  API Ridenominazione file o indirizzario, Conservazione nuovo

Qp0lRenameUnlink, QlgRenameUnlink
API Ridenominazione file o indirizzario, Scollegamento nuovo

RMVLNK
Rimozione collegamento

RNM Ridenominazione oggetto

RST Ripristino oggetto

symlink, QlgSymlink
API Effettuazione di un collegamento simbolico

unlink, QlgUnlink
API Rimozione di un collegamento al file

WRKLNK
Gestione collegamenti oggetto

- Operazioni che non sono controllate

lstat, lstat64, QlgLstat, QlgLstat64
API Stato del collegamento

Operazioni per la descrizione macchina S/36 (*S36)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla descrizione macchina S/36 (*S36) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

Nessuna

- Operazione di modifica

CHGS36
Modifica della configurazione S/36

CHGS36A
Modifica degli attributi di configurazione S/36

SET Procedura SET

CRTDEVXXX
Quando si aggiunge un'unità alla tabella delle configurazioni

DLTDEVD
Quando si cancella un'unità dalla tabella delle configurazioni

RNMOBJ
Ridenominazione descrizione unità

- Operazioni che non sono controllate

DSPS36
Visualizzazione configurazione S/36

RTVS36A
Richiamo attributi configurazione S/36

STRS36
Avvio S/36

ENDS36
Fine S/36

Operazioni per la tabella (*TBL)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla tabella (*TBL) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  QDCXLATE
  Conversione stringa caratteri

  QTBXLATE
  Conversione stringa caratteri

  QLGRTVSS
  Richiamo tabella sequenza ordinamento

  CRTLF
  Tabella conversione durante il comando CRTLF

  Lettura
  Utilizzo della Tabella sequenza di ordinamento durante l'esecuzione di qualsiasi comando che può specificare una sequenza di ordinamento

- Operazione di modifica

  Nessuna

- Operazioni che non sono controllate

  WRKTBL
  Gestione tabella

Operazioni per l'indice utente (*USRIDX)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'indice utente (*USRIDX) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  QUSRTVUI
  API Richiamo voci indice utente

- Operazione di modifica

  QUSADDUI
  API Aggiunta voci indice utente

  QUSRMVUI
  API Rimozione voci indice utente

- Operazioni che non sono controllate

  Accesso
  Accesso diretto ad un indice utente utilizzando istruzioni MI (consentite solo per un indice utente dominio utente in una libreria specificata nel valore di sistema QALWUSRDMN.)

  QUSRUIAT
  API Richiamo attributi indice utente

Operazioni per il profilo utente (*USRPRF)

Questo elenco descrive le operazioni che è possibile effettuare rispetto al profilo utente (*USRPRF) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

RCLOBJOWN
Richiamo oggetti per proprietario

- Operazione di modifica

CHGPRF
Modifica profilo

CHGPWD
Modifica parola d'ordine

CHGUSRPRF
Modifica profilo utente

CHKPWD
Controllo parola d'ordine

DLTUSRPRF
Cancellazione profilo utente

GRTUSRAUT
Concessione autorizzazione utente (*a-profilo-utente*)

QSYCHGPW
API Modifica parola d'ordine

RSTUSRPRF
Ripristino profilo utente

- Operazioni che non sono controllate

DSPPGMADP
Visualizzazione programmi di adozione

DSPUSRPRF
Visualizzazione profilo utente

GRTUSRAUT
Concessione autorizzazione utente (*da-profilo-utente*)

PRTPRFINT
Stampa valori interni profilo

PRTUSRPRF
Stampa profilo utente

QSYCUSRS
API Controllo autorizzazioni speciali utente

QSYLOBJA
API Elenco oggetti autorizzati

QSYLOBJP
API Elenco oggetti di adozione

QSYRUSRI
API Richiamo informazioni utente

RTVUSRPRF
Richiamo profilo utente

WRKOBJOWN
Gestione oggetti di proprietà

WRKUSRPRF
Gestione profili utente

Operazioni per la coda utente (*USRQ)

Questo elenco descrive le operazioni che è possibile effettuare rispetto alla coda utente (*USRQ) e se tali operazioni vengono controllate o meno.

- Non viene controllata alcuna operazione di Lettura o Modifica per il tipo di oggetto *USRQ.
- Operazioni che non sono controllate

  Accesso
  Accesso diretto alle code utente utilizzando istruzioni MI (consentite solo per una coda utente dominio utente in una libreria specificata nel valore di sistema QALWUSRDMN.)

Operazioni per lo spazio utente (*USRSPC)

Questo elenco descrive le operazioni che è possibile effettuare rispetto allo spazio utente (*USRSPC) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  QUSRTVUS
  API Richiamo spazio utente
- Operazione di modifica

  QUSCHGUS
  API Modifica spazio utente

  QUSCUSAT
  API Modifica attributi spazio utente
- Operazioni che non sono controllate

  Accesso
  Accesso diretto allo spazio utente utilizzando istruzioni MI (consentite solo per spazi utente dominio utente nelle librerie specificate nel valore di sistema QALWUSRDMN.)

  QUSRUSAT
  API Richiamo attributi spazio utente

Operazioni per elenco di convalida (*VLDL)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'elenco di convalida (*VLDL) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  QSYFDVLE
  API Reperimento voce elenco di convalida
- Operazione di modifica

  QSYADVLE
  API Aggiunta voce elenco di convalida

  QSYCHVLE
  API Modifica voce elenco di convalida

  QSYRMVLE
  API Rimozione voce elenco di convalida

Operazioni per l'oggetto personalizzazione stazione di lavoro (*WSCST)

Questo elenco descrive le operazioni che è possibile effettuare rispetto all'oggetto personalizzazione stazione di lavoro (*WSCST) e se tali operazioni vengono controllate o meno.

- Operazione di lettura

  Variazione
  Quando viene attivata un'unità personalizzata

  RTVWSCST
  Richiamo dell'origine oggetto personalizzazione stazione di lavoro (solo quando è specificato *TRANSFORM per il tipo di unità)

  SNDTCPSPLF
  Invio file di spool TCP/IP (solo quando è specificato TRANSFORM(*YES))

  STRPRTWTR
  Avvio programma di stampa (solo per file di spool che sono stampati in una stampante personalizzata utilizzando la funzione trasformazione stampa host)

  STRRMTWTR
  Avvio programma di scrittura remoto (solo quando la coda di emissione è configurata con CNNTYPE(*IP) e TRANSFORM(*YES))

  Stampa
  Quando l'emissione viene stampata direttamente (non in spool) in una stampante personalizzata utilizzando la funzione trasformazione stampa host

- Operazione di modifica

  Nessuna

- Operazioni che non sono controllate

  Nessuna

Appendice F. Layout di voci di giornale di controllo

Questa sezione contiene informazioni sul layout per tutti i tipi di voce con codice giornale T nel giornale di controllo (QAUDJRN). Queste voci sono controllate tramite il controllo operazione e oggetto definito dall'utente.

I layout di voce di giornale descritti in questa appendice sono simili alla modalità di definizione di un file fisico utilizzando DDS. Ad esempio, viene definito un Binary (4) per conservare informazioni da 1 a 4 cifre con requisiti di memorizzazione di due byte; un Binary (5), invece, conserva informazioni da 1 a 5 cifre con requisiti di memorizzazione di 4 byte. I linguaggi come RPG utilizzano e forzano tali definizioni. Il sistema scrive voci supplementari nel giornale di controllo per eventi quali l'IPL di sistema o il salvataggio del ricevitore di giornale. I layout per questi tipi di voci possono essere reperiti nell'argomento Gestione giornale.

La "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 contiene il layout per i campi comuni a tutti i tipi di voce quando si specifica OUTFILFMT(*TYPE2) nel comando DSPJRN. Questo layout, denominato QJORDJE2, viene definito nel file QADSPJR2 nella libreria QSYS.

La "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 contiene il layout per campi che sono comuni a tutti i tipi di voci quando si specifica OUTFILFMT(*TYPE4) nel comando DSPJRN. Questo layout, denominato QJORDJE4, viene definito nel file QADSPJR4 nella libreria QSYS. L'emissione *TYPE4 include tutte le informazioni *TYPE2, oltre ad informazioni sugli identificativi di giornale, i trigger e limiti di riferimento.

Nota: i formati di emissione TYPE2 e *TYPE4 non vengono più aggiornati; perciò si consiglia di smettere di utilizzare i formati *TYPE2 e *TYPE4 ed utilizzare solo i formati *TYPE5.

La "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596 contiene il layout per i campi che sono comuni a tutti i tipi di voci quando si specifica OUTFILFMT(*TYPE5) sul comando DSPJRN. Questo layout, denominato QJORDJE5, viene definito nel file QADSPJR5 nella libreria QSYS. L'emissione *TYPE5 include tutte le informazioni *TYPE4, oltre alle informazioni sulla libreria di programma, sul nome unità ASP programma, sul numero unità ASP programma, sul ricevitore, sulla libreria ricevitore, sul nome unità ASP ricevitore, sul numero unità ASP ricevitore, sul numero braccetto, sull'ID sottoprocesso, sulla famiglia indirizzi, sulla porta remota e sull'indirizzo remoto.

Le tabelle che vanno dalla "Voci di giornale AD (Modifica controllo)" a pagina 602 alla "Voci di giornale ZR (Lettura di oggetto)" a pagina 745 contengono layout per i file di emissione database modello forniti per definire dati specifici della voce. È possibile utilizzare il comando CRTDUPOBJ per creare qualsiasi file di emissione vuoto con lo stesso layout di uno dei file di emissione database modello. È possibile utilizzare il comando DSPJRN per copiare voci selezionate dal giornale di controllo nel file di emissione per l'analisi. La sezione "Analisi delle voci giornale di controllo con la query o un programma" a pagina 319 fornisce esempi di utilizzo dei file di emissione database modello. Consultare inoltre l'argomento Gestione giornale.

Nota: In queste tabelle di voci di giornale, potrebbe essere visualizzata una colonna vuota nella colonna scostamento JE o J4. Ciò significa che non sono presenti file di emissione modello per tale tipo di giornale di controllo.

Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)

Questa tabella elenca i valori possibili per i campi comuni a tutti i tipi di voce quando si specifica OUTFILFMT(*TYPE5) sul comando DSPJRN.

Tabella 156. Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)

Scost.	Campo	Formato	Descrizione
1	Lunghezza della voce	Zoned(5,0)	Lunghezza totale della voce di giornale incluso il campo lunghezza voce.
6	Numero di sequenza	Char(20)	Applicato ad ogni voce di giornale. Inizialmente impostato su 1 per ogni giornale nuovo o ripristinato. Facoltativamente, reimpostare su 1 quando viene collegato un nuovo ricevitore.
26	Codice giornale	Char(1)	Sempre T.
27	Tipo di voce	Char(2)	Consultare la "Tipi di voce giornale di controllo (QAUDJRN)" a pagina 600 per un elenco di tipi di voce e relative descrizioni.
29	Registrazione data/ora della voce	Char(26)	La data e l'ora in cui è stata creata la voce nel formato registrazione data/ora SAA.
55	Nome del lavoro	Char(10)	Il nome del lavoro che ha dato luogo alla creazione della voce.
65	Nome utente	Char(10)	Il nome profilo utente associato al lavoro[1].
75	Numero lavoro	Zoned(6,0)	Il numero del lavoro.
81	Nome programma	Char(10)	Il nome del programma che ha creato la voce di giornale. Può essere anche il nome di un programma di servizio o il nome parziale di un file di classe utilizzato in un programma Java compilato. Se un programma dell'applicazione o un programma CL non ha creato la voce, il campo contiene il nome di un programma fornito dal sistema come ad esempio QCMD. Il campo ha valore *NONE se è in atto una delle seguenti condizioni: • Il nome programma non si applica a questo tipo di voce. • Il nome programma non era disponibile.
91	Libreria programma	Char(10)	Nome della libreria in cui è il programma che ha aggiunto la voce di giornale.
101	Unità ASP programma	Char(10)	Nome dell'unità ASP che contiene il programma che ha aggiunto la voce di giornale.
111	Numero ASP programma	Zoned(5,0)	Numero dell'ASP che contiene il programma che ha aggiunto la voce di giornale.
116	Nome dell'oggetto	Char(10)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
126	Libreria oggetti	Char(10)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
136	Nome membro	Char(10)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
146	Conteggio/RRN	Char(20)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
166	Indicatore	Char(1)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
167	Identificativo ciclo sincronizzazione	Char(20)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.

Tabella 156. Campi intestazione standard per voci giornale di controllo (Continua). Formato record QJORDJE5 (*TYPE5)

Scost.	Campo	Formato	Descrizione
187	Profilo utente	Char(10)	Il nome del profilo utente corrente[1].
197	Nome sistema	Char(8)	Il nome del sistema.
205	Identificativo giornale	Char(10)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
215	Limite di riferimento	Char(1)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
216	Trigger	Char(1)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
217	Dati incompleti	Char(1)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
218	Ignorato da APY/ RMVJRNCHG	Char(1)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
219	ESD minimizzato	Char(1)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
220	Indicatore oggetto	Char(1)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
221	Sequenza sistema	Char(20)	Un numero assegnato dal sistema ad ogni voce di giornale.
241	Ricevitore	Char(10)	Il nome del ricevitore che contiene la voce di giornale.
251	Libreria ricevitore	Char(10)	Il nome della libreria in cui si trova il ricevitore che contiene la voce di giornale.
261	Unità ASP ricevitore	Char(10)	Nome dell'unità ASP che contiene il ricevitore.
271	Numero ASP ricevitore	Zoned(5,0)	Numero dell'ASP che contiene il ricevitore che contiene la voce di giornale.
276	Numero braccetto	Zoned(5,0)	Il numero del braccetto disco che contiene la voce di giornale.
281	Identificativo sottoprocesso	Hex(8)	Identifica il sottoprocesso nell'ambito del processo che ha aggiunto la voce di giornale.
289	Esadecimale identificativo sottoprocesso	Char(16)	Versione esadecimale visualizzabile dell'identificativo sottoprocesso.
305	Famiglia indirizzi	Char(1)	Il formato dell'indirizzo remoto per questa voce di giornale.
306	Porta remota	Zoned(5,0)	Il numero porta dell'indirizzo remoto associato alla voce di giornale.
311	Indirizzo remoto	Char(46)	L'indirizzo remoto associato alla voce di giornale.
357	Unità logica di lavoro	Char(39)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
396	ID transazione	Char(140)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
536	Riservato	Char(20)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
556	Indicatori valore nullo	Char(50)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
606	Lunghezza dati specifici voce	Binary(5)	La lunghezza dei dati specifici della voce.

Tabella 156. Campi intestazione standard per voci giornale di controllo (Continua). Formato record QJORDJE5 (*TYPE5)

Scost.	Campo	Formato	Descrizione
Nota: i tre campi che iniziano dallo scostamento 55 costituiscono il nome lavoro del sistema. Nella maggior parte dei casi, il campo Nome utente allo scostamento 65 ed il campo Nome profilo utente allo scostamento 187 hanno lo stesso valore. Per lavori preavviati, il campo Nome profilo utente contiene il nome dell'utente che dà inizio alla transazione. Per alcuni lavori, entrambi questi campi contengono QSYS come nome utente. Il campo Nome profilo utente nei dati specifici della voce contiene l'effettivo utente che ha dato origine alla voce. Se si utilizza un'API per scambiare i profili utente, il campo Nome profilo utente contiene il nome del nuovo profilo utente (scambiato).			

Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)

Questa tabella elenca i valori possibili per i campi comuni a tutti i tipi di voce quando si specifica OUTFILFMT(*TYPE4) sul comando DSPJRN.

Tabella 157. Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)

Scost.	Campo	Formato	Descrizione
1	Lunghezza della voce	Zoned(5,0)	Lunghezza totale della voce di giornale incluso il campo lunghezza voce.
6	Numero di sequenza	Zoned(10,0)	Applicato ad ogni voce di giornale. Inizialmente impostato su 1 per ogni giornale nuovo o ripristinato. Facoltativamente, reimpostare su 1 quando viene collegato un nuovo ricevitore.
16	Codice giornale	Char(1)	Sempre T.
17	Tipo di voce	Char(2)	Consultare la "Tipi di voce giornale di controllo (QAUDJRN)" a pagina 600 per un elenco di tipi di voce e relative descrizioni.
19	Registrazione data/ora della voce	Char(26)	La data e l'ora in cui è stata creata la voce nel formato registrazione data/ora SAA.
45	Nome del lavoro	Char(10)	Il nome del lavoro che ha dato luogo alla creazione della voce.
55	Nome utente	Char(10)	Il nome profilo utente associato al lavoro[1].
65	Numero lavoro	Zoned(6,0)	Il numero del lavoro.
71	Nome programma	Char(10)	Il nome del programma che ha creato la voce di giornale. Può essere anche il nome di un programma di servizio o il nome parziale di un file di classe utilizzato in un programma Java compilato. Se un programma dell'applicazione o un programma CL non ha creato la voce, il campo contiene il nome di un programma fornito dal sistema come ad esempio QCMD. Il campo ha valore *NONE se è in atto una delle seguenti condizioni: • Il nome programma non si applica a questo tipo di voce. • Il nome programma non era disponibile.
81	Nome oggetto	Char(10)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
91	Nome libreria	Char(10)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
101	Nome membro	Char(10)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
111	Conteggio/RRN	Zoned(10)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.

Tabella 157. Campi intestazione standard per voci giornale di controllo (Continua). Formato record QJORDJE4 (*TYPE4)

Scost.	Campo	Formato	Descrizione
121	Indicatore	Char(1)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
122	ID ciclo sincronizzazione	Zoned(10)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
132	Profilo utente	Char(10)	Il nome del profilo utente corrente[1].
142	Nome sistema	Char(8)	Il nome del sistema.
150	Identificativo giornale	Char(10)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
160	Limite di riferimento	Char(1)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
161	Trigger	Char(1)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
162	(Area riservata)	Char(8)	
170	Indicatori valore nullo	Char(50)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
220	Lunghezza dati specifici voce	Binary (4)	La lunghezza dei dati specifici della voce.

Nota: i tre campi che iniziano dallo scostamento 45 costituiscono il nome lavoro del sistema. Nella maggior parte dei casi, il campo Nome utente allo scostamento 55 ed il campo Nome profilo utente allo scostamento 132 hanno lo stesso valore. Per lavori preavviati, il campo Nome profilo utente contiene il nome dell'utente che dà inizio alla transazione. Per alcuni lavori, entrambi questi campi contengono QSYS come nome utente. Il campo Nome profilo utente nei dati specifici della voce contiene l'effettivo utente che ha dato origine alla voce. Se si utilizza un'API per scambiare i profili utente, il campo Nome profilo utente contiene il nome del nuovo profilo utente (scambiato).

Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)

Questa tabella elenca i valori possibili per i campi comuni a tutti i tipi di voce quando si specifica OUTFILFMT(*TYPE2) sul comando DSPJRN.

Tabella 158. Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)

Scost.	Campo	Formato	Descrizione
1	Lunghezza della voce	Zoned(5,0)	Lunghezza totale della voce di giornale incluso il campo lunghezza voce.
6	Numero di sequenza	Zoned(10,0)	Applicato ad ogni voce di giornale. Inizialmente impostato su 1 per ogni giornale nuovo o ripristinato. Facoltativamente, reimpostare su 1 quando viene collegato un nuovo ricevitore.
16	Codice giornale	Char(1)	Sempre T.
17	Tipo di voce	Char(2)	Consultare la "Tipi di voce giornale di controllo (QAUDJRN)" a pagina 600 per un elenco di tipi di voce e relative descrizioni.
19	Registrazione data/ora	Char(6)	La data di sistema in cui è stata creata la voce.
25	Ora voce	Zoned(6,0)	L'ora di sistema in cui è stata creata la voce.
31	Nome del lavoro	Char(10)	Il nome del lavoro che ha dato luogo alla creazione della voce.
41	Nome utente	Char(10)	Il nome profilo utente associato al lavoro[1].

Tabella 158. Campi intestazione standard per voci giornale di controllo (Continua). Formato record QJORDJE2 (*TYPE2)

Scost.	Campo	Formato	Descrizione
51	Numero lavoro	Zoned(6,0)	Il numero del lavoro.
57	Nome programma	Char(10)	Il nome del programma che ha creato la voce di giornale. Può essere anche il nome di un programma di servizio o il nome parziale di un file di classe utilizzato in un programma Java compilato. Se un programma dell'applicazione o un programma CL non ha creato la voce, il campo contiene il nome di un programma fornito dal sistema come ad esempio QCMD. Il campo ha valore *NONE se è in atto una delle seguenti condizioni: • Il nome programma non si applica a questo tipo di voce. • Il nome programma non era disponibile.
67	Nome oggetto	Char(10)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
77	Nome libreria	Char(10)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
87	Nome membro	Char(10)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
97	Conteggio/RRN	Zoned(10)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
107	Indicatore	Char(1)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
108	ID ciclo sincronizzazione	Zoned(10)	Utilizzato per gli oggetti registrati su giornale. Non utilizzato per voci di giornale di controllo.
118	Profilo utente	Char(10)	Il nome del profilo utente corrente[1].
128	Nome sistema	Char(8)	Il nome del sistema.
136	(Area riservata)	Char(20)	

[1] I tre campi che iniziano dallo scostamento 31 costituiscono il nome lavoro del sistema. Nella maggior parte dei casi, il campo *Nome utente* allo scostamento 41 e il campo *Nome profilo utente* allo scostamento 118 hanno lo stesso valore. Per lavori preavviati, il campo *Nome profilo utente* contiene il nome dell'utente che dà inizio alla transazione. Per alcuni lavori, entrambi questi campi contengono QSYS come nome utente. Il campo *Nome profilo utente* nei dati specifici della voce contiene l'utente effettivo che ha dato origine alla voce. Se si utilizza un'API per scambiare i profili utente, il campo *Nome profilo utente* contiene il nome del nuovo profilo utente (scambiato).

Tipi di voce giornale di controllo (QAUDJRN)

Questa tabella introduce tutti i tipi di voce disponibili per il giornale di controllo.

Tabella 159. Tipi di voce giornale di controllo (QAUDJRN)

Tipo di voce	Descrizione
AD	Modifiche controllo
AF	Errore autorizzazione
AP	Acquisizione autorizzazione adottata
AU	Modifiche attributo
CA	Modifiche autorizzazione
CD	Controllo stringa comando

Tabella 159. Tipi di voce giornale di controllo (QAUDJRN) (Continua)

Tipo di voce	Descrizione
CO	Creazione oggetto
CP	Profilo utente modificato, creato o ripristinato
CQ	Modifica dell'oggetto *CRQD
CU	Operazioni cluster
CV	Verifica collegamento
CY	Configurazione crittografica
DI	Server indirizzario
DO	Cancellazione oggetto
DS	Reimpostazione parola d'ordine sicurezza DST
EV	Variabili d'ambiente di sistema
GR	Record generico
GS	Descrizione socket fornita ad un altro lavoro
IM	Controllo intrusione
IP	Comunicazioni tra processi
IR	Azioni regole IP
IS	Gestione sicurezza Internet
JD	Modifica a parametro utente di una descrizione lavoro
JS	Operazioni che influenzano i lavori
KF	File key ring
LD	Collegamento, scollegamento o ricerca voce indirizzario
ML	Operazioni posta servizi Office
NA	Attributo rete modificato
ND	Violazione filtro ricerca indirizzario APPN
NE	Violazione filtro endpoint APPN
OM	Spostamento o ridenominazione oggetto
OR	Ripristino oggetto
OW	Proprietà oggetto modificata
O1	(Accesso unità ottica) Singolo file o indirizzario
O2	(Accesso unità ottica) Doppio file o indirizzario
O3	(Accesso unità ottica) Volume
PA	Programma modificato per adottare autorizzazione
PG	Modifica del gruppo principale di un oggetto
PO	Emissione stampata
PS	Interscambio profilo
PW	Parola d'ordine non valida
RA	Modifica autorizzazione durante ripristino
RJ	Ripristino descrizione lavoro con profilo utente specificato
RO	Modifica proprietario oggetto durante ripristino
RP	Ripristino programma autorizzazione adottata

Tabella 159. Tipi di voce giornale di controllo (QAUDJRN) (Continua)

Tipo di voce	Descrizione
RQ	Ripristino di un oggetto *CRQD
RU	Ripristino autorizzazione profilo utente
RZ	Modifica di un gruppo principale durante il ripristino
SD	Modifiche all'indirizzario di distribuzione sistema
SE	Voce di instradamento del sottosistema modificata
SF	Operazioni su file di spool
SG	Segnali asincroni
SK	Connessioni socket protette
SM	Modifiche alla gestione sistemi
SO	Operazioni di informazioni utente sicurezza server
ST	Utilizzo dei programmi di manutenzione
SV	Valore di sistema modificato
VA	Modifica di un ACL (access control list)
VC	Avvio o fine di un collegamento
VF	Chiusura file server
VL	Limite account superato
VN	Collegamento e scollegamento rete
VO	Operazioni elenco di convalida
VP	Errore parola d'ordine di rete
VR	Accesso risorsa di rete
VS	Avvio o fine sessione server
VU	Modifica di un profilo di rete
VV	Modifica stato servizio
X0	Autenticazione rete
X1	Token di identità
XD	Estensione server indirizzario
YC	Accesso ad oggetto DLO (modifica)
YR	Accesso ad oggetto DLO (lettura)
ZC	Accesso ad oggetto (modifica)
ZR	Accesso ad oggetto (lettura)

Voci di giornale AD (Modifica controllo)

Questa tabella fornisce il formato delle voci di giornale AD (Modifica Controllo).

Tabella 160. Voci di giornale AD (Modifica controllo). File descrizione campo QASYADJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	**D** Comando CHGDLOAUD **O** Comando CHGOBJAUD o CHGAUD **S** L'attributo scansione è stato modificato utilizzando il comando CHGATR o l'API Qp0lSetAttr, o quando è stato creato l'oggetto. **U** Comando CHGUSRAUD
157	225	611	Nome oggetto	Char(10)	Nome dell'oggetto per cui è stato modificato il controllo.
167	235	621	Nome libreria	Char(10)	Nome della libreria per l'oggetto.
177	245	631	Tipo oggetto	Char(8)	Il tipo di oggetto.
185	253	639	Valore controllo oggetto	Char(10)	Se il tipo di voce è D, O o U, il campo contiene il valore di controllo specificato. Se il tipo di voce è S, il campo contiene il valore dell'attributo di scansione.
195	263	649	CHGUSRAUD *CMD	Char(1)	Y = Controllare comandi per questo utente.
196	264	650	CHGUSRAUD *CREATE	Char(1)	Y = Scrivere un record di controllo quando questo utente crea un oggetto.
197	265	651	CHGUSRAUD *DELETE	Char(1)	Y = Scrivere un record di controllo quando questo utente cancella un oggetto.
198	266	652	CHGUSRAUD *JOBDTA	Char(1)	Y = Scrivere un record di controllo quando questo utente modifica un lavoro.
199	267	653	CHGUSRAUD *OBJMGT	Char(1)	Y = Scrivere un record di controllo quando questo utente sposta o ridenomina un oggetto.
200	268	654	CHGUSRAUD *OFCSRV	Char(1)	Y = Scrivere un record di controllo quando questo utente esegue funzioni Office.
201	269	655	CHGUSRAUD *PGMADP	Char(1)	Y = Scrivere un record di controllo quando questo utente ottiene l'autorizzazione tramite autorizzazione adottata.
202	270	656	CHGUSRAUD *SAVRST	Char(1)	Y = Scrivere un record di controllo quando questo utente salva o ripristina oggetti.
203	271	657	CHGUSRAUD *SECURITY	Char(1)	Y = Scrivere un record di controllo quando questo utente esegue operazioni rilevanti per la sicurezza.
204	272	658	CHGUSRAUD *SERVICE	Char(1)	Y = Scrivere un record di controllo quando questo utente esegue funzioni di servizio.

Tabella 160. Voci di giornale AD (Modifica controllo) (Continua). File descrizione campo QASYADJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
205	273	659	CHGUSRAUD *SPLFDTA	Char(1)	Y = Scrivere un record di controllo quando questo utente gestisce file di spool.
206	274	660	CHGUSRAUD *SYSMGT	Char(1)	Y = Scrivere un record di controllo quando questo utente apporta modifiche alla gestione sistemi.
207	275	661	CHGUSRAUD *OPTICAL	Char(1)	Y = Scrivere un record di controllo quando questo utente accede ad unità ottiche.
208	276	662	CHGUSRAUD *AUTFAIL	Char(1)	Y = Scrivere un record di controllo quando questo utente dispone di un errore autorizzazione.
		663	CHGUSRAUD *JOBBAS	Char(1)	Y = Scrivere un record di controllo quando questo utente esegue la funzione di base del lavoro.
		664	CHGUSRAUD *JOBCHGUSR	Char(1)	Y = Scrivere un record di controllo quando questo utente modifica il profilo utente attivo di un sottoprocesso o il relativo file di gruppo.
		665	CHGUSRAUD *NETBAS	Char(1)	Y = Scrivere un record di controllo quando questo utente esegue funzioni di base della rete.
		666	CHGUSRAUD *NETCLU	Char(1)	Y = Scrivere un record di controllo quando questo utente esegue funzioni gruppo risorsa cluster o cluster.
		667	CHGUSRAUD *NETCMN	Char(1)	Y = Scrivere un record di controllo quando questo utente esegue funzioni di comunicazione di rete.
		668	CHGUSRAUD *NETFAIL	Char(1)	Y = Scrivere un record di controllo quando questo utente dispone di un errore di rete.
		669	CHGUSRAUD *NETSCK	Char(1)	Y = Scrivere un record di controllo quando questo utente esegue attività socket.
		670	CHGUSRAUD *PGMFAIL	Char(1)	Y = Scrivere un record di controllo quando questo utente dispone di un errore programma.
		671	CHGUSRAUD *PRTDTA	Char(1)	Y = Scrivere un record di controllo quando questo utente esegue una funzione di stampa con parametro SPOOL(*NO).
		672	CHGUSRAUD *SECCFG	Char(1)	Y = Scrivere un record di controllo quando questo utente esegue configurazione della sicurezza.
		673	CHGUSRAUD *SECDIRSRV	Char(1)	Y = Scrivere un record di controllo quando questo utente apporta modifiche o aggiornamenti utilizzando le funzioni del servizio indirizzario.
		674	CHGUSRAUD *SECIPC	Char(1)	Y = Scrivere un record di controllo quando questo utente apporta modifiche alle comunicazioni tra processi.
		675	CHGUSRAUD *SECNAS	Char(1)	Y = Scrivere un record di controllo quando questo utente esegue azioni di servizio autenticazione di rete.

Tabella 160. Voci di giornale AD (Modifica controllo) (Continua). File descrizione campo QASYADJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
		676	CHGUSRAUD *SECRUN	Char(1)	Y = Scrivere un record di controllo quando questo utente esegue funzioni di tempo di esecuzione della sicurezza.
		677	CHGUSRAUD *SECSCKD	Char(1)	Y = Scrivere un record di controllo quando questo utente esegue funzioni descrittore socket.
		678	CHGUSRAUD *SECVFY	Char(1)	Y = Scrivere un record di controllo quando questo utente utilizza funzioni di verifica.
		679	CHGUSRAUD *SECVLDL	Char(1)	Y = Scrivere un record di controllo quando questo utente manipola elenchi di convalida.
		680	(Area riservata)	Char(19)	
227	295	681	Nome DLO	Char(12)	Nome dell'oggetto DLO per il controllo è stato modificato.
239	307	693	(Area riservata)	Char(8)	
247	315	701	Percorso cartella	Char(63)	Percorso della cartella.
310			(Area riservata)	Char(20)	
	378	764	(Area riservata)	Char(18)	
	396	782	Lunghezza nome oggetto[1]	Binary (4)	La lunghezza del nome oggetto.
330	398	784	CCSID nome oggetto[1]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
334	402	788	ID paese o regione nome oggetto[1]	Char(2)	L'ID paese o regione per il nome oggetto.
336	404	790	ID lingua nome oggetto[1]	Char(3)	L'ID lingua per il nome oggetto.
339	407	793	(Area riservata)	Char(3)	
342	410	796	ID file principale[1,2]	Char(16)	L'ID file dell'indirizzario principale.
358	426	812	ID file oggetto[1,2]	Char(16)	L'ID file dell'oggetto.
374	442	828	Nome oggetto[1]	Char(512)	Il nome dell'oggetto.
	954	1340	ID file oggetto[1]	Char(16)	L'ID file dell'oggetto.
	970	1356	Nome ASP[5]	Char(10)	Il nome dell'unità ASP
	980	1366	Numero ASP[5]	Char(5)	Il numero dell'unità ASP.
	985	1371	CCSID nome percorso[1]	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	989	1375	ID paese o regione nome percorso[1]	Char(2)	L'ID paese o regione per il nome percorso.
	991	1377	ID lingua nome percorso[1]	Char(3)	L'ID lingua per il nome percorso.
	994	1380	Lunghezza nome percorso[1]	Binary (4)	La lunghezza del nome percorso.

Tabella 160. Voci di giornale AD (Modifica controllo) (Continua). File descrizione campo QASYADJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
	996	1382	Indicator nome percorso[1]	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	997	1383	ID file indirizzario relativo[1, 3]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[3]
	1013	1399	Nome percorso[1, 4]	Char(5002)	Il nome percorso dell'oggetto.

| [1] Questi campi vengono utilizzati solo per oggetti nei file system "root" (/), QOpenSys e negli UDFS (user-defined file systems).

[2] Un ID con il bit all'estrema sinistra impostato ed il resto dei bit zero indica che l'ID NON è impostato.

[3] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[4] Questo è un campo a lunghezza variabile. I primi due byte contengono la lunghezza del nome percorso.

[5] Se l'oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.

Voci di giornale AF (Errore autorizzazione)

Questa tabella fornisce il formato delle voci di giornale A (Errore autorizzazione).

Tabella 161. Voci di giornale AF (Errore autorizzazione). File descrizione campo QASYAFJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.

Tabella 161. Voci di giornale AF (Errore autorizzazione) (Continua). File descrizione campo QASYAFJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
156	224	610	Tipo di violazione[1]	Char(1)	**A** Non autorizzato per l'oggetto **B** Istruzione limitata **C** Errore di convalida (vedere J5 scostamento 639) **D** Utilizzo di interfaccia non supportata, errore dominio oggetto **E** Errore protezione memoria hardware, violazione spazio costante programma **F** Errore autorizzazione ICAPI **G** Errore autorizzazione ICAPI **H** Operazione programma di uscita di scansione (vedere J5 scostamento 639) **I**[7] Eredità sistema Java non consentita **J** Errore inoltro profilo lavoro **K** Violazione autorizzazione speciale **N** Token profilo non rigenerabile **O** Errore autorizzazione oggetto unità ottica **P** Errore interscambio profilo **R** Errore protezione hardware **S** Tentativo di accesso predefinito **T** Nessuna autorizzazione per la porta TCP/IP **U** Richiesta permesso utente non valida **V** Token profilo non valido per la creazione di un nuovo token profilo **W** Token profilo non valido per lo swap **X** Violazione di sistema — vedere J5 scostamento 723 per codici violazione **Y** Non autorizzato per il campo JUID corrente un'operazione di ripulitura JUID. **Z** Non autorizzato per il campo JUID corrente un'operazione di impostazione JUID.
157	225	611	Nome oggetto [1, 5, 12, 17]	Char(10)	Il nome dell'oggetto.
167	235	621	Nome libreria[13]	Char(10)	Il nome della libreria in cui è memorizzato l'oggetto o il numero correzione del LIC la cui applicazione non è riuscita.[11]
177	245	631	Tipo oggetto[14, 17]	Char(8)	Il tipo di oggetto.

Tabella 161. Voci di giornale AF (Errore autorizzazione) (Continua). File descrizione campo QASYAFJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
185	253	639	Operazione errore di convalida	Char(1)	Operazione eseguita dopo rilevamento errore di convalida, impostata solo se il tipo di violazione (J5 scostamento 610) è C o H. **A** Conversione oggetto non tentata o non riuscita. L'impostazione del valore di sistema QALWOBJRST ha permesso il ripristino dell'oggetto. L'utente che esegue il ripristino non ha autorizzazione speciale *ALLOBJ e il livello sicurezza sistema è impostato su 10, 20 o 30. Autorizzazioni all'oggetto conservate. **B** Conversione oggetto non tentata o non riuscita. L'impostazione del valore di sistema QALWOBJRST ha permesso il ripristino dell'oggetto. L'utente che esegue il ripristino non ha autorizzazione speciale *ALLOBJ e il livello sicurezza sistema è impostato su 40 o superiore. Autorizzazioni all'oggetto revocate. **C** Conversione oggetto riuscita. La copia convertita è stata ripristinata sul sistema. **D** Conversione oggetto non tentata o non riuscita. L'impostazione del valore di sistema QALWOBJRST ha permesso il ripristino dell'oggetto. L'utente che esegue il ripristino ha autorizzazione speciale *ALLOBJ. Autorizzazioni all'oggetto conservate. **E** Rilevato errore tempo installazione sistema. **F** Oggetto non ripristinato, la firma non è in formato i5/OS. **G** Oggetto stato sistema non firmato o eredità rilevato durante il controllo del sistema. **H** Oggetto stato utente non firmato rilevato durante il controllo del sistema. **I** Mancata corrispondenza oggetto/firma rilevata durante il controllo del sistema. **J** Certificato IBM non rilevato durante il controllo del sistema. **K** Formato firma non valido rilevato durante il controllo del sistema. **M** Il prog. uscita scansione ha modificato l'oggetto sottoposto a scansione **X** Il prog. uscita scansione richiede che per l'oggetto sia indicato un errore di scansione

Tabella 161. Voci di giornale AF (Errore autorizzazione) (Continua). File descrizione campo QASYAFJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
186	254	640	Nome lavoro	Char(10)	Il nome del lavoro.
196	264	650	Nome utente	Char(10)	Il nome utente lavoro.
206	274	660	Numero lavoro	Zoned(6,0)	Il numero del lavoro.
212	280	666	Nome programma	Char(10)	Il nome del programma.
222	290	676	Libreria programma	Char(10)	Il nome della libreria dove è stato reperito il programma.
232	300	686	Profilo utente [2]	Char(10)	Il nome dell'utente che ha causato l'errore di autorizzazione.
242	310	696	Nome stazione di lavoro	Char(10)	Il nome della stazione di lavoro o il tipo della stazione di lavoro.
252	320	706	Numero istruzione programma	Zoned(7,0)	Il numero istruzione del programma.
259	327	713	Nome campo	Char(10)	Il nome del campo.
269	337	723	Codice di violazione operazione	Char(3)	Il tipo di violazione operazione che si è verificato, impostato solo se il tipo di violazione (J5 scostamento 610) è X. **AAC** Non autorizzato all'utilizzo del comando di analisi avanzata SST. **HCA** Profilo utente programmi di manutenzione non autorizzato ad eseguire un'operazione di configurazione hardware (QYHCHCOP). **LIC** LIC indica che una correzione del LIC non è stata applicata a causa di una violazione della firma. **SFA** Non autorizzato ad attivare l'attributo ambiente per l'accesso file di sistema. **CMD** È stato effettuato un tentativo di utilizzare un comando disabilitato da un responsabile di sistema.
272	340	726	Utente Office	Char(10)	Il nome dell'utente Office.
282	350	736	Nome DLO	Char(12)	Il nome del DLO (document library object).
294	362	748	(Area riservata)	Char(8)	
302	370	756	Percorso cartella[15, 16]	Char(63)	Il percorso della cartella.
365	433	819	Office per conto dell'utente	Char(10)	Utente che opera per conto di un altro utente.
375			(Area riservata)	Char(20)	
	443	829	(Area riservata)	Char(18)	
	461	847	Lunghezza nome oggetto[3]	Binary (4)	La lunghezza del nome oggetto.

Tabella 161. Voci di giornale AF (Errore autorizzazione) (Continua). File descrizione campo QASYAFJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
395	463	849	CCSID nome oggetto[3]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
399	467	853	ID paese o regione nome oggetto[3]	Char(2)	L'ID paese o regione per il nome oggetto.
401	469	855	ID lingua nome oggetto[3]	Char(3)	L'ID lingua per il nome oggetto.
404	472	858	(Area riservata)	Char(3)	
407	475	861	ID file principale[3,4]	Char(16)	L'ID file dell'indirizzario principale.
423	491	877	ID file oggetto[3,4]	Char(16)	L'ID file dell'oggetto.
439	507	893	Nome oggetto[3,6]	Char(512)	Il nome dell'oggetto.
	1019	1405	ID file oggetto [3]	Char(16)	L'ID file dell'oggetto.
	1035	1421	Nome ASP[10]	Char(10)	Il nome dell'unità ASP
	1045	1431	Numero ASP[10]	Char(5)	Il numero dell'unità ASP.
	1050	1436	CCSID nome percorso[3]	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	1054	1440	ID paese o regione nome percorso[3]	Char(2)	L'ID paese o regione per il nome percorso.
	1056	1442	ID lingua nome percorso[3]	Char(3)	L'ID lingua per il nome percorso.
	1059	1445	Lunghezza nome percorso[3]	Binary (4)	La lunghezza del nome percorso.
	1061	1447	Indicatore nome percorso[3]	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	1062	1448	ID file indirizzario relativo[3, 8]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[8]
	1078	1464	Nome percorso[3, 9]	Char(5002)	Il nome percorso dell'oggetto.
		6466	Nome libreria programma ASP	Char(10)	Nome ASP per libreria programma

Tabella 161. Voci di giornale AF (Errore autorizzazione) (Continua). File descrizione campo QASYAFJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
		6476	Numero libreria programma ASP	Char(5)	Numero ASP per libreria programma

[1] Quando il tipo di violazione è per la descrizione G, il nome oggetto contiene il nome del *SRVPGM che a sua volta conteneva l'uscita che ha rilevato l'errore. Per ulteriori informazioni sui tipi di violazione, consultare la "Voci di giornale di controllo sicurezza" a pagina 289.

[2] Il campo contiene il nome dell'utente che ha dato origine alla voce. QSYS potrebbe essere l'utente per le seguenti voci:

- scostamenti 41 e 118 per record *TYPE2
- scostamenti 55 e 132 per record *TYPE4
- scostamenti 65 e 187 per record *TYPE5

[3] Questi campi vengono utilizzati solo per oggetti nei file system ″root″ (/), QOpenSys e negli UDFS (user-defined file systems).

[4] Un ID con il bit all'estrema sinistra impostato ed il resto dei bit zero indica che l'ID NON è impostato.

[5] Quando il tipo di violazione è T, il nome oggetto contiene la porta TCP/IP che l'utente non è autorizzato ad utilizzare. Il valore è giustificato a sinistra e vuoto. Il campi relativi alla libreria oggetto e al tipo di di oggetto saranno vuoti.

[6] Quando il tipo di violazione è O, il nome oggetto dell'unità ottica è contenuto nel campo nome oggetto IFS. I campi ID paese o regione, ID lingua, ID file principale e ID file oggetto conterranno tutti spazi.

[7] L'oggetto classe Java che viene creato non è in grado di estendere la propria classe base poiché la classe base ha attributi di sistema Java.

[8] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[9] Questo è un campo a lunghezza variabile. I primi due byte contengono la lunghezza del nome percorso.

[10] Se l'oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.

[11] Quando il tipo di violazione è X e il valore del codice Violazione operazione è LIC, ciò indica che una correzione del LIC non è stata applicata a causa di una violazione della firma. Questo campo conterrà il numero correzione LIC la cui applicazione non è riuscita.

[12] Quando il tipo di violazione è K, il nome oggetto contiene il nome del comando o programma che ha rilevato l'errore. Se il comando presenta numerosi nomi alternativi, il nome comando nel record di controllo potrebbe non corrispondere al nome comando specifico utilizzato ma sarà una delle alternative equivalenti. Il valore speciale *INSTR indica che un'istruzione macchina ha rilevato l'errore.

[13] Quando il tipo di violazione è K, il nome libreria contiene il nome della libreria del programma *N per la libreria del comando che ha rilevato l'errore.

[14] Quando il tipo di violazione è K, il tipo di oggetto contiene il tipo di oggetto del comando o programma che ha rilevato l'errore.

[15] Quando il tipo di violazione è K, il percorso cartella potrebbe contenere il nome API completo o il nome del punto di uscita che ha rilevato l'errore.

[16] Quando il tipo di violazione è X e il valore del codice Violazione operazione è AAC, il Percorso cartella conterrà un nome comando di analisi avanzata di 30 caratteri.

[17] Quando il tipo di oggetto è *LIC e la libreria oggetto è *N, il nome oggetto è un nome Ru LIC (Licensed Internal Code).

Voci di giornale AP (Autorizzazione adottata)

Questa tabella fornisce il formato delle voci di giornale AP (Autorizzazione adottata).

Tabella 162. Voci di giornale AP (Autorizzazione adottata). File descrizione campo QASYAPJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	**S** Avvio **E** Fine **A** Autorizzazione adottata utilizzata durante attivazione programma
157	225	611	Nome oggetto	Char(10)	Il nome del programma, del programma di servizio o del pacchetto SQL
167	235	621	Nome libreria	Char(10)	Il nome della libreria.
177	245	631	Tipo oggetto	Char(8)	Il tipo di oggetto.
185	253	639	Profilo utente proprietario	Char(10)	Il nome del profilo utente la cui autorizzazione viene adottata.
195	263	649	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	279	665	Nome ASP[1]	Char(10)	Il nome dell'unità ASP
	289	675	Numero ASP[1]	Char(5)	Il numero dell'unità ASP.

[1] Se l'oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.

Voci di giornale AU (Modifiche attributo)

Questa tabella fornisce il formato delle voci di giornale AU (Modifiche attributo).

Tabella 163. Voci di giornale AU (Modifiche attributo). File descrizione campo QASYAUJ5

Scost.			
J5	**Campo**	**Formato**	**Descrizione**
610	Tipo di voce	Char(1)	Il tipo di voce. **E** Attributi configurazione EIM
611	Operazione	Char(3)	Operazione **CHG** Attributi modificati
614	Nome	Char(100)	Nome attributo
714	Nuova lunghezza del valore	Binary (4)	Lunghezza nuovo valore

Tabella 163. Voci di giornale AU (Modifiche attributo) (Continua). File descrizione campo QASYAUJ5

Scost. J5	Campo	Formato	Descrizione
716	Nuovo CCSID valore	Binary(5)	CCSID nuovo valore
720	ID paese o regione nuovo valore	Char(2)	ID paese o regione nuovo valore
722	ID lingua nuovo valore	Char(3)	ID lingua nuovo valore
725	Nuovo valore	Char(2002) [1]	Nuovo valore
2727	Lunghezza vecchio valore	Binary (4)	Lunghezza vecchio valore
2729	CCSID vecchio valore	Binary(5)	CCSID vecchio valore
2733	ID paese o regione vecchio valore	Char(2)	ID paese o regione vecchio valore
2735	ID lingua vecchio valore	Char(3)	ID lingua vecchio valore
2738	Vecchio valore	Char(2002) [1]	Vecchio valore
1 Questo è un campo a lunghezza variabile. I primi due byte contengono la lunghezza del campo.			

Voci di giornale CA (Modifiche autorizzazione)

Questa tabella fornisce il formato delle voci di giornale CA (Modifiche autorizzazione).

Tabella 164. Voci di giornale CA (Modifiche autorizzazione). File descrizione campo QASYCAJE/J4/J5

Scost. JE	Scost. J4	Scost. J5	Campo	Formato	Descrizione
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Modifiche all'autorizzazione
157	225	611	Nome oggetto	Char(10)	Il nome dell'oggetto.
167	235	621	Nome libreria	Char(10)	Il nome della libreria dove è memorizzato l'oggetto.
177	245	631	Tipo oggetto	Char(8)	Il tipo di oggetto.
185	253	639	Nome utente	Char(10)	Il nome del profilo utente con autorizzazione in fase di concessione o revoca.
195	263	649	Nome elenco autorizzazioni	Char(10)	Il nome dell'elenco autorizzazioni.

Tabella 164. Voci di giornale CA (Modifiche autorizzazione) (Continua). File descrizione campo QASYCAJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
					Autorizzazioni concesse o eliminate:
205	273	659	Esistenza oggetto	Char(1)	**Y** *OBJEXIST
206	274	660	Gestione oggetto	Char(1)	**Y** *OBJMGT
207	275	661	Operativo oggetto	Char(1)	**Y** *OBJOPR
208	276	662	Gestione elenco autoriz.	Char(1)	**Y** *AUTLMGT
209	277	663	Elenco di autorizzazioni	Char(1)	**Y** Autorizzazione pubblica *AUTL
210	278	664	Autorizzazione alla lettura	Char(1)	**Y** *READ
211	279	665	Autorizzazione all'aggiunta	Char(1)	**Y** *ADD
212	280	666	Autorizzazione all'aggiornam.	Char(1)	**Y** *UPD
213	281	667	Autorizzazione alla cancellazione	Char(1)	**Y** *DLT
214	282	668	Autorizzazione all'esclusione	Char(1)	**Y** *EXCLUDE
215	283	669	Autorizzazione all'esecuzione	Char(1)	**Y** *EXECUTE
216	284	670	Autorizzazione Alterazione oggetto	Char(1)	**Y** *OBJALTER
217	285	671	Autorizzazione Riferimento oggetto	Char(1)	**Y** *OBJREF
218	286	672	(Area riservata)	Char(4)	
222	290	676	Tipo comando	Char(3)	Il tipo di comando utilizzato. **GRT** Concessione **RPL** Concessione con sostituzione **RVK** Revoca **USR** Operazione GRTUSRAUT
225	293	679	Nome campo	Char(10)	Il nome del campo.
235	303		(Area riservata)	Char(10)	
		689	Attributo oggetto	Char(10)	L'attributo dell'oggetto.
245	313	699	Utente Office	Char(10)	Il nome dell'utente Office.
255	323	709	Nome DLO	Char(12)	Il nome del DLO.
267	335	721	(Area riservata)	Char(8)	

Tabella 164. Voci di giornale CA (Modifiche autorizzazione) (Continua). File descrizione campo QASYCAJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
275	343	729	Percorso cartella	Char(63)	Il percorso della cartella.
338	406	792	Office per conto dell'utente	Char(10)	Utente che opera per conto di un altro utente.
348	416	802	Stato personale	Char(1)	**Y** Stato personale modificato
349	417	803	Codice accesso	Char(1)	**A** Codice accesso aggiunto **R** Codice accesso eliminato
350	418	804	Codice accesso	Char(4)	Codice accesso.
354			(Area riservata)	Char(20)	
	422	808	(Area riservata)	Char(18)	
	440	826	Lunghezza nome oggetto[1]	Binary (4)	La lunghezza del nome oggetto.
374	442	828	CCSID nome oggetto[1]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
378	446	832	ID paese o regione nome oggetto[1]	Char(2)	L'ID paese o regione per il nome oggetto.
380	448	834	ID lingua nome oggetto[1]	Char(3)	L'ID lingua per il nome oggetto.
383	451	837	(Area riservata)	Char(3)	
386	454	840	ID file principale[1,2]	Char(16)	L'ID file dell'indirizzario principale.
402	470	856	ID file oggetto[1,2]	Char(16)	L'ID file dell'oggetto.
418	486	872	Nome oggetto[1]	Char(512)	Il nome dell'oggetto.
	998	1384	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	1014	1400	Nome ASP[5]	Char(10)	Il nome dell'unità ASP
	1024	1410	Numero ASP[5]	Char(5)	Il numero dell'unità ASP.
	1029	1415	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	1033	1419	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	1035	1421	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	1038	1424	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.

Tabella 164. Voci di giornale CA (Modifiche autorizzazione) (Continua). File descrizione campo QASYCAJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
	1040	1426	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	1041	1427	ID file indirizzario relativo[3]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[3]
	1057	1443	Nome percorso[4]	Char(5002)	Il nome percorso dell'oggetto.

[1] Questi campi vengono utilizzati solo per oggetti nei file system "root" (/), QOpenSys e negli UDFS (user-defined file systems).

[2] Un ID con il bit all'estrema sinistra impostato ed il resto dei bit zero indica che l'ID NON è impostato.

[3] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[4] Questo è un campo a lunghezza variabile. I primi due byte contengono la lunghezza del nome percorso.

[5] Se l'oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.

Voci di giornale CD (Stringa comando)

Questa tabella fornisce il formato delle voci di giornale CD (Stringa comando).

Tabella 165. Voci di giornale CD (Stringa comando). File descrizione campo QASYCDJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.

Tabella 165. Voci di giornale CD (Stringa comando) (Continua). File descrizione campo QASYCDJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **C** Comando eseguito **L** Istruzione OCL **O** Comando controllo operatore **P** Procedura S/36 **S** Esecuzione comando dopo l'avvenuta sostituzione del comando **U** Istruzione controllo programma di utilità
157	225	611	Nome oggetto	Char(10)	Il nome dell'oggetto.
167	235	621	Nome libreria	Char(10)	Il nome della libreria dove è memorizzato l'oggetto.
177	245	631	Tipo oggetto	Char(8)	Il tipo di oggetto.
185	253	639	Esecuzione da un programma CL	Char(1)	**Y** Sì **N** No
186	254	640	Stringa comando	Char(6000)	Il comando che è stato eseguito, con i parametri.
		6640	Nome ASP per libreria comando	Char(10)	Nome ASP per libreria comando
		6650	Numero ASP per libreria comando	Char(5)	Numero ASP per libreria comando

Voci di giornale CO (Creazione oggetto)

Questa tabella fornisce il formato delle voci di giornale CO (Creazione Oggetto.

Tabella 166. Voci di giornale CO (Creazione oggetto). File descrizione campo QASYCOJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **N** Creazione di un nuovo oggetto **R** Sostituzione di un oggetto esistente

Tabella 166. Voci di giornale CO (Creazione oggetto) (Continua). File descrizione campo QASYCOJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
157	225	611	Nome oggetto	Char(10)	Il nome dell'oggetto.
167	235	621	Nome libreria	Char(10)	Il nome della libreria in cui si trova l'oggetto.
177	245	631	Tipo oggetto	Char(8)	Il tipo di oggetto.
185	253		(Area riservata)	Char(20)	
		639	Attributo oggetto	Char(10)	L'attributo dell'oggetto.
		649	(Area riservata)	Char(10)	
205	273	659	Utente Office	Char(10)	Il nome dell'utente Office.
215	283	669	Nome DLO	Char(12)	Il nome del DLO (document library object) creato.
227	295	681	(Area riservata)	Char(8)	
235	303	689	Percorso cartella	Char(63)	Il percorso della cartella.
298	366	752	Office per conto dell'utente	Char(10)	Utente che opera per conto di un altro utente.
308			(Area riservata)	Char(20)	
	376	762	(Area riservata)	Char(18)	
	394	780	Lunghezza nome oggetto	Binary (4)	La lunghezza del nome oggetto.
328	396	782	CCSID nome oggetto[1]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
332	400	786	ID paese o regione nome oggetto[1]	Char(2)	L'ID paese o regione per il nome oggetto.
334	402	788	ID lingua nome oggetto[1]	Char(3)	L'ID lingua per il nome oggetto.
337	405	791	(Area riservata)	Char(3)	
340	408	794	ID file principale[1,2]	Char(16)	L'ID file dell'indirizzario principale.
356	424	810	ID file oggetto[1,2]	Char(16)	L'ID file dell'oggetto.
372	440	826	Nome oggetto[1]	Char(512)	Il nome dell'oggetto.
	952	1338	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	968	1354	Nome ASP[5]	Char(10)	Il nome dell'unità ASP
	978	1364	Numero ASP[5]	Char(5)	Il numero dell'unità ASP.
	983	1369	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	987	1373	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	989	1375	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.

Tabella 166. Voci di giornale CO (Creazione oggetto) (Continua). File descrizione campo QASYCOJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	992	1378	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.
	994	1380	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	995	1381	ID file indirizzario relativo[3]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[3]
	1011	1397	Nome percorso[4]	Char(5002)	Il nome percorso dell'oggetto.

[1] Questi campi vengono utilizzati solo per oggetti nei file system "root" (/), QOpenSys e negli UDFS (user-defined file systems).

[2] Un ID con il bit all'estrema sinistra impostato ed il resto dei bit zero indica che l'ID NON è impostato.

[3] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[4] Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza del nome percorso.

[5] Se l'oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.

Voci di giornale CP (Modifiche profilo utente)

Questa tabella fornisce il formato delle voci di giornale CP (Modifiche profilo utente).

Tabella 167. Voci di giornale CP (Modifiche profilo utente). File descrizione campo QASYCPJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Modifica ad un profilo utente

Tabella 167. Voci di giornale CP (Modifiche profilo utente) (Continua). File descrizione campo QASYCPJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
157	225	611	Nome profilo utente	Char(10)	Il nome del profilo utente che è stato modificato.
167	235	621	Nome libreria	Char(10)	Il nome della libreria.
177	245	631	Tipo oggetto	Char(8)	Il tipo di oggetto.
185	256	639	Nome comando	Char(3)	Il tipo di comando utilizzato. **CRT** CRTUSRPRF **CHG** CHGUSRPRF **RST** RSTUSRPRF **DST** Parola d'ordine QSECOFR reimpostata utilizzando DST **RPA** API QSYRESPA
188	256	642	Parola d'ordine modificata	Char(1)	**Y** Parola d'ordine modificata
189	257	643	Parola d'ordine *NONE	Char(1)	**Y** La parola d'ordine è *NONE.
190	258	644	Parola d'ordine scaduta	Char(1)	**Y** Il valore della parola d'ordine scaduta è *YES **N** Il valore della parola d'ordine scaduta è *NO
191	259	645	Autorizzazione speciale Tutti gli oggetti	Char(1)	**Y** autorizzazione speciale *ALLOBJ
192	260	646	Autorizzazione speciale Controllo lavoro	Char(1)	**Y** Autorizzazione speciale *JOBCTL
193	261	647	Autorizzazione speciale Salvataggio sistema	Char(1)	**Y** Autorizzazione speciale *SAVSYS
194	262	648	Autorizzazione speciale amministratore della riservatezza	Char(1)	**Y** Autorizzazione speciale *SECADM
195	263	649	Autorizzazione speciale Controllo spool	Char(1)	**Y** Autorizzazione speciale *SPLCTL
196	264	650	Autorizzazione speciale Servizio	Char(1)	**Y** Autorizzazione speciale *SERVICE
197	265	651	Autorizzazione speciale Controllo	Char(1)	**Y** Autorizzazione speciale *AUDIT

Tabella 167. Voci di giornale CP (Modifiche profilo utente) (Continua). File descrizione campo QASYCPJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
198	266	652	Autorizzazione speciale Configurazione di sistema	Char(1)	**Y** Autorizzazione speciale *IOSYSCFG
199	267	653	(Area riservata)	Char(13)	
212	280	666	Profilo di gruppo	Char(10)	Il nome di un profilo gruppo.
222	290	676	Proprietario	Char(10)	Proprietario degli oggetti creato come membro di un profilo gruppo.
232	300	686	Autorizzazione gruppo	Char(10)	Autorizzazione profilo gruppo.
242	310	696	Programma iniziale	Char(10)	Il nome del programma iniziale dell'utente.
252	320	706	Libreria programma iniziale	Char(10)	Il nome della libreria dove è stato reperito il programma iniziale.
262	330	716	Menu iniziale	Char(10)	Il nome del menu iniziale dell'utente.
272	340	726	Libreria menu iniziale	Char(10)	Il nome della libreria dove è stato reperito il menu iniziale.
282	350	736	Libreria corrente	Char(10)	Il nome della libreria corrente dell'utente.
292	360	746	Possibilità limitate	Char(10)	Il valore del parametro possibilità limitate.
302	370	756	Classe utente	Char(10)	La classe utente dell'utente.
312	380	766	Limite priorità	Char(1)	Il valore del parametro limite priorità.
313	381	767	Stato profilo	Char(10)	Stato profilo utente.
323	391	777	Tipo autorizzazione gruppo	Char(10)	Il valore del parametro GRPAUTTYP.
333	401	787	Profili gruppo supplementari	Char(150)	I nomi di un massimo di 15 profili gruppo supplementari per l'utente.
483	551	937	Identificazione utente	Char(10)	Uid per l'utente.
493	561	947	Identificazione gruppo	Char(10)	Il gid per l'utente.
503	571	957	Gestione parola d'ordine locale	Char(10)	Il valore del parametro LCLPWDMGT.

Tabella 167. Voci di giornale CP (Modifiche profilo utente) (Continua). File descrizione campo QASYCPJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
		967	Conformità composizione parola d'ordine	Char(10)	Indica se la nuova parola d'ordine è conforme alle regole di composizione della parola d'ordine. ***PASSED** Verificata e conforme. ***SYSVAL** Verificata ma non conforme a causa di una regola basata su un valore di sistema. ***EXITPGM** Verificata ma non conforme a causa di una risposta del programma di uscita. ***NONE** Non verificata; è stato specificato *NONE per la nuova parola d'ordine. ***NOCHECK** Non verificata; la parola d'ordine è stata modificata. Questo campo ha significato solo quando il campo della parola d'ordine modificata contiene una *Y*.
		977	Intervallo scadenza parola d'ordine	Char (7)	Specifica il valore in cui è stato modificato l'intervallo di scadenza della parola d'ordine. ***NOMAX** Nessun intervallo di scadenza. ***SYSVAL** Viene utilizzato il valore di sistema QPWDEXPITV. **number** La dimensione dell'intervallo di scadenza in giorni.
		984	Blocco modifica parola d'ordine	Char(10)	Specifica il valore in cui è stato modificato il blocco modifica parola d'ordine. ***SYSVAL** Viene utilizzato il valore di sistema QPWDCHGBLK. ***NONE** Nessun periodo di blocco. **1-99** Ore bloccate.

Voci di giornale CQ (Modifiche *CRQD)

Questa tabella fornisce il formato delle voci di giornale CQ (Modifiche *CRQD).

*Tabella 168. Voci di giornale CQ (Modifiche *CRQD).* File descrizione campo QASYCQJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Modifica ad un oggetto *CRQD
157	225	611	Nome oggetto	Char(10)	Il nome dell'oggetto che è stato modificato.
167	235	621	Nome libreria	Char(10)	Il nome della libreria oggetto.
177	245	631	Tipo oggetto	Char(8)	Il tipo di oggetto.
		639	Nome ASP	Char(10)	Nome ASP per libreria CRQD
		649	Numero ASP	Char(5)	Numero ASP per libreria CRQD

Voci di giornale CU (Operazioni cluster)

Questa tabella fornisce il formato delle voci di giornale CU (Operazioni cluster).

Tabella 169. Voci di giornal CU (Operazioni cluster). File descrizione campo QASYCUJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 per l'elenco dei campi.
	224	610	Tipo di voce	Char(1)	Il tipo di voce. **M** Operazione controllo cluster **R** Operazione gestione gruppo risorse cluster (*GRP)

Tabella 169. Voci di giornal CU (Operazioni cluster) (Continua). File descrizione campo QASYCUJ4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
	225	611	Immissione azione	Char(3)	Il tipo di azione. **ADD** Aggiunta **CRT** Creazione **DLT** Cancellazione **DST** Distribuzione **END** Fine **FLO** Fail over **LST** Elenco informazioni **RMV** Eliminazione **STR** Avvio **SWT** Commutazione **UPC** Aggiornamento attributi
	228	614	Stato	Char(3)	Lo stato della richiesta. **ABN** La richiesta ha avuto una fine anomala **AUT** Errore autorizzazione, è necessaria *IOSYSCFG **END** La richiesta è terminata con esito positivo **STR** La richiesta è stata avviata
	231	617	Nome oggetto CRG	Char(10)	Il nome oggetto Gruppo risorse cluster. **Nota:** Questo valore viene compilato quando il tipo di voce è R.
	241	627	Nome libreria CRG	Char(10)	La libreria oggetto Gruppo risorse cluster. **Nota:** Questo valore viene compilato quando il tipo di voce è R.
	251	637	Nome cluster	Char(10)	Il nome del cluster.
	261	647	ID nodo	Char(8)	L'ID del nodo.
	269	655	ID nodo origine	Char(8)	L'ID nodo origine.
	277	663	Nome utente origine	Char(10)	Il nome dell'utente sistema origine che ha iniziato la richiesta.
	287	673	Nome coda utente	Char(10)	Nome della coda utente nella quale vengono inviate le risposte.
	297	683	Libreria coda utente	Char(10)	La libreria della coda utente.
		693	Nome ASP	Char(10)	Nome ASP per la libreria della coda coda utente
		703	Numero ASP	Char(5)	Numero ASP per la libreria della coda utente

Voci di giornale CV (Verifica connessione)

Questa tabella fornisce il formato delle voci di giornale CV (Verifica connessione).

Tabella 170. Voci di giornale CV (Verifica connessione). File descrizione campo QASYCVJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 per l'elenco dei campi.
	224	610	Tipo di voce	Char(1)	Il tipo di voce. **C** Collegamento stabilito **E** Collegamento terminato **R** Collegamento rifiutato
	225	611	Operazione	Char(1)	Operazione intrapresa per il tipo di collegamento. " " Collegamento stabilito o terminato normalmente. Utilizzato per il tipo di voce C o E. **A** Peer non autenticato. Utilizzato per tipo di voce E o R. **C** Nessuna risposta dal server di autenticazione. Utilizzato per il tipo di voce R. **L** Errore di configurazione LCP. Utilizzato per il tipo di voce R. **N** Errore di configurazione NCP. Utilizzato per il tipo di voce R. **P** La parola d'ordine non è valida. Utilizzato per tipo di voce E o R. **R** L'autenticazione è stata rifiutata dal peer. Utilizzato per il tipo di voce R. **T** Errore di configurazione L2TP. Utilizzato per tipo di voce E o R. **U** Utente non valido. Utilizzato per tipo di voce E o R.
	226	612	Nome profilo Point to Point	Char(10)	Il nome profilo point-to-point.
	236	622	Protocollo	Char(10)	Il tipo di voce. **L2TP** Layer Two Tunneling protocol **PPP** Point-to-Point protocol. **SLIP** Serial Line Internet Protocol.

Tabella 170. Voci di giornale CV (Verifica connessione) (Continua). File descrizione campo QASYCVJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	246	632	Metodo di autenticazione locale	Char(10)	Il tipo di voce. **CHAP** Challenge Handshake Authentication Protocol. **PAP** Password Authentication Protocol. **SCRIPT** Metodo script.
	256	642	Metodo di autenticazione remota	Char(10)	Il tipo di voce. **CHAP** Challenge Handshake Authentication Protocol. **PAP** Password Authentication Protocol. **RADIUS** Metodo Radius. **SCRIPT** Metodo script.
	266	652	Nome oggetto	Char(10)	Il nome dell'oggetto *VLDL.
	276	662	Nome libreria	Char(10)	Il nome della libreria dell'oggetto *VLDL.
	286	672	Nome utente *VLDL	Char(100)	Il nome utente *VLDL.
	386	772	Indirizzo IP locale	Char(40)	L'indirizzo IP locale.
	426	812	Indirizzo IP remoto	Char(40)	L'indirizzo IP remoto.
	466	852	Inoltro IP	Char(1)	Il tipo di voce. **Y** L'inoltro IP è attivato. **N** L'inoltro IP è disattivato.

Tabella 170. Voci di giornale CV (Verifica connessione) (Continua). File descrizione campo QASYCVJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	467	853	Proxy ARP	Char(1)	Il tipo di voce. **Y** Il Proxy ARP è abilitato. **N** Il Proxy ARP non è abilitato.
	468	854	Nome radius	Char(10)	Il nome profilo AAA.
	478	864	Indirizzo IP di autenticazione	Char(40)	L'indirizzo IP di autenticazione.
	518	904	ID sessione account	Char(14)	L'ID della sessione account.
	532	918	ID multisessione account	Char(14)	L'ID di più sessioni account.
	546	932	Conteggio collegamenti account	Binary (4)	Il conteggio dei collegamenti account.
	548	934	Tipo tunnel	Char(1)	Il tipo di tunnel: **0** Senza tunnel **3** L2TP **6** AH **9** ESP
	549	935	Endpoint client tunnel	Char(40)	Endpoint client tunnel.
	589	975	Endpoint server tunnel	Char(40)	Endpoint server tunnel.
	629	1015	Ora sessione account	Char(8)	L'ora della sessione account. Utilizzato per tipo di voce E o R.
	637	1023	Riservato	Binary (4)	Sempre zero
		1025	Nome ASP	Char(10)	Nome ASP per libreria elenco di convalida
		1035	Numero ASP	Char(5)	Numero ASP per libreria elenco di convalida

Voci di giornale CY (Configurazione crittografica)

Questa tabella fornisce il formato delle voci di giornale CY (Configurazione crittografica).

Tabella 171. Voci di giornale CY (Configurazione crittografica). File descrizione campo QASYCYJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Funzione controllo accesso di Cryptographic Coprocessor **F** Funzione Facility Control di Cryptographic Coprocessor **K** Funzione chiave principale Cryptographic Services **M** Funzione chiave principale di Cryptographic Coprocessor
	225	611	Operazione	Char(3)	La funzione di configurazione crittografica eseguita: **CCP** Definizione di un profilo scheda. **CCR** Definizione di un ruolo scheda. **CLK** Impostazione orologio. **CLR** Eliminazione chiavi principali. **CRT** Creazione chiavi principali. **DCP** Cancellazione di un profilo scheda. **DCR** Cancellazione di un ruolo scheda. **DST** Distribuzione di chiavi principali. **EID** Impostazione ID ambiente. **FCV** Caricamento o eliminazione FCV. **INI** Reinizializzazione scheda. **LOD** Caricamento chiave principale. **QRY** Query informazioni ruolo o profilo. **RCP** Sostituzione di un profilo scheda. **RCR** Sostituzione di un ruolo scheda. **RCV** Ricezione chiavi principali. **SET** Impostazione chiavi principali. **SHR** Clonazione condivisioni. **TST** Verifica chiave principale.
	228	614	Profilo scheda	Char(8)	Il nome del profilo scheda.[2]

Tabella 171. Voci di giornale CY (Configurazione crittografica) (Continua). File descrizione campo QASYCYJ4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	236	622	Ruolo scheda	Char(8)	Il ruolo del profilo scheda.[2]
	244	630	Nome unità	Char(10)	Il nome dell'unità crittografica.[2]
		640	ID chiave principale[1]	Binary (4)	L'ID chiave principale dei servizi crittografici[3]. Valori possibili sono i seguenti: **-2** Chiave principale di salvataggio/ripristino **-1** Chiave principale ASP **1** Chiave principale 1 **2** Chiave principale 2 **3** Chiave principale 3 **4** Chiave principale 4 **5** Chiave principale 5 **6** Chiave principale 6 **7** Chiave principale 7 **8** Chiave principale 8
		644	Codifica chiave principale	Char(1)	Chiave principale codificata con chiave principale di S/R predefinita. **Y** La chiave principale è stata impostata e codificata con la chiave principale di salvataggio/ripristino predefinita. **N** La chiave principale è stata impostata e codificata con una chiave principale di salvataggio/ripristino impostata dall'utente.
		645	Versione chiave principale	Char(8)	La versione della chiave principale che è stata eliminata. **NEW** La nuova versione è stata eliminata. **CURRENT** La versione corrente è stata eliminata. **OLD** La versione precedente è stata eliminata. **PENDING** La versione in sospeso è stata eliminata.

[1] Quando il tipo di voce è (J5 scostamento 610) K, il profilo della scheda (J5 scostamento 614), il ruolo scheda (J5 offset 622) e il nome dell'unità (J5 scostamento 630) vengono lasciati vuoti.

[2] Quando il tipo di voce è K, questo campo è vuoto.

[3] Quando il tipo di voce non è K, questo campo è vuoto.

Voci di giornale DI (Server indirizzario)

Questa tabella fornisce il formato delle voci di giornale DI (Server indirizzario).

Tabella 172. Voci di giornale DI (Server indirizzario). File descrizione campo QASYDIJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
	224	610	Tipo di voce	Char(1)	Il tipo di voce. **L** Operazione LDAP
	225	611	Tipo di operazione	Char(2)	Il tipo di operazione LDAP: **AD** Modifica attributo controllo. **AF** Errore autorizzazione. **BN** Collegamento con esito positivo. **CA** Modifica autorizzazione oggetto. **CF** Modifica configurazione. **CI** Creazione istanza **CO** Creazione oggetto. **CP** Modifica parola d'ordine. **DI** Cancellazione istanza **DO** Cancellazione oggetto. **EX** Esportazione indirizzario LDAP. **IM** Importazione indirizzario LDAP. **OM** Gestione oggetto (ridenominazione). **OW** Modifica proprietà. **PO** Modifica normativa. **PW** Errore parola d'ordine. **RM** Gestione replica **UB** Scollegamento con esito positivo. **ZC** Modifica oggetto. **ZR** Lettura oggetto.

Tabella 172. Voci di giornale DI (Server indirizzario) (Continua). File descrizione campo QASYDIJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	227	613	Codice errore autorizzazione	Char(1)	Codice per gli errori di autorizzazione. Questo campo viene utilizzato solo se il tipo di operazione (scostamento J5 611) è AF. **A** Tentativo non autorizzato di modificare il valore del controllo. **B** Tentativo non autorizzato di collegamento. **C** Tentativo non autorizzato di creazione oggetto. **D** Tentativo non autorizzato di cancellazione oggetto. **E** Tentativo non autorizzato di esportazione. **F** Modifica non autorizzata alla configurazione (amministratore, registrazione modifiche, libreria di backend, repliche, pubblicazione repliche). **G** Tentativo di gestione replica non autorizzato. **I** Tentativo di importazione non autorizzato. **M** Tentativo di modifica non autorizzato. **P** Tentativo di modifica normativa non autorizzato. **R** Tentativo di lettura non autorizzato (ricerca). **U** Tentativo di lettura configurazione controllo non autorizzato. **X** Tentativo di autorizzazione proxy non autorizzato.

Tabella 172. Voci di giornale DI (Server indirizzario) (Continua). File descrizione campo QASYDIJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	228	614	Modifica configurazione	Char(1)	Modifiche di configurazione. Questo campo viene utilizzato solo se il tipo di operazione (scostamento J5 611) è CF. **A** Modifica ND amministratore. **C** Collegamento/scollegamento modifica. **L** Modifica nome libreria backend. **P** Modifica agent di pubblicazione. **R** Modifica server di replica. Se il tipo di operazione (scostamento J5 611) è RM, potrebbero essere presenti i seguenti valori. **U** Interruzione replica. **V** Ripresa replica. **W** Replica modifiche in sospeso. **X** Ignorare una o più modifiche in sospeso. **Y** Chiusura contesto di replica. **Z** Annullamento chiusura contesto di replica.
	229	615	Codice modifica configurazione	Char(1)	Codice modifiche configurazione. Questo campo viene utilizzato solo se il tipo di operazione (scostamento J5 611) è CF. **A** Voce aggiunta alla configurazione **D** Voce cancellata dalla configurazione **M** Voce modificata
	230	616	Indicatore propagazione	Char(1)	Indica la nuova impostazione del proprietario o del valore di propagazione ACL. Questo campo viene utilizzato solo se il tipo di operazione (scostamento J5 611) è CA o OW. **T** True **F** False
	231	617	Scelta autenticazione collegamento	Char(20)	La scelta dell'autenticazione collegamento. Questo campo viene utilizzato solo se il tipo di operazione (scostamento J5 611) è BN.
	251	637	Versione LDAP	Char(4)	Versione del client che effettua la richiesta. Questo campo viene utilizzato solo se l'operazione è stata eseguita tramite il server LDAP. **2** LDAP Versione 2 **3** LDAP Versione 3

Tabella 172. Voci di giornale DI (Server indirizzario) (Continua). File descrizione campo QASYDIJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	255	641	Indicatore SSL	Char(1)	Indica se è stato utilizzato SSL nella richiesta. Questo campo viene utilizzato solo se l'operazione è stata eseguita tramite il server LDAP. **0** No **1** Sì
	256	642	Tipo di richiesta	Char(1)	Il tipo di richiesta. Questo campo viene utilizzato solo se l'operazione è stata eseguita tramite il server LDAP. **A** Autenticato **N** Anonimo **U** Non autenticato
	257	643	ID collegamento	Char(20)	ID collegamento della richiesta. Questo campo viene utilizzato solo se l'operazione è stata eseguita tramite il server LDAP.
	277	663	Indirizzo IP client	Char(50)	Indirizzo IP e numero porta della richiesta client. Questo campo viene utilizzato solo se l'operazione è stata eseguita tramite il server LDAP.
	327	713	CCSID nome utente	Bin(5)	Il CCSID (coded character set identifier) del nome utente.
	331	717	Lunghezza nome utente	Bin(4)	La lunghezza del nome utente.
	333	719	Nome utente[1]	Char(2002)	Il nome dell'utente LDAP.
	2335	2721	CCSID nome oggetto	Bin(5)	Il CCSID (coded character set identifier) del nome oggetto.
	2339	2725	Lunghezza nome oggetto	Bin(4)	La lunghezza del nome oggetto.
	2341	2727	Nome oggetto[1]	Char(2002)	Il nome dell'oggetto LDAP.
	4343	4729	CCSID nome proprietario	Bin(5)	Il CCSID (coded character set identifier) del nome proprietario. Questo campo viene utilizzato solo se il tipo di operazione (scostamento J5 611) è OW.
	4347	4733	Lunghezza nome proprietario	Bin(4)	La lunghezza del nome proprietario. Questo campo viene utilizzato solo se il tipo di operazione è OW.
	4349	4735	Nome proprietario[1]	Char(2002)	Il nome del proprietario. Questo campo viene utilizzato solo se il tipo di operazione (scostamento J5 611) è OW.

Tabella 172. Voci di giornale DI (Server indirizzario) (Continua). File descrizione campo QASYDIJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	6351	6737	CCSID nuovo nome	Bin(5)	Il CCSID (coded character set identifier) del nuovo nome. Questo campo viene utilizzato solo se il tipo di operazione (scostamento J5 611) è OM, OW, PO, ZC, AF+M o AF+P. • Per il tipo di operazione OM, questo campo conterrà il CCSID del nuovo nome oggetto. • Per il tipo di operazione OW, questo campo conterrà il CCSID del nuovo nome proprietario. • Per tipi di operazione PO, ZC, AF+M, o AF+P, questo campo conterrà il CCSID dell'elenco di tipi di attributo modificati nel campo Nuovo nome.
	6355	6741	Lunghezza nuovo nome	Bin(4)	La lunghezza del nuovo nome. Questo campo viene utilizzato solo se il tipo di operazione (scostamento J5 611) è OM, OW, PO, ZC, AF+M o AF+P. • Per il tipo di operazione OM, questo campo conterrà la lunghezza del nuovo nome oggetto. • Per il tipo di operazione OW, questo campo conterrà la lunghezza del nuovo nome proprietario. • Per tipi di operazione PO, ZC, AF+M, o AF+P, questo campo conterrà la lunghezza dell'elenco di tipi di attributo modificati nel campo Nuovo nome.
	6357	6743	Nome nuovo[1]	Char(2002)	Il nuovo nome. Questo campo viene utilizzato solo se il tipo di operazione (scostamento J5 611) è OM, OW, PO, ZC, AF+M o AF+P. • Per il tipo di operazione OM, questo campo conterrà il nuovo nome oggetto. • Per il tipo di operazione OW, questo campo conterrà il nuovo nome proprietario. • Per tipi di operazione PO, ZC, AF+M, o AF+P, questo campo conterrà un elenco di tipi di attributo modificati.
	8359	8745	ID file oggetto[2]	Char(16)	L'ID file dell'oggetto per l'esportazione.
	8375	8761	Nome ASP[2]	Char(10)	Il nome dell'unità ASP
	8385	8771	Numero ASP[2]	Char(5)	Il numero dell'unità ASP.
	8390	8776	CCSID nome percorso[2]	Bin(5)	Il CCSID (coded character set identifier) del nome percorso.
	8394	8780	ID paese o regione nome percorso[2]	Char(2)	L'ID paese o regione del nome percorso.
	8396	8782	ID lingua nome percorso[2]	Char(3)	L'ID lingua del nome percorso.
	8399	8785	Lunghezza nome percorso[2]	Bin(4)	La lunghezza del nome percorso.

Tabella 172. Voci di giornale DI (Server indirizzario) (Continua). File descrizione campo QASYDIJ4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
	8401	8787	Indicatore nome percorso[2]	Char(1)	Indicatore nome percorso. **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	8402	8788	ID file indirizzario relativo[2,3]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[3]
	8418	8804	Nome percorso[1,2]	Char(5002)	Il nome percorso dell'oggetto.
		13806	Profilo utente locale	Char(10)	Il nome profilo utente locale messo in corrispondenza con il nome utente LDAP (J5 scostamento 719). Uno spazio vuoto indica che non è stato messo in corrispondenza alcun profilo utente.
		13816	Indicatore amministratore	Char(1)	Indicatore amministratore per il nome utente LDAP (J5 scostamento 719). **Y** L'utente LDAP è un amministratore. **N** L'utente LDAP non è un amministratore. **U** Al momento non è possibile sapere se l'utente LDAP è un amministratore.
		13817	CCSID ID proxy	Bin(5)	Il CCSID (coded character set identifier) dell'ID del proxy.
		13821	Lunghezza ID proxy	Bin(4)	La lunghezza dell'ID proxy.
		13823	ID Proxy[1]	Char(2002)	Il nome dell'ID proxy. Questo campo viene utilizzato quando viene utilizzato il controllo di autorizzazione proxy per richiedere che è possibile effettuare un'operazione con l'autorizzazione dell'ID proxy o per un collegamento SASL in cui il client ha specificato un ID di autorizzazione differente dall'ID di collegamento.
		15825	Asserzione gruppo	Char(1)	Asserzione appartenenza gruppo **0** I gruppi non sono stati specificati dal client. **1** I gruppi sono stati specificati dal client.
		15826	Riferimenti incrociati	Char(36)	Stringa riferimenti incrociati utilizzata per mettere in correlazione questa voce con la voce/le voci XD che elencano i gruppi.

Tabella 172. Voci di giornale DI (Server indirizzario) (Continua). File descrizione campo QASYDIJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
		15862	Nome istanza	Char(8)	Nome istanza
		15870	CCSID Instradamento	Bin(5)	CCSID di instradamento
		15874	Lunghezza instradamento	Bin(4)	Lunghezza di instradamento
		15876	Instradamento	Char(502)	Richiesta instradamento

[1] Questo è un campo a lunghezza variabile. I primi due byte contengono la lunghezza del valore nel campo.

[2] Questi campi vengono utilizzati solo se il tipo di operazione (J5 scostamento 611) è EX o IM.

[3] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

Voci di giornale DO (operazione di cancellazione)

Questa tabella fornisce il formato delle voci di giornale DO (operazione di cancellzione).

Tabella 173. Voci di giornale DO (operazione di cancellazione). File descrizione campo QASYDOJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** L'oggetto è stato cancellato senza controllo sincronizzazione **C** Cancellazione oggetto in sospeso sincronizzata **D** La creazione oggetto in sospeso è stata sottoposta a rollback **I** Inizializzazione spazio variabile di ambiente **P** La cancellazione dell'oggetto è in sospeso (la cancellazione è stata eseguita sotto il controllo sincronizzazione) **R** La cancellazione oggetto in sospeso è stata sottoposta a rollback
157	225	611	Nome oggetto	Char(10)	Il nome dell'oggetto.
167	235	621	Nome libreria	Char(10)	Il nome della libreria dove è memorizzato l'oggetto.

Tabella 173. Voci di giornale DO (operazione di cancellazione) (Continua). File descrizione campo QASYDOJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
177	245	631	Tipo oggetto	Char(8)	Il tipo di oggetto.
185	253		(Area riservata)	Char(20)	
		639	Attributo oggetto	Char(10)	L'attributo dell'oggetto.
		649	(Area riservata)	Char(10)	
205	273	659	Utente Office	Char(10)	Il nome dell'utente Office.
215	283	669	Nome DLO	Char(12)	Il nome del DLO (document library object).
227	295	681	(Area riservata)	Char(8)	
235	303	689	Percorso cartella	Char(63)	Il percorso della cartella.
298	366	752	Office per conto dell'utente	Char(10)	Utente che opera per conto di un altro utente.
308			(Area riservata)	Char(20)	
	376	762	(Area riservata)	Char(18)	
	394	780	Lunghezza nome oggetto[1]	Binary (4)	La lunghezza del nome oggetto.
328	396	782	CCSID nome oggetto[1]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
332	400	786	ID paese o regione nome oggetto[1]	Char(2)	L'ID paese o regione per il nome oggetto.
334	402	788	ID lingua nome oggetto[1]	Char(3)	L'ID lingua per il nome oggetto.
337	405	791	(Area riservata)	Char(3)	
340	408	794	ID file principale[1,2]	Char(16)	L'ID file dell'indirizzario principale.
356	424	810	ID file oggetto[1,2]	Char(16)	L'ID file dell'oggetto.
372	440	826	Nome oggetto[1]	Char(512)	Il nome dell'oggetto.
	952	1338	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	968	1354	Nome ASP[5]	Char(10)	Il nome dell'unità ASP
	978	1364	Numero ASP[5]	Char(5)	Il numero dell'unità ASP.
	983	1369	CCSID nome percorso	Binary5)	Il CCSID (coded character set identifier) per il nome percorso.
	987	1373	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.

Tabella 173. Voci di giornale DO (operazione di cancellazione) (Continua). File descrizione campo QASYDOJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
	989	1375	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	992	1378	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.
	994	1380	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	995	1381	ID file indirizzario relativo[3]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[3]
	1011	1397	Nome percorso[4]	Char(5002)	Il nome percorso dell'oggetto.

[1] Questi campi vengono utilizzati solo per oggetti nei file system "root" (/), QOpenSys e negli UDFS (user-defined file systems).

[2] Un ID con il bit all'estrema sinistra impostato ed il resto dei bit zero indica che l'ID NON è impostato.

[3] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[4] Questo è un campo a lunghezza variabile. I primi due byte contengono la lunghezza del nome percorso.

[5] Se l'oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.

Voci di giornale DS (Reimpostazione ID utente programmi di manutenzione forniti da IBM)

Questa tabella fornisce il formato delle voci di giornale DS (Reimpostazione ID utente programmi di manutenzione forniti da IBM).

Tabella 174. Voci di giornale DS (Reimpostazione ID utente programmi di manutenzione forniti da IBM). File descrizione campo QASYDSJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Reimpostazione di una parola d'ordine ID utente programmi di manutenzione. **C** Modificato in un ID utente programmi di manutenzione. **P** La parola d'ordine ID utente programmi di manutenzione è stata modificata.
157	225	611	Reimpostazione ID utente programmi di manutenzione forniti da IBM	Char(1)	**Y** Richiesta di reimpostazione di un ID utente programmi di manutenzione forniti da IBM
158	226	612	Tipo ID utente programmi di manutenzione	Char(10)	Il tipo di ID utente dei programmi di manutenzione ***SECURITY** ***FULL** ***BASIC**
168	236	622	Nuovo nome ID utente programmi di manutenzione	Char(8)	Il nome dell'ID utente dei programmi di manutenzione.
176	244	630	Modifica parola d'ordine ID utente programmi di manutenzione	Char(1)	Richiesta di modifica della parola d'ordine ID utente dei programmi di manutenzione. **Y** Richiesta di modifica della parola d'ordine ID utente dei programmi di manutenzione.
	245	631	Nuovo nome ID utente programmi di manutenzione	Char(10)	Il nome dell'ID utente dei programmi di manutenzione.
	255	641	Profilo richiedente ID utente programmi di manutenzione	Char(10)	Il nome dell'ID utente dei programmi di manutenzione che ha richiesto la modifica.

Voci di giornale EV (Variabile d'ambiente)

Questa tabella fornisce il formato delle voci di giornale EV (Variabile d'ambiente).

Tabella 175. Voci di giornale EV (Variabile d'ambiente). File descrizione campo QASYEVJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Aggiunta **C** Modifica **D** Cancellazione **I** Inizializzazione spazio variabile d'ambiente
	225	611	Nome troncato	Char(1)	Indica se il nome della variabile d'ambiente (scostamento 232) è troncato. **Y** Nome della variabile d'ambiente troncato. **N** Nome della variabile d'ambiente non troncato.
	226	612	CCSID	Binary(5)	Il CCSID il nome della variabile d'ambiente.
	230	616	Lunghezza	Binary (4)	La lunghezza del nome variabile d'ambiente.
	232	618	Nome variabile ambiente[2]	Char(1002)	Il nome della variabile ambiente.
	1234	1620	Nuovo nome troncato[1]	Char(1)	Indica se il nuovo nome della variabile di ambiente (scostamento 1241) è troncato. **Y** Valore variabile ambiente troncato. **N** Valore della variabile d'ambiente non troncato.
	1235	1621	CCSID nuovo nome[1]	Binary(5)	Il CCSID il nuovo nome variabile ambiente.
	1239	1625	Lunghezza nuovo nome[1]	Binary (4)	La lunghezza del nuovo nome variabile ambiente.
	1241	1627	Nuovo nome variabile ambiente[1,2]	Char (1002)	Il nuovo nome variabile ambiente.

[1] Questi campi sono utilizzati quando il tipo di voce è C.

[2] Questo è un campo a lunghezza variabile. I primi due byte contengono la lunghezza del nome variabile ambiente.

Voci di giornale GR (Record generico)

Questa tabella fornisce il formato delle voci di giornale GR (Record generico).

Tabella 176. Voci di giornale GR (Record generico). File descrizione campo QASYGRJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 per l'elenco dei campi.
	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Aggiunto programma di uscita **C** Operazioni monitoraggio risorsa e operazioni controllo **D** Programma di uscita rimosso **F** Operazioni registrazione funzione **R** Programma di uscita sostituito
	225	611	Operazione	Char(2)	L'operazione eseguita. **ZC** Modifica **ZR** Lettura
	227	613	Nome utente	Char(10)	Nome profilo utente Per il tipo di voce F, questo campo contiene il nome dell'utente rispetto al quale è stata eseguita l'operazione di registrazione.
	237	623	CCSID campo 1	Binary(5)	Il valore CCSID per il campo 1.
	241	627	Lunghezza campo 1	Binary (4)	La lunghezza dei dati nel campo 1.

Tabella 176. Voci di giornale GR (Record generico) (Continua). File descrizione campo QASYGRJ4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	243	629	Campo 1	Char(102)[1]	Dati campo 1 Per il tipo di voce F, questo campo contiene la descrizione dell'operazione di registrazione funzione che è stata eseguita. Valori possibili: ***REGISTER:** Funzione registrata ***REREGISTER:** Funzione aggiornata ***DEREGISTER:** Registrazione funzione annullata ***CHGUSAGE:** Informazioni di utilizzo funzione modificate ***CHKUSAGE:** Utilizzo funzione controllato per un utente e controllo superato ***USAGEFAILURE:** Utilizzo funzione controllato per un utente e controllo non superato Per tipi di voce A, D e R, questo campo conterrà le informazioni sul programma di uscita per la specifica funzione eseguita. Per il tipo di voce C, questo campo contiene il nome della funzione RMC che si sta tentando. Valori possibili: • **mc_reg_event_select** Registrare l'evento con la selezione attributo • **mc_reg_event_handle** Registrare l'evento utilizzando la gestione risorsa • **mc_reg_class_event** Registrare l'evento per una classe risorse • **mc_unreg_event** Annullare la registrazione dell'evento • **mc_define_resource** Definire una nuova risorsa • **mc_undefine_resource** Annullare la definizione della risorsa • **mc_set_select** Impostare i valori attributo risorsa con la selezione attributo • **mc_set_handle** Impostare i valori attributo risorsa utilizzando la gestione risorsa • **mc_class_set** Impostare i valori attributo classe risorse • **mc_query_p_select** Eseguire la query degli attributi persistenti della risorsa con la selezione attributo • **mc_query_d_select** Eseguire la query degli attributi dinamici della risorsa con la selezione attributo

Tabella 176. Voci di giornale GR (Record generico) (Continua). File descrizione campo QASYGRJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
243 (cont)					• **mc_query_p_handle** Eseguire la query degli attributi persistenti della risorsa utilizzando la gestione risorsa **mc_query_d_handle** Eseguire la query degli attributi dinamici della risorsa utilizzando la gestione risorsa **mc_class_query_p** Eseguire la query degli attributi persistenti della classe risorse **mc_class_query_d** Eseguire la query degli attributi dinamici della classe risorse **mc_qdef_resource_class** Eseguire la query della definizione classe risorse **mc_qdef_p_attribute** Eseguire la query della definizione attributo persistente **mc_qdef_d_attribute** Eseguire la query della definizione attributo dinamico **mc_qdef_sd** Eseguire la query della definizione dati strutturati **mc_qdef_valid_values** Eseguire la query della definizione dei valori validi di un attributo persistente **mc_qdef_actions** Eseguire la query della definizione delle operazioni di una risorsa **mc_invoke_action** Richiamare operazione su una risorsa **mc_invoke_class_action** Richiamare operazione su una classe risorse
	345	731	CCSID campo 2	Binary(5)	Il valore CCSID per il campo 2.
	349	735	Lunghezza campo 2	Binary (4)	La lunghezza dei dati nel campo 2.
	351	737	Campo 2	Char (102)[1]	Dati campo 2 Per il tipo di voce F, questo campo contiene il nome della funzione su cui si è operato. Per il tipo di voce C, questo campo contiene il nome della risorsa o della classe di risorse rispetto a cui è stata tentata l'operazione.
	453	839	CCSID campo 3	Binary(5)	Il valore CCSID per il campo 3.
	457	843	Lunghezza campo 3	Binary (4)	La lunghezza dei dati nel campo 3.

Tabella 176. Voci di giornale GR (Record generico) (Continua). File descrizione campo QASYGRJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	459	845	Campo 3	Char(102)[1]	Dati campo 3. Per il tipo di voce F, questo campo contiene l'impostazione di utilizzo per un utente. Esiste un valore per questo campo solo se l'operazione di registrazione della funzione è uno dei seguenti valori: ***REGISTER:** Quando l'operazione è *REGISTER, questo campo contiene il valore di utilizzo predefinito. Il nome utente sarà *DEFAULT. ***REREGISTER:** Quando l'operazione è *REREGISTER, questo campo contiene il valore di utilizzo predefinito. Il nome utente sarà *DEFAULT. ***CHGUSAGE:** Quando l'operazione è *CHGUSAGE, questo campo contiene il valore di utilizzo per l'utente specificato nel campo nome utente. Per il tipo di voce C, questo campo contiene il risultato di qualsiasi controllo di autorizzazione effettuato per l'operazione indicata nel campo 1. I seguenti sono possibili valori: • *NOAUTHORITYCHECKED: quando l'operazione indicata nel campo 1 non richiede un controllo dell'autorizzazione o se per qualsiasi altra ragione non è stato tentato un controllo dell'autorizzazione. • *AUTHORITYPASSED: quando l'ID utente definito indicato nel Nome profilo utente ha superato con esito positivo il controllo autorizzazione appropriato per l'operazione indicata nel campo 1 rispetto alla risorsa o classe di risorse indicata nel campo 2. • *AUTHORITYFAILED: quando l'ID utente definito indicato nel Nome profilo utente non ha superato il controllo autorizzazione appropriato per l'operazione indicata nel campo 1 rispetto alla risorsa o classe di risorse indicata nel campo 2.
	561	947	CCSID campo 4	Binary(5)	Il valore CCSID per il campo 4.
	565	951	Lunghezza campo 4	Binary (4)	La lunghezza dei dati nel campo 4.

Tabella 176. Voci di giornale GR (Record generico) (Continua). File descrizione campo QASYGRJ4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
	567	953	Campo 4	Char(102)[1]	Dati campo 4. Per il tipo di voce F, questo campo contiene l'impostazione *ALLOBJ consentita per la funzione. Esiste un valore per questo campo solo se l'operazione di registrazione della funzione è uno dei seguenti valori: ***REGISTER** ***REREGISTER**

[1] Questo è un campo a lunghezza variabile. I primi due byte contengono la lunghezza del campo.

Voci di giornale GS (Fornire descrittore)

Questa tabella fornisce il formato delle voci di giornale GS (Fornire descrittore).

Tabella 177. Voci di giornale GS (Fornire descrittore). File descrizione campo QASYGSJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **G** Assegnazione identificativo **R** Identificativo ricevuto **U** Impossibile utilizzare identificativo
157	225	611	Nome lavoro	Char(10)	Il nome del lavoro.
167	235	621	Nome utente	Char(10)	Il nome dell'utente.
177	245	631	Numero lavoro	Zoned(6,0)	Il numero del lavoro.
183	251	637	Nome profilo utente	Char(10)	Il nome del profilo utente.
	261	647	JUID	Char(10)	L'ID utente lavoro del lavoro di destinazione. (Questo valore si applica solo a record di controllo sottotipo G.)

Voci di giornale IM (Monitoraggio intrusione)

Questa tabella fornisce il formato delle voci di giornale IM (Monitoraggio intrusione).

Tabella 178. Voci di giornale IM (Monitoraggio intrusione). File descrizione campo QASYIMJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
		1			Campi intestazione comuni a tutti i tipi di voce
		610	Tipo di voce	Char(1)	Il tipo di voce. **P** Rilevato potenziale evento di intrusione
		611	Ora evento	TIMESTAMP	L'ora in cui l'evento è stato rilevato, in formato della registrazione data/ora SAA.
		637	Identificativo punto di rilevazione	Char(4)	Un identificativo univoco per l'ubicazione di elaborazione che ha rilevato l'evento di intrusione. Questo campo è pensato per essere utilizzato da parte del personale di assistenza.
		641	Famiglia indirizzi locali	Char(1)	Famiglia di indirizzi IP locali associati con l'evento rilevato.
		642	Numero porta locale	Zone(5, 0)	Numero porta locale associato all'evento rilevato.
		647	Indirizzo IP locale	Char(46)	Indirizzo IP locale associato all'evento rilevato.
		693	Famiglia indirizzi remoti	Char(1)	Famiglia di indirizzi remoti associati all'evento rilevato.
		694	Numero porta remota	Zoned(5, 0)	Numero porta remoto associato all'evento rilevato.
		699	Indirizzo IP remoto	Char(46)	Indirizzo IP remoto associato all'evento rilevato.
		745	Identificativo del tipo di sonda	Char(6)	Identifica il tipo di sonda utilizzato per rilevare la potenziale intrusione. Valori possibili sono i seguenti: **ATTACK** Evento rilevato azione di attacco **TR-TCP** Evento rilevato su TCP azione di regolamento del traffico **TR-UDP** Evento rilevato su UDP azione di regolamneto del traffico **SCANE** Evento rilevato azione evento di scansione **SCANG** Evento rilevato azione globale di scansione **XATTACK** Possibile attacco estrusione **XTRTCP** Evento rilevato (TCP) TR in uscita **XTRUDP** Evento rilevato (UDP) TR in uscita **XSCAN** Evento rilevato scansione in uscita

Tabella 178. Voci di giornale IM (Monitoraggio intrusione) (Continua). File descrizione campo QASYIMJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
		751	Correlatore evento	Char(4)	Identificativo univoco per questo specifico evento di intrusione. È possibile utilizzare questo identificativo per mettere in correlazione questo record di controllo con altre informazioni di rilevazione intrusione.
		755	Tipo di evento	Char(8)	Identifica il tipo intrusione potenziale rilevato. Valori possibili: **ACKSTORM** TCP ACK storm **ADRPOISN** Danneggiamento indirizzi **FLOOD** Evento di allagamento **FRAGGLE** Attacco Fraggle **ICMPRED** Reindirizzamento ICMP (Internet Control Message Protocol) **IPFRAG** Frammento IP **MALFPKT** Pacchetto specificato in modo errato **OUTRAW** attacco pacchetto grezzo in uscita **PERPECH** Echo perpetuo **PNGDEATH** Ping of death **RESTOPT** Opzioni IP limitate **RESTPROT** Protocollo IP limitato **SMURF** Attacco smurf
		763	Protocollo	Char(3)	Numero protocollo
		766	Condizione	Char(4)	Numero condizione da file normativa IDS
		770	Filtraggio	Char(1)	• 0 = non attivo • 1 = attivo
		771	Pacchetti scartati	Zoned(5,0)	Numero di pacchetti scartati quando filtrato
		776	Stack TCP/IP di destinazione	Char(1)	**P** Stack produzione **S** Stack servizio
		777	Riservato	Char(6)	Riservato per utilizzo futuro

Tabella 178. Voci di giornale IM (Monitoraggio intrusione) (Continua). File descrizione campo QASYIMJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
		783	Pacchetto sospetto	Char(1002)[1]	Un campo a lunghezza variabile può contenere fino ai primi 1000 byte del pacchetto IP associato all'evento rilevato. Questo campo contiene dati binari che dovrebbero essere trattati come se disponessero di un CCSID 65 535.

[1] Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza delle informazioni del pacchetto sospetto.

Voci di giornale IP (Comunicazione tra processi)

Questa tabella fornisce il formato delle voci di giornale IM (Monitoraggio intrusione).

Tabella 179. Voci di giornale IP (Comunicazione tra processi). File descrizione campo QASYIPJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Modifiche proprietà e/o autorizzazione **C** Creazione **D** Cancellazione **F** Errore autorizzazione **G** Assegnazione **M** Collegamento memoria condivisa **Z** Chiusura segnalatore normale o scollegamento memoria condivisa
157	225	611	Tipo IPC	Char(1)	Tipo IPC **M** Memoria condivisa **N** Segnalatore normale **Q** Coda messaggi **S** Segnalatore
158	226	612	Gestione IPC	Binary(5)	ID gestione IPC
162	230	616	Nuovo proprietario	Char(10)	Nuovo proprietario dell'entità IPC

Tabella 179. Voci di giornale IP (Comunicazione tra processi) (Continua). File descrizione campo QASYIPJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
172	240	626	Vecchio proprietario	Char(10)	Vecchio proprietario dell'entità IPC
182	250	636	Autorizzazione proprietario	Char(3)	Autorizzazione del proprietario all'entità IPC ***R** lettura ***W** scrittura ***RW** lettura e scrittura
185	253	639	Nuovo gruppo	Char(10)	Gruppo associato all' entità IPC
195	263	649	Vecchio gruppo	Char(10)	Precedente gruppo associato all'entità IPC
205	273	659	Autorizzazione gruppo	Char(3)	Autorizzazione del gruppo all'entità IPC ***R** lettura ***W** scrittura ***RW** lettura e scrittura
208	276	662	Autorizzaz. pubblica	Char(3)	Autorizzazione degli utenti pubblici all'entità IPC ***R** lettura ***W** scrittura ***RW** lettura e scrittura
211	279	665	Nome del segnalatore CCSID	Binary(5)	Il CCSID del nome del segnalatore.
216	283	669	Lunghezza nome segnalatore	Binary (4)	La lunghezza del nome segnalatore.
218	285	671	Nome segnalatore	Char(2050)	Il nome del segnalatore. **Nota:** Questo è un campo a lunghezza variabile. I primi due caratteri contengono la lunghezza del nome del segnalatore.

Voci di giornale IR (Azioni regole IP)

Questa tabella fornisce il formato delle voci di giornale IR (Azioni regole IP).

Tabella 180. Voci di giornale IR (Azioni regole IP). File descrizione campo QASYIRJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 per l'elenco dei campi.

Tabella 180. Voci di giornale IR (Azioni regole IP) (Continua). File descrizione campo QASYIRJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	224	610	Tipo di voce	Char(1)	Il tipo di voce. **L** Regole IP caricate da un file. **N** Regole IP scaricate per un collegamento Sicurezza IP **P** Regole IP caricate per un collegamento Sicurezza IP **R** Regole IP lette o copiate su un file. **U** Regole IP scaricate (rimosse).
	225	611	Nome file	Char(10)	Il nome del file QSYS utilizzato per caricare o ricevere le regole IP. Questo valore è vuoto se il file utilizzato non era nel file system QSYS.
	235	621	Libreria file	Char(10)	Il nome della libreria file QSYS.
	245	631	Riservato	Char(18)	
	263	649	Lunghezza nome file	Binary (4)	La lunghezza del nome file.
	265	651	CCSID nome file[1]	Binary(5)	Il CCSID (coded character set identifier) per il nome file.
	269	655	ID paese o regione file[1]	Char(2)	L'ID paese o regione per il nome file.
	271	657	ID lingua file[1]	Char(3)	L'ID lingua per il nome file.
	274	660	Riservato	Char(3)	
	277	663	ID file principale[1, 2]	Char(16)	L'ID file dell'indirizzario principale.
	293	679	ID file oggetto[1, 2]	Char(16)	L'ID file del file.
	309	695	Nome file[1]	Char(512)	Il nome del file.
	821	1207	Sequenza collegamento	Char(40)	Il nome del collegamento.
	861	1247	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	877	1263	Nome ASP	Char(10)	Il nome dell'unità ASP
	887	1273	Numero ASP[5]	Char(5)	Il numero dell'unità ASP.
	892	1278	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	896	1282	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	898	1284	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	901	1287	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.

Tabella 180. Voci di giornale IR (Azioni regole IP) (Continua). File descrizione campo QASYIRJ4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
	903	1289	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	904	1290	ID file indirizzario relativo[3]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[3]
	920	1306	Nome percorso[4]	Char(5002)	Il nome percorso dell'oggetto.

[1] Questi campi vengono utilizzati solo per oggetti nei file system "root" (/), QOpenSys e negli UDFS (user-defined file system).

[2] Se l'ID ha il bit all'estrema sinistra impostato ed il resto dei bit hanno valore zero, l'ID non è impostato.

[3] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[4] Questo è un campo a lunghezza variabile. I primi due byte contengono la lunghezza del campo.

[5] Se l'oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.

Voci di giornale IS (Gestione sicurezza Internet)

Questa tabella fornisce il formato delle voci di giornale IS (Gestione sicurezza Internet).

Tabella 181. Voci di giornale IS (Gestione sicurezza Internet). File descrizione campo QASYISJ4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 per l'elenco dei campi.

Tabella 181. Voci di giornale IS (Gestione sicurezza Internet) (Continua). File descrizione campo QASYISJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Errore (questo tipo non viene più utilizzato) **C** Normale (questo tipo non viene più utilizzato) **U** Utente mobile (questo tipo non viene più utilizzato) **1** Negoziato IKE Phase 1 SA **2** Negoziato IKE Phase 2 SA
	225	611	Indirizzo IP locale[1]	Char(15)	Indirizzo IP locale.
	240	626	Porta ID client locale	Char(5)	Porta ID client locale
	245	631	Indirizzo IP remoto[1]	Char(15)	Indirizzo IP remoto.
	260	646	Porta ID client remoto	Char(5)	Porta ID client remoto (valida per la fase 2).
	265	651	Famiglia di indirizzi IP locali	Char (1)	Famiglia di indirizzi IP locali **4** IPv4 **6** IPv6
		652	Indirizzo IP locale	Char (46)	Indirizzo IP locale
		698	Famiglia di indirizzi IP remoti	Char (1)	Famiglia di indirizzi IP remoti **4** IPv4 **6** IPv6
		699	Indirizzo IP remoto	Char (46)	Indirizzo IP remoto
		745	Riservato	Char (162)	Riservato
	521	907	Codice risultato	Char(4)	Risultato negoziato: **0** Esito positivo **1–30** Errori specifici del protocollo (documentati in ISAKMP RFC2408, reperibile all'indirizzo: http://www.ietf.org) **82xx** Errori specifici VPN Key Manager
	525	911	CCSID	Bin(5)	Il CCSID (coded character set identifier) per i seguenti campi: • ID locale • Valore ID client locale • ID remoto • Valore ID client remoto
	529	915	ID locale	Char(256)	Identificativo IKE locale

Tabella 181. Voci di giornale IS (Gestione sicurezza Internet) (Continua). File descrizione campo QASYISJ4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	785	1171	Tipo ID client locale	Char(2)	Tipo di ID client (valido per la fase 2): **1** Indirizzo IP versione 4 **2** Nome dominio completo **3** Nome dominio completo utente **4** Sottorete IP versione 4 **5** Indirizzo IP versione 6 **6** Sottorete IP versione 6 **7** Intervallo indirizzi IP versione 4 **8** Intervallo Indirizzo IP versione 6 **9** DN (Distinguished name) **11** Identificativo chiave
	787	1173	Valore ID client locale	Char(256)	ID client locale (valido per la fase 2)
	1043	1429	Protocollo ID client locale	Char(4)	Protocollo ID client locale (valido per la fase 2)
	1047	1433	ID remoto	Char(256)	Identificativo IKE remoto
	1303	1689	Tipo ID client remoto	Char(2)	Tipo di ID client (valido per la fase 2) **1** Indirizzo IP versione 4 **2** Nome dominio completo **3** Nome dominio completo utente **4** Sottorete IP versione 4 **5** Indirizzo IP versione 6 **6** Sottorete IP versione 6 **7** Intervallo indirizzi IP versione 4 **8** Intervallo Indirizzo IP versione 6 **9** DN (Distinguished name) **11** Identificativo chiave
	1305	1691	Valore ID client remoto	Char(256)	ID client remoto (valido per la fase 2)
	1561	1947	Protocollo ID client remoto	Char(4)	Protocollo ID client remoto (valido per la fase 2)
[1] Questo campo supporta indirizzi IPv4.					

Voci di giornale JD (Modifica descrizione lavoro)

Questa tabella fornisce il formato delle voci di giornale JD (Modifica descrizione lavoro).

Tabella 182. Voci di giornale JD (Modifica descrizione lavoro). File descrizione campo QASYJDJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Profilo utente specificato per il parametro USER di una descrizione lavoro
157	225	611	Descrizione lavoro	Char(10)	Il nome della descrizione lavoro per cui è stato modificato il parametro USER.
167	235	621	Nome libreria	Char(10)	Il nome della libreria dove è memorizzato l'oggetto.
177	245	631	Tipo oggetto	Char(8)	Il tipo di oggetto.
185	253	639	Tipo comando	Char(3)	Il tipo di comando utilizzato. **CHG** Comando CHGJOBD (Modifica descrizione lavoro). **CRT** Comando CRTJOBD (Creazione descrizione lavoro).
188	256	642	Vecchio utente	Char(10)	Il nome del profilo utente specificato per il parametro USER prima che la descrizione venisse modificata.
198	266	652	Nuovo utente	Char(10)	Il nome del profilo USER specificato per il parametro utente quando la descrizione lavoro è stata modificata.
		662	Nome ASP	Char(10)	Nome ASP per la libreria JOBD
		672	Numero ASP	Char(5)	Numero ASP per la libreria JOBD

Voci di giornale JS (Modifica lavoro)

Questa tabella fornisce il formato delle voci di giornale JS (Modifica lavoro) .

Tabella 183. Voci di giornale JS (Modifica lavoro). File descrizione campo QASYJSJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** comando ENDJOBABN **B** Inoltro **C** Modifica **E** Fine **H** Congelamento **I** Scollegamento **J** Il lavoro corrente sta tentando di interrompere un altro lavoro **K** Il lavoro corrente sta per essere interrotto **L** L'interruzione del lavoro corrente è stato completato **M** Modifica profilo o profilo gruppo **N** Comando ENDJOB **P** Collegamento lavoro di preavvio o lavoro immediato batch **Q** Modifica attributi query **R** Rilascio **S** Avvio **T** Modifica profilo o profilo gruppo utilizzando un token profilo **U** CHGUSRTRC **V** Unità virtuale modificata dall'API QWSACCDS.

Tabella 183. Voci di giornale JS (Modifica lavoro) (Continua). File descrizione campo QASYJSJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
157	225	611	Tipo lavoro	Char(1)	Il tipo di lavoro. **A** Avvio automatico **B** Batch **I** Interattivo **M** Monitor sottosistema **R** Programma di lettura **S** Sistema **W** Programma di scrittura **X** SCPF
158	226	612	Sottotipo lavoro	Char(1)	Il sottotipo del lavoro. **' '** Nessun sottotipo **D** Immediato batch **E** Richiesta procedura di avvio **J** Preavvio **P** Stampa driver unità **Q** Query **T** MRT **U** Utente spool alternativo
159	227	613	Nome lavoro	Char(10)	La prima parte del nome lavoro completo su cui si opera
169	237	623	Nome utente lavoro	Char(10)	La seconda parte del nome lavoro completo su cui si opera
179	247	633	Numero lavoro	Char(6)	La terza parte del nome lavoro completo su cui si opera
185	253	639	Nome unità	Char(10)	Il nome dell'unità
195	263	649	Profilo utente valido[2]	Char(10)	Il nome del profilo utente valido per il sottoprocesso
205	273	659	Nome descrizione lavoro	Char(10)	Il nome della descrizione lavoro per il lavoro
215	283	669	Libreria descrizione lavoro	Char(10)	Il nome della libreria per la descrizione lavoro
225	293	679	Nome coda lavori	Char(10)	Il nome della coda lavori per il lavoro
235	303	689	Libreria coda lavori	Char(10)	Il nome della libreria per la coda lavori
245	313	699	Nome coda di emissione	Char(10)	Il nome della coda di emissione per il lavoro
255	323	709	Libreria coda di emissione	Char(10)	Il nome della libreria per la coda di emissione

Tabella 183. Voci di giornale JS (Modifica lavoro) (Continua). File descrizione campo QASYJSJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
265	333	719	Unità stampante	Char(10)	Il nome dell'unità stampante per il lavoro
275	343	729	Elenco librerie[2]	Char(430)	L'elenco librerie per il lavoro
705	773	1159	Nome profilo gruppo effettivo[2]	Char(10)	Il nome del profilo gruppo effetivo per il sottoprocesso
715	783	1169	Profili gruppo supplementari[2]	Char(150)	I nomi dei profili gruppo supplementari per il sottoprocesso.
	933	1319	Descrizione JUID	Char(1)	Descrive il significato del campo JUID: ' ' Il campo JUID contiene il valore per JOB. **C** È stata chiamata l'API Eliminazione JUID. Il campo JUID contiene il nuovo valore. **S** È stata chiamata l'API Impostazione JUID. Il campo JUID contiene il nuovo valore.
	934	1320	Campo JUID	Char(10)	Contiene il valore JUID
	944	1330	Profilo utente reale	Char(10)	Il nome del profilo utente reale per il sottoprocesso.
	954	1340	Profilo utente salvato	Char(10)	Il nome del profilo utente salvato per il sottoprocesso.
	964	1350	Profilo gruppo reale	Char(10)	Il nome del profilo gruppo reale per il sottoprocesso
	974	1360	Profilo gruppo salvato	Char(10)	Il nome del profilo gruppo salvato per il sottoprocesso.
	984	1370	Utente reale modificato[3]	Char(1)	Il profilo utente reale è stato modificato. **Y** Sì **N** No
	985	1371	Utente valido modificato[3]	Char(1)	Il profilo utente valido è stato modificato. **Y** Sì **N** No
	986	1372	Utente salvato modificato[3]	Char(1)	Il profilo utente salvato è stato modificato **Y** Sì **N** No
	987	1373	Gruppo reale modificato[3]	Char(1)	Il profilo gruppo reale è stato modificato. **Y** Sì **N** No
	988	1374	Gruppo effettivo modificato[3]	Char(1)	Il profilo gruppo effettivo è stato modificato **Y** Sì **N** No

Tabella 183. Voci di giornale JS (Modifica lavoro) (Continua). File descrizione campo QASYJSJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	989	1375	Gruppo salvato modificato[3]	Char(1)	Il profilo gruppo salvato è stato modificato. **Y** Sì **N** No
	990	1376	Gruppi supplementari modificati[3]	Char(1)	I profili gruppo supplementari sono stati modificati. **Y** Sì **N** No
	991	1377	Numero elenco librerie[4]	Bin(4)	Il numero di librerie nel campo estensione elenco librerie (scostamento 993).
	993	1379	Estensione elenco librerie[4,5]	Char(2252)	L'estensione nell'elenco librerie per il lavoro.
		3631	Gruppo ASP libreria	Char(10)	Gruppo ASP libreria
		3641	Nome ASP	Char(10)	Nome ASP per la libreria JOBD
		3651	Numero ASP	Char(5)	Numero ASP per la libreria JOBD
		3656	Nome fuso orario	Char(10)	Il nome di descrizione del fuso orario
		3666	Nome lavoro di uscita	Char(10)	Il nome del lavoro che ha interrotto il lavoro corrente o il nome del lavoro che è stato interrotto dal lavoro corrente
		3676	Utente lavoro di uscita	Char(10)	L'utente del lavoro che ha interrotto il lavoro corrente o l'utente del lavoro che è stato interrotto dal lavoro corrente
		3686	Numero lavoro di uscita[6, 7]	Char(6)	Il numero del lavoro che ha interrotto il lavoro corrente o il numero del lavoro che è stato interrotto dal lavoro corrente
		3692	Nome programma di uscita[6]	Char(10)	Il programma di uscita utilizzato per interrompere il lavoro
		3702	Libreria programma di uscita[6]	Char(10)	Il nome libreria del programma di uscita utilizzato per interrompere il lavoro
		3712	Nome ASP libreria JOBQ	Char(10)	Nome ASP per la libreria JOBQ
		3722	Numero ASP libreria JOBQ	Char(5)	Numero ASP della libreria JOBQ

Tabella 183. Voci di giornale JS (Modifica lavoro) (Continua). File descrizione campo QASYJSJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
[1]	Questo campo è vuoto se il lavoro si trova nella coda lavori e non è stato eseguito.				
[2]	Quando viene creato il record di controllo JS poiché un lavoro esegue un'operazione su un altro lavoro questo campo conterrà dati dal sottoprocesso iniziale del lavoro su cui si sta operando. In tutti gli altri casi, il campo conterrà i dati dal sottoprocesso che ha eseguito l'operazione.				
[3]	Questo campo viene utilizzato solo quando il tipo di voce (scostamento 610) è M o T.				
[4]	Questo campo viene utilizzato solo se il numero di librerie nell'elenco librerie supera la dimensione del campo allo scostamento 729.				
[5]	Questo è un campo a lunghezza variabile. I primi due byte contengono la lunghezza dei dati nel campo.				
[6]	Questo campo viene utilizzato solo quando il tipo di voce (scostamento 610) è J, K o L.				
[7]	Quando il tipo di voce è J, questo campo contiene informazioni sul lavoro che è stato interrotto. Quando il tipo di voce è K, questo campo contiene informazioni sul lavoro che ha richiesto l'interruzione del lavoro corrente.				

Voci di giornale KF (File key ring)

Questa tabella fornisce il formato delle voci di giornale KF (File Key Ring).

Tabella 184. Voci di giornale KF (File key ring). File descrizione campo QASYKFJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 per l'elenco dei campi.
	224	610	Tipo di voce	Char(1)	Il tipo di voce. **C** Operazione certificato **K** Operazione file key ring **P** Parola d'ordine non corretta **T** Operazione root garantita
	225	611	Operazione certificato	Char(3)	Tipo di azione[4]. **ADK** Aggiunto certificato con chiave privata **ADD** Aggiunto certificato **REQ** Certificato richiesto **SGN** Certificato firmato

Tabella 184. Voci di giornale KF (File key ring) (Continua). File descrizione campo QASYKFJ4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
	228	614	Operazione Key Ring	Char(3)	Tipo di azione[5]. **ADD** Aggiunta coppia key ring **DFT** Coppia key ring designata come valore predefinito. **EXP** Coppia key ring esportata **IMP** Coppia key ring importata **LST** Elenco delle etichette coppia key ring in un file **PWD** Modifica parola d'ordine file key ring **RMV** Coppia key ring eliminata **INF** Richiamo informazioni coppia key ring **2DB** File key ring convertito in formato file database chiavi **2YR** File database chiavi convertito in file key ring
	231	617	Operazione root garantita	Char(3)	Tipo di azione[6]. **TRS** Coppia key ring designata come root garantita **RMV** Designazione root garantita eliminata **LST** Elenco root garantite
	234	620	Riservato	Char(18)	
	252	638	Lunghezza nome oggetto	Binary (4)	Lunghezza nome file key ring.
	254	640	CCSID nome oggetto	Binary(5)	CCSID nome file key ring.
	258	644	ID paese o regione nome oggetto	Char(2)	ID paese o regione nome file key ring.
	260	646	ID lingua nome oggetto	Char(3)	ID lingua nome file key ring.
	263	649	Riservato	Char(3)	
	266	652	ID file principale	Char(16)	ID file indirizzario principale key ring.
	282	668	ID file oggetto	Char(16)	Nome file indirizzario key ring.
	298	684	Nome oggetto	Char(512)	Nome file key ring.
	810	1196	Riservato	Char(18)	
	828	1214	Lunghezza nome oggetto	Binary (4)	Lunghezza nome file origine o destinazione.
	830	1216	CCSID nome oggetto	Binary(5)	CCSID nome file origine o destinazione.

Tabella 184. Voci di giornale KF (File key ring) (Continua). File descrizione campo QASYKFJ4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	834	1220	ID paese o regione nome oggetto	Char(2)	ID paese o regione nome file origine o destinazione.
	836	1222	ID lingua nome oggetto	Char(3)	ID lingua nome file origine o destinazione.
	839	1225	Riservato	Char(3)	
	842	1228	ID file principale	Char(16)	ID file indirizzario principale origine o destinazione.
	858	1244	ID file oggetto	Char(16)	ID file indirizzario origine o destinazione.
	874	1260	Nome oggetto	Char(512)	Nome file origine o destinazione.
	1386	1772	Lunghezza etichetta certificato	Binary (4)	La lunghezza dell'etichetta certificato.
	1388	1774	Etichetta certificato[1]	Char(1026)	L'etichetta certificato.
	2414	2800	ID file oggetto	Char(16)	L'ID file del file key ring.
	2430	2816	Nome ASP	Char(10)	Il nome dell'unità ASP
	2440	2826	Numero ASP	Char(5)	Il numero dell'unità ASP.
	2445	2831	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
|	2449	2835	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
|	2451	2837	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
|	2454	2840	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.
	2456	2842	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per il file key ring. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	2457	2843	ID file indirizzario relativo[2]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[2]
	2473	2859	Nome percorso assoluto[1]	Char(5002)	Il nome percorso assoluto del file key ring.

Tabella 184. Voci di giornale KF (File key ring) (Continua). File descrizione campo QASYKFJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	7475	7861	ID file oggetto	Char(16)	L'ID file del file origine o destinazione.
	7491	7877	Nome ASP	Char(10)	Nome ASP del file origine o destinazione
	7501	7887	Numero ASP	Char(5)	Numero ASP del file origine o destinazione
	7506	7892	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	7510	7896	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	7512	7898	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	7515	7901	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.
	7517	7903	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per il file origine o destinazione. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	7518	7904	ID file indirizzario relativo[3]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[2]
	7534	7920	Nome percorso assoluto[1]	Char(5002)	Il nome percorso assoluto del file origine o destinazione.

[1] Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza del nome percorso.

[2] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[3] Quando l'indicatore nome percorso (scostamento 7517) è N, questo campo conterrà l'ID file relativo del nome percorso assoluto allo scostamento 7534. Quando l'indicatore nome percorso è Y, questo campo conterrà 16 byte di zero esadecimali.

[4] Il campo risulterà vuoto quando non si tratta di un'operazione certificato.

[5] Il campo risulterà vuoto quando non si tratta di un'operazione file key ring.

[6] Il campo risulterà vuoto quando non si tratta di un'operazione root garantita.

Voci di giornale LD (Collegamento, Scollegamento, Ricerca indirizzario)

Questa tabella fornisce il formato delle voci di giornale LD (Collegamento, Scollegamento, Ricerca indirizzario).

Tabella 185. Voci di giornale LD (Collegamento, Scollegamento, Ricerca indirizzario). File descrizione campo QASYLDJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **L** Collegamento indirizzario **U** Scollegamento indirizzario **K** Ricerca indirizzario
157			(Area riservata)	Char(20)	
	225	611	(Area riservata)	Char(18)	
	243	629	Lunghezza nome oggetto[1]	Binary (4)	La lunghezza del nome oggetto.
177	245	631	CCSID nome oggetto[1]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
181	249	635	ID paese o regione nome oggetto[1]	Char(2)	L'ID paese o regione per il nome oggetto.
183	251	637	ID lingua nome oggetto[1]	Char(3)	L'ID lingua per il nome oggetto.
186	254	640	(Area riservata)	Char(3)	
189	257	643	ID file principale[1,2]	Char(16)	L'ID file dell'indirizzario principale.
205	273	659	ID file oggetto[1,2]	Char(16)	L'ID file dell'oggetto.
221	289	675	Nome oggetto[1]	Char(512)	Il nome dell'oggetto.
	801	1187	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	817	1203	Nome ASP	Char(10)	Il nome dell'unità ASP
	827	1213	Numero ASP	Char(5)	Il numero dell'unità ASP.
	832	1218	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.

Tabella 185. Voci di giornale LD (Collegamento, Scollegamento, Ricerca indirizzario) (Continua). File descrizione campo QASYLDJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	836	1222	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	838	1224	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	841	1227	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.
	843	1229	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	844	1230	ID file indirizzario relativo[1]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[1]
	860	1246	Nome percorso[2]	Char(5002)	Il nome percorso dell'oggetto.

[1] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[2] Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza del nome percorso.

Voci di giornale ML (Operazioni posta)

Questa tabella fornisce il formato delle voci di giornale ML (Operazioni posta).

Tabella 186. Voci di giornale ML (Operazioni posta). File descrizione campo QASYMLJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.

Tabella 186. Voci di giornale ML (Operazioni posta) (Continua). File descrizione campo QASYMLJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **O** Registrazione posta aperta
157	225	611	Profilo utente	Char(10)	Nome profilo utente.
167	235	621	ID utente	Char(8)	Identificativo utente
175	243	629	Indirizzo	Char(8)	Indirizzo utente

Voci di giornale NA (Modifica attributo)

Questa tabella fornisce il formato delle voci di giornale NA (Modifica attributo).

Tabella 187. Voci di giornale NA (Modifica attributo). File descrizione campo QASYNAJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Modifica in attributo di rete. **T** Modifica in attributo TCP/IP.
157	225	611	Attributo	Char(10)	Il nome dell'attributo.
167	235	621	Nuovo valore attributo	Char(250)	Il valore dell'attributo una volta modificato.
417	485	871	Vecchio valore attributo	Char(250)	Il valore dell'attributo prima della modifica.

Voci di giornale ND (Filtro ricerca indirizzario APPN)

Questa tabella fornisce il formato delle voci di giornale ND (Filtro ricerca indirizzario APPN).

Tabella 188. Voci di giornale ND (Filtro ricerca indirizzario APPN). File descrizione campo QASYNDJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la “Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)” a pagina 596, la “Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)” a pagina 598 e la “Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)” a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Violazione filtro ricerca indirizzario
157	225	611	Nome punto di controllo filtrato	Char(8)	Nome punto di controllo filtrato
165	233	619	NETID punto di controllo filtrato.	Char(8)	NETID punto di controllo filtrato.
173	241	627	Nome ubicazione CP filtrato	Char(8)	Nome ubicazione CP (Control Point/Punto di controllo) filtrato.
181	249	635	NETID ubicazione CP filtrato	Char(8)	NETID ubicazione CP (Control Point/Punto di controllo) filtrato.
189	257	643	Nome ubicazione partner	Char(8)	Nome ubicazione partner.
197	265	651	NETID ubicazione partner	Char(8)	NETID ubicazione partner.
205	273	659	Sessione di ricezione	Char(1)	Sessione di ricezione. **Y** Questa è una sessione di ricezione **N** Questa non è una sessione di ricezione
206	274	660	Sessione in uscita	Char(1)	Sessione in uscita. **Y** Questa è una sessione in uscita **N** Questa non è una sessione in uscita

Per ulteriori informazioni sul Filtro ricerca indirizzario APPN e e sull’endpoint APPN, consultare Protection of your system in an APPN and HPR environment per dettagli.

Voci di giornale NE (Filtro endpoint APPN)

Questa tabella fornisce il formato delle voci di giornale NE (Filtro endpoint APPN).

Tabella 189. Voci di giornale NE (Filtro endpoint APPN). File descrizione campo QASYNEJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Violazione filtro endpoint
157	225	611	Nome ubicazione locale	Char(8)	Nome ubicazione locale.
165	233	619	Nome ubicazione remota	Char(8)	Nome ubicazione remota.
173	241	627	NETID remoto	Char(8)	NETID remoto.
181	249	635	Sessione di ricezione	Char(1)	Sessione di ricezione. **Y** Questa è una sessione di ricezione **N** Questa non è una sessione di ricezione
182	250	636	Sessione in uscita	Char(1)	Sessione in uscita. **Y** Questa è una sessione in uscita **N** Questa non è una sessione in uscita

Per ulteriori informazioni sul Filtro ricerca indirizzario APPN e e sull'endpoint APPN, consultare Protection of your system in an APPN and HPR environment per dettagli.

Voci di giornale OM (Modifica gestione oggetto)

Questa tabella fornisce il formato delle voci di giornale OM (Modifica gestione oggetto).

Tabella 190. Voci di giornale OM (Modifica gestione oggetto). File descrizione campo QASYOMJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.

Tabella 190. Voci di giornale OM (Modifica gestione oggetto) (Continua). File descrizione campo QASYOMJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **M** Oggetto spostato in una libreria differente. **R** Oggetto ridenominato.
157	225	611	Vecchio nome oggetto	Char(10)	Il vecchio nome dell'oggetto.
167	235	621	Vecchio nome libreria	Char(10)	Il nome della libreria in cui risiede l'oggetto precedente.
177	245	631	Tipo oggetto	Char(8)	Il tipo di oggetto.
185	253	639	Nuovo nome oggetto	Char(10)	Il nuovo nome dell'oggetto.
195	263	649	Nuovo nome libreria	Char(10)	Il nome della libreria da cui l'oggetto è stato spostato.
205	273		(Area riservata)	Char(20)	
		659	Attributo oggetto	Char(10)	L'attributo dell'oggetto.
		669	(Area riservata)	Char(10)	
225	293	679	Utente Office	Char(10)	Il nome dell'utente Office.
235	303	689	Vecchio nome cartella o documento	Char(12)	Il vecchio nome della cartella o del documento.
247	315	701	(Area riservata)	Char(8)	
255	323	709	Vecchio percorso cartella	Char(63)	Il vecchio percorso della cartella.
318	386	772	Nuovo nome cartella o documento	Char(12)	Il nuovo nome della cartella o del documento.
330	398	784	(Area riservata)	Char(8)	
338	406	792	Nuovo percorso cartella	Char(63)	Il nuovo percorso della cartella.
401	469	855	Office per conto dell'utente	Char(10)	Utente che opera per conto di un altro utente.
411			(Area riservata)	Char(20)	
	479	865	(Area riservata)	Char(18)	
	497	883	Lunghezza nome oggetto	Binary (4)	La lunghezza del campo vecchio nome oggetto.

Tabella 190. Voci di giornale OM (Modifica gestione oggetto) (Continua). File descrizione campo QASYOMJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
431	499	885	CCSID nome oggetto[1]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
435	503	889	ID paese o regione nome oggetto[1]	Char(2)	L'ID paese o regione per il nome oggetto.
437	505	891	ID lingua nome oggetto[1]	Char(3)	L'ID lingua per il nome oggetto.
440	508	894	(Area riservata)	Char(3)	
443	511	897	Vecchio ID file principale[1,2]	Char(16)	L'ID file del vecchio indirizzario principale.
459	527	913	ID file vecchio oggetto[1,2]	Char(16)	L'ID file del vecchio oggetto.
475	543	929	Nome vecchio oggetto[1]	Char(512)	Il nome del vecchio oggetto.
987	1055	1441	Nuovo ID file principale[1,2]	Char(16)	L'ID file del nuovo indirizzario principale.
1003	1071	1457	Nuovo nome oggetto[1, 2 ,6]	Char(512)	Il nuovo nome dell'oggetto.
	1583	1969	ID file oggetto[1,2]	Char(16)	L'ID file dell'oggetto.
	1599	1985	Nome ASP[7]	Char(10)	Il nome dell'unità ASP
	1609	1995	Numero ASP[7]	Char(5)	Il numero dell'unità ASP.
	1614	2000	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	1618	2004	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	1620	2006	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	1623	2009	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.
	1625	2011	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.

Tabella 190. Voci di giornale OM (Modifica gestione oggetto) (Continua). File descrizione campo QASYOMJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	1626	2012	ID file indirizzario relativo[3]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[3]
	1642	2028	Nome percorso assoluto[5]	Char(5002)	Il vecchio nome percorso assoluto dell'oggetto.
	6644	7030	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	6660	7046	Nome ASP[8]	Char(10)	Il nome dell'unità ASP
	6670	7056	Numero ASP[8]	Char(5)	Il numero dell'unità ASP.
	6675	7061	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	6679	7065	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	6681	7067	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	6684	7070	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.
	6686	7072	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	6687	7073	ID file indirizzario relativo[4]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[3]
	6703	7089	Nome percorso assoluto[5]	Char(5002)	Il nuovo nome percorso assoluto dell'oggetto.

Tabella 190. Voci di giornale OM (Modifica gestione oggetto) (Continua). File descrizione campo QASYOMJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
			[1] Questi campi vengono utilizzati solo per oggetti nei file system ″root″ (/), QOpenSys e negli UDFS (user-defined file systems).		
			[2] Un ID con il bit all'estrema sinistra impostato ed il resto dei bit zero indica che l'ID NON è impostato.		
			[3] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.		
			[4] Quando l'indicatore nome percorso (scostamento 6686) è N, questo campo conterrà l'ID file relativo del nome percorso assoluto allo scostamento 6703. Quando l'indicatore nome percorso è Y, questo campo conterrà 16 byte di zero esadecimali.		
			[5] Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza del nome percorso.		
			[6] Non vi è alcun campo lunghezza associato per questo valore. La stringa contiene il carattere di riempimento nullo a meno che non sia completa nei 512 caratteri di lunghezza.		
			[7] Se il vecchio oggetto si trova nella libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se il vecchio oggetto non si trova in una libreria, queste sono le informazioni ASP dell'oggetto.		
			[8] Se il nuovo oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se il nuovo oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.		

Voci di giornale OR (Ripristino oggetto)

Questa tabella fornisce il formato delle voci di giornale OR (Ripristino oggetto).

Tabella 191. Voci di giornale OR (Ripristino oggetto). File descrizione campo QASYORJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **N** È stato ripristinato un nuovo oggetto sul sistema. **E** Un oggetto esistente è stato ripristinato nel sistema.
157	225	611	Nome oggetto ripristinato	Char(10)	Il nome dell'oggetto ripristinato.
167	235	621	Nome libreria ripristinata	Char(10)	Il nome della libreria dell'oggetto ripristinato.
177	245	631	Tipo oggetto.	Char(8)	Il tipo di oggetto.

Tabella 191. Voci di giornale OR (Ripristino oggetto) (Continua). File descrizione campo QASYORJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
185	253	639	Nome oggetto di salvataggio	Char(10)	Il nome dell'oggetto di salvataggio.
195	263	649	Nome libreria di salvataggio	Char(10)	Il nome della libreria da cui l'oggetto è stato salvato.
205	273	659	Stato programma[1]	Char(1)	**I** Un programma stato eredità è stato ripristinato. **Y** Un programma stato sistema è stato ripristinato. **N** Un programma stato utente è stato ripristinato.
206	274	660	Comando sistema [2]	Char(1)	**Y** Un comando sistema è stato ripristinato. **N** Un comando stato utente è stato ripristinato.
207			(Area riservata)	Char(18)	
	275	661	Modalità SETUID	Char(1)	L'indicatore modalità SETUID. **Y** Il bit della modalità SETUID per l'oggetto ripristinato è attivo. **N** Il bit della modalità SETUID per l'oggetto ripristinato non è attivo.
	276	662	Modalità SETGID	Char(1)	L'indicatore modalità SETGID. **Y** Il bit della modalità SETGID per l'oggetto ripristinato è attivo. **N** Il bit della modalità SETGID per l'oggetto ripristinato non è attivo.
	277	663	Stato firma	Char(1)	Lo stato della firma dell'oggetto ripristinato. **B** La firma non era nel formato i5/OS **E** La firma esiste ma non è verificata **F** La firma non corrisponde al contenuto dell'oggetto **I** Firma ignorata **N** Oggetto non firmabile **S** Firma non valida **T** Firma non garantita **U** Oggetto non firmato

Tabella 191. Voci di giornale OR (Ripristino oggetto) (Continua). File descrizione campo QASYORJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	278	664	Attributo di scansione	Char(1)	Se il file fosse un oggetto IFS (integrated file system), il valore dell'attributo di scansione per tale oggetto sarebbe **Y** *YES **N** *NO **C** *CHGONLY Consultare il comando CHGATR per la descrizione di questi valori.
	279		(Area riservata)	Char(14)	
		665	Attributo oggetto	Char(10)	L'attributo dell'oggetto.
		675	(Area riservata)	Char(4)	
225	293	679	Utente Office	Char(10)	Il nome dell'utente Office.
235	303	689	Nome DLO di ripristino	Char(12)	Il nome DLO (document library object) dell'oggetto ripristinato.
247	315	701	(Area riservata)	Char(8)	
255	323	709	Percorso cartella di ripristino	Char(63)	La cartella in cui il DLO è stato ripristinato.
318	386	772	Nome DLO di salvataggio	Char(12)	Il nome DLO dell'oggetto salvato.
330	398	784	(Area riservata)	Char(8)	
338	406	792	Percorso cartella di salvataggio	Char(63)	La cartella da cui il DLO è stato salvato.
401	469	855	Office per conto dell'utente	Char(10)	Utente che opera per conto di un altro utente.
411			(Area riservata)	Char(20)	
	479		(Area riservata)	Char(18)	
		865	Ripristino autorizzazioni private	Char(1)	Le autorizzazioni private di cui è stato richiesto il ripristino (PVTAUT(*YES) specificata sul comando di rispristino) **Y** PVTAUT(*YES) specificata sul comando di rispristino **N** PVTAUT(*NO) specificata sul comando di rispristino
		866	Autorizzazioni private salvate[8]	Binary(5)	Numero di autorizzazioni private salvate

Tabella 191. Voci di giornale OR (Ripristino oggetto) (Continua). File descrizione campo QASYORJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
		870	Autorizzazioni private ripristinate[8]	Binary(5) [8]	Numero di autorizzazioni private ripristinate
		874	(Area riservata)	Char(9)	
	497	883	Lunghezza nome oggetto	Binary (4)	La lunghezza del campo vecchio nome oggetto.
431	499	885	CCSID nome oggetto[3]	Binary(5)	Il CCSID (coded character set identifer) per il nome oggetto.
435	503	889	ID paese o regione nome oggetto[3]	Char(2)	L'ID paese o regione per il nome oggetto.
437	505	891	ID lingua nome oggetto[3]	Char(3)	L'ID lingua per il nome oggetto.
440	508	894	(Area riservata)	Char(3)	
443	511	897	ID file principale[3,4]	Char(16)	L'ID file dell'indirizzario principale.
459	527	913	ID file oggetto[3,4]	Char(16)	L'ID file dell'oggetto.
475	543	929	Nome oggetto[3]	Char(512)	Il nome dell'oggetto.
	1055	1441	Vecchio ID file	Char(16)	L'ID file per il vecchio oggetto.
	1071	1457	ID file supporto magnetico	Char(16)	L'ID file (FID) che è stato memorizzato nel file di supporto magnetico. **Nota:** Il FID memorizzato nel supporto magnetico è il FID che l'oggetto aveva nel sistema origine.
	1087	1473	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	1103	1489	Nome ASP[7]	Char(10)	Il nome dell'unità ASP
	1113	1499	Numero ASP[7]	Char(5)	Il numero dell'unità ASP.
	1118	1504	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	1122	1508	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	1124	1510	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	1127	1513	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.

Tabella 191. Voci di giornale OR (Ripristino oggetto) (Continua). File descrizione campo QASYORJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	1129	1515	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	1130	1516	ID file indirizzario relativo[5]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[5]
	1146	1532	Nome percorso[6]	Char(5002)	Il nome percorso dell'oggetto.

[1] Questo campo contiene una voce solo se l'oggetto che viene ripristinato è un programma.

[2] Questo campo contiene una voce solo se l'oggetto che viene ripristinato è un comando.

[3] Questo campo viene utilizzato solo per gli oggetti nel file system "root" (/) ,QOpenSys, e UDFS (user-defined file system).

[4] Un ID con il bit all'estrema sinistra impostato ed il resto dei bit zero indica che l'ID NON è impostato.

[5] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[6] Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza del nome percorso.

[7] Se l'oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.

[8] Questo campo è zero se Ripristino autorizzazioni private (scostamento 865) è N.

Voci di giornale OW (Modifica proprietà)

Questa tabella fornisce il formato delle voci di giornale OW (Modifica proprietà).

Tabella 192. Voci di giornale OW (Modifica proprietà). File descrizione campo QASYOWJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Modifica del proprietario dell'oggetto
157	225	611	Nome oggetto	Char(10)	Il nome dell'oggetto.
167	235	621	Nome libreria	Char(10)	Il nome della libreria dove è memorizzato l'oggetto.
177	245	631	Tipo oggetto	Char(8)	Il tipo di oggetto.
185	253	639	Vecchio proprietario	Char(10)	Vecchio proprietario dell'oggetto.
195	263	649	Nuovo proprietario	Char(10)	Nuovo proprietario dell'oggetto.
205	273	659	(Area riservata)	Char(20)	
225	293	679	Utente Office	Char(10)	Il nome dell'utente Office.
235	303	689	Nome DLO	Char(12)	Il nome del DLO (document library object).
247	315	701	(Area riservata)	Char(8)	
255	323	709	Percorso cartella	Char(63)	Il percorso della cartella.
318	386	772	Office per conto dell'utente	Char(10)	Utente che opera per conto di un altro utente.
328			(Area riservata)	Char(20)	
	396	782	(Area riservata)	Char(18)	
	414	800	Lunghezza nome oggetto	Binary (4)	La lunghezza del nuovo nome oggetto.
348	416	802	CCSID nome oggetto[1]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
352	420	806	ID paese o regione nome oggetto[1]	Char(2)	L'ID paese o regione per il nome oggetto.
354	422	808	ID lingua nome oggetto[1]	Char(3)	L'ID lingua per il nome oggetto.
357	425	811	(Area riservata)	Char(3)	

Tabella 192. Voci di giornale OW (Modifica proprietà) (Continua). File descrizione campo QASYOWJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
360	428	814	ID file principale[1,2]	Char(16)	L'ID file dell'indirizzario principale.
376	444	830	ID file oggetto[1,2]	Char(16)	L'ID file dell'oggetto.
392	460	846	Nome oggetto[1]	Char(512)	Il nome dell'oggetto.
	972	1358	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	988	1374	Nome ASP[5]	Char(10)	Il nome dell'unità ASP
	998	1384	Numero ASP[5]	Char(5)	Il numero dell'unità ASP.
	1003	1389	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	1007	1393	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	1009	1395	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	1012	1398	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.
	1014	1400	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	1015	1401	ID file indirizzario relativo[3]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[3]
	1031	1417	Nome percorso[4]	Char(5002)	Il nome percorso dell'oggetto.

[1] Questi campi vengono utilizzati solo per oggetti nei file system "root" (/), QOpenSys e negli UDFS (user-defined file system).

[2] Un ID con il bit all'estrema sinistra impostato ed il resto dei bit zero indica che l'ID NON è impostato.

[3] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[4] Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza del nome percorso.

[5] Se l'oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.

Voci di giornale O1 (Accesso unità ottica)

Questa tabella fornisce il formato delle voci di giornale O1 (Accesso unità ottica).

Tabella 193. Voci di giornale O1 (Accesso unità ottica). File descrizione campo QASY01JE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	R-Lettura U-Aggiornamento D-Cancellazione C-Creazione indir. X-Rilascio file congelato
157	225	611	Tipo oggetto	Char(1)	F-File D-Fine indirizzario S-Memoria
158	226	612	Tipo accesso	Char(1)	D-Dati file A-Attributi indirizzario file R-Operazione di ripristino S-Operazione di salvataggio
159	227	613	Nome unità	Char(10)	Nome LUD libreria
169	237	623	Nome CSI	Char(8)	Nome oggetto laterale
177	245	631	Libreria CSI	Char(10)	Libreria oggetto laterale
187	255	641	Nome volume	Char(32)	Nome volume unità ottica
219	287	673	Nome oggetto	Char(256)	Nome indirizzario/file unità ottica
		929	Nome ASP	Char(10)	Nome ASP per libreria CSI
		939	Numero ASP	Char(5)	Numero ASP per libreria CSI

Nota: questa voce viene utilizzata per controllare le seguenti funzioni dell'unità ottica:

- Apertura file o indirizzario
- Creazione indirizzario
- Cancellazione indirizzario file
- Modifica o richiamo attributi
- Rilascio file unità ottica congelato

Voci di giornale O2 (Accesso unità ottica)

Questa tabella fornisce il formato delle voci di giornale O2 (Accesso unità ottica).

Tabella 194. Voci di giornale O2 (Accesso unità ottica). File descrizione campo QASY02JE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	C-Copia R-Ridenominazione B-Copia di riserva dati indir. o file S-Salvataggio file congelato M-Spostamento file
157	225	611	Tipo oggetto	Char(1)	F-File D-Indirizzario
158	226	612	Nome unità orig.	Char(10)	Nome LUD libreria origine
168	236	622	Nome CSI orig.	Char(8)	Nome oggetto laterale origine
176	244	630	Libreria CSI orig.	Char(10)	Libreria oggetto laterale origine
186	254	640	Nome volume orig.	Char(32)	Nome volume unità ottica origine
218	286	672	Nome ogg. orig.	Char(256)	Nome indirizzario/file unità ottica origine
474	542	928	Nome unità dest.	Char(10)	Nome LUD libreria dest.
484	552	938	Nome CSI dest.	Char(8)	Nome oggetto laterale destinazione
492	560	946	Libreria CSI dest.	Char(10)	Libreria oggetto laterale dest.
502	570	956	Nome volume dest.	Char(32)	Nome volume unità ottica destinazione
534	602	988	Nome ogg. dest.	Char(256)	Nome indirizzario/file unità ottica destinazione
		1244	Nome ASP	Char(10)	Nome ASP per libreria CSI origine
		1254	Numero ASP	Char(5)	Numero ASP per libreria CSI origine

Tabella 194. Voci di giornale O2 (Accesso unità ottica) (Continua). File descrizione campo QASY02JE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
		1259	Nome ASP per libreria CSI destinazione	Char(10)	Nome ASP per libreria CSI destinazione
		1269	Numero ASP per libreria CSI destinazione	Char(5)	Numero ASP per libreria CSI destinazione

Voci di giornale O3 (Accesso unità ottica)

Questa tabella fornisce il formato delle voci di giornale O3 (Accesso unità ottica).

Tabella 195. Voci di giornale O3 (Accesso unità ottica). File descrizione campo QASY03JE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	**A** Modifica attributi volume **B** Copia di riserva dati del volume **C** Conversione copia di riserva dati volume in principale **E** Esportare **I** Inizializzazione **K** Verifica del volume **L** Modifica elenco autorizzazioni **M** Importare **N** Ridenominazione **R** Lettura assoluta
157	225	611	Nome unità	Char(10)	Nome LUD libreria
167	235	621	Nome CSI	Char(8)	Nome oggetto laterale
175	243	629	Libreria CSI	Char(10)	Libreria oggetto laterale
185	253	639	Nome vecchio volume	Char(32)	Nome vecchio volume unità ottica
217	285	671	Nome nuovo volume[1]	Char(32)	Nome nuovo volume unità ottica

Tabella 195. Voci di giornale O3 (Accesso unità ottica) (Continua). File descrizione campo QASY03JE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
249	317	703	Vecchio elenco autoriz. [2]	Char(10)	Vecchio elenco autorizzazioni
259	327	713	Nuovo elenco autoriz. [3]	Char(10)	Nuovo elenco autorizzazioni
269	337	723	Indirizzo [4]	Binary(5)	Blocco di avvio
273	341	727	Lunghezza [4]	Binary(5)	Lunghezza letta
		731	Nome ASP	Char(10)	Nome ASP per libreria CSI
		741	Numero ASP	Char(5)	Numero ASP per libreria CSI

[1] Questo campo contiene il nome del nuovo volume per le funzioni Inizializzazione, Ridenominazione e Conversione; contiene il nome del volume copia di riserva per le funzioni Copia di riserva. Contiene il nome volume per l'Importazione, Esportazione, la Modifica elenco autorizzazioni, la Modifica attributi volume e Settore letto.

[2] Utilizzato solo per Importazione, Esportazione e Modifica elenco autorizzazioni.

[3] Utilizzato solo per Modifica elenco autorizzazioni.

[4] Utilizzato solo per Settore letto.

Voci giornale PA (Program Adopt/Adozione programma)

Questa tabella fornisce il formato delle voci di giornale PA (Program adopt/ Adozione programma).

Tabella 196. Voci giornale PA (Program Adopt/Adozione programma). File descrizione campo QASYPAJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Modificare il programma in modo che adotti l'autorizzazione del proprietario. **J** Il programma Java adotta l'autorizzazione del proprietario. **M** Modificare il SETUID, il SETGID o l'indicatore di ridenominazione limitata e modalità di scollegamento dell'oggetto.
157	225	611	Nome programma[3]	Char(10)	Il nome del programma.
167	235	621	Libreria programma[3]	Char(10)	Il nome della libreria dove è stato reperito il programma.

Tabella 196. Voci giornale PA (Program Adopt/Adozione programma) (Continua). File descrizione campo QASYPAJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
177	245	631	Tipo oggetto	Char(8)	Il tipo di oggetto.
185	253	639	Proprietario	Char(10)	Il nome del proprietario.
	263	649	Modalità IXVTX	Char(1)	L'indicatore di ridenominazione limitata e modalità (ISVTX) di scollegamento. **Y** L'indicatore modalità ISVTX è attivo sull'oggetto. **N** L'indicatore di modalità ISVTX non è attivo per l'oggetto.
	263	649	Riservato	Char(17)	
	281	667	Lunghezza nome oggetto[1]	Binary (4)	La lunghezza del nome oggetto.
	283	669	CCSID nome oggetto[1]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
	287	673	ID paese o regione nome oggetto	Char(2)	L'ID paese o regione per il nome oggetto.
	289	675	ID lingua nome oggetto[1]	Char(3)	L'ID lingua per il nome oggetto.
	292	678	Riservato	Char(3)	
	295	681	ID principale[1, 2, 3]	Char(16)	ID file principale.
	311	697	ID file oggetto [3]	Char(16)	ID file per l'oggetto
	327	713	Nome oggetto[1]	Char(512)	Nome oggetto per l'oggetto.
	839	1225	Modalità SETUID	Char(1)	L'indicatore modalità SETUID (Set effective user ID). **Y** Il bit della modalità SETUID è attivo per l'oggetto. **N** Il bit della modalità SETUID non è attivo per l'oggetto.
	840	1226	Modalità SETGID	Char(1)	L'indicatore di modalità SETGID (Set effective group ID) **Y** Il bit della modalità SETGID è attivo per l'oggetto. **N** Il bit della modalità SETGID non è attivo per l'oggetto.
	841	1227	Proprietario del gruppo principale	Char(10)	Il nome del proprietario del gruppo principale.
	851	1237	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	867	1253	Nome ASP[6]	Char(10)	Il nome dell'unità ASP
	877	1263	Numero ASP[6]	Char(5)	Il numero dell'unità ASP.
	882	1268	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.

Tabella 196. Voci giornale PA (Program Adopt/Adozione programma) (Continua). File descrizione campo QASYPAJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	886	1272	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	888	1274	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	891	1277	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.
	893	1279	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	894	1280	ID file indirizzario relativo[4]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[4]
	910	1296	Nome percorso[5]	Char(5002)	Il nome percorso dell'oggetto.

[1] Questi campi vengono utilizzati solo per oggetti nei file system "root" (/), QOpenSys e negli UDFS (user-defined file systems).

[2] Un ID con il bit all'estrema sinistra impostato ed il resto dei bit zero indica che l'ID NON è impostato.

[3] Quando il tipo di voce è J, i campi nome programma e nome libreria conterranno *N. Inoltre, i campi ID file principale e ID file oggetto conterranno zero binari.

[4] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[5] Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza del nome percorso.

[6] Se l'oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.

Voci di giornale PG (Primary Group Change/Modifica gruppo principale)

Questa tabella fornisce il formato delle voci di giornale PG (Primary Group Change/ Modifica gruppo principale).

Tabella 197. Voci di giornale PG (Primary Group Change/Modifica gruppo principale). File descrizione campo QASYPGJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Modificare gruppo principale.
157	225	611	Nome oggetto	Char(10)	Il nome dell'oggetto.
167	235	621	Libreria oggetto	Char(10)	Il nome della libreria dove è stato reperito l'oggetto.
177	245	631	Tipo oggetto	Char(8)	Il tipo di oggetto.
185	253	639	Vecchio gruppo principale	Char(10)	Il precedente gruppo principale per l'oggetto.[5]
195	263	649	Nuovo gruppo principale	Char(10)	Il nuovo gruppo principale per l'oggetto.
					Autorizzazioni del nuovo gruppo principale:
205	273	659	Esistenza oggetto	Char(1)	**Y** *OBJEXIST
206	274	660	Gestione oggetto	Char(1)	**Y** *OBJMGT
207	275	661	Operativo oggetto	Char(1)	**Y** *OBJOPR
208	276	662	Modifica oggetto	Char(1)	**Y** *OBJALTER
209	277	663	Riferimento oggetto	Char(1)	**Y** *OBJREF
210	278	664	(Area riservata)	Char(10)	
220	288	674	Gestione elenco autoriz.	Char(1)	**Y** *AUTLMGT
221	289	675	Autorizzazione alla lettura	Char(1)	**Y** *READ
222	290	676	Autorizzazione all'aggiunta	Char(1)	**Y** *ADD
223	291	677	Autorizzazione all'aggiornam.	Char(1)	**Y** *UPD
224	292	678	Autorizzazione alla cancellazione	Char(1)	**Y** *DLT
225	293	679	Autorizzazione all'esecuzione	Char(1)	**Y** *EXECUTE

Tabella 197. Voci di giornale PG (Primary Group Change/Modifica gruppo principale) (Continua). File descrizione campo QASYPGJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
226	294	680	(Area riservata)	Char(10)	
236	304	690	Autorizzazione all'esclusione	Char(1)	**Y** *EXCLUDE
237	305	691	Revocare vecchio gruppo principale	Char(1)	**Y** Revocare l'autorizzazione del gruppo principale precedente. ' ' Non revocare l'autorizzazione del gruppo principale precedente.
238	306	692	(Area riservata)	Char (20)	
258	326	712	Utente Office	Char(10)	Il nome dell'utente Office.
268	336	722	Nome DLO	Char(12)	Il nome del DLO o della cartella.
280	348	734	(Area riservata)	Char(8)	
288	356	742	Percorso cartella	Char(63)	Il percorso della cartella.
351	419	805	Office per conto dell'utente	Char(10)	Utente che opera per conto di un altro utente.
361			(Area riservata)	Char(20)	
	429	815	(Area riservata)	Char(18)	
	447	833	Lunghezza nome oggetto[1]	Binary (4)	La lunghezza del nome oggetto.
381	449	835	CCSID nome oggetto[1]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
385	453	839	ID paese o regione nome oggetto[1]	Char(2)	L'ID paese o regione per il nome oggetto.
387	455	841	ID lingua nome oggetto[1]	Char(3)	L'ID lingua per il nome oggetto.
390	458	844	(Area riservata)	Char(3)	
393	461	847	ID file principale[1,2]	Char(16)	L'ID file dell'indirizzario principale.
409	477	863	ID file oggetto[1,2]	Char(16)	L'ID file dell'oggetto.
425	493	879	Nome oggetto[1]	Char(512)	Il nome dell'oggetto.
	1005	1391	ID file oggetto	Char(16)	L'ID file dell'oggetto.
		1407	Nome ASP[6]	Char(10)	Il nome dell'unità ASP
		1417	Numero ASP[6]	Char(5)	Il numero dell'unità ASP.
	1035	1422	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	1040	1426	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	1042	1428	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.

Tabella 197. Voci di giornale PG (Primary Group Change/Modifica gruppo principale) (Continua). File descrizione campo QASYPGJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	1045	1431	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.
	1047	1433	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	1048	1434	ID file indirizzario relativo[3]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[3]
	1064	1450	Nome percorso[4]	Char(5002)	Il nome percorso dell'oggetto.

[1] Questi campi vengono utilizzati solo per oggetti nei file system "root" (/), QOpenSys e negli UDFS (user-defined file systems).

[2] Un ID con il bit all'estrema sinistra impostato ed il resto dei bit zero indica che l'ID NON è impostato.

[3] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[4] Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza del nome percorso.

[5] Un valore di *N implica che il valore del Vecchio gruppo principale non era disponibile.

[6] Se l'oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.

Voci di giornale PO (Printer Output/Emissione di stampa)

Questa tabella fornisce il formato delle voci di giornale PO (Printer Output/ Emissione di stampa).

Tabella 198. Voci di giornale PO (Printer Output/Emissione di stampa). File descrizione campo QASYPOJE/J4/J5

Scost.					
JE	**`J4**	**J5**	**Campo**	**Formato**	**Descrizione**
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.

Tabella 198. Voci di giornale PO (Printer Output/Emissione di stampa) (Continua). File descrizione campo QASYPOJE/J4/J5

Scost.					
JE	**`J4**	**J5**	**Campo**	**Formato**	**Descrizione**
156	224	610	Tipo emissione	Char(1)	Il tipo di emissione. **D** Stampa diretta **R** Inviato al sistema remoto per la stampa **S** File di spool stampato
157	225	611	Stato dopo la stampa	Char(1)	**D** Cancellato dopo la stampa **H** Congelato dopo la stampa **S** Salvato dopo la stampa **' '** Stampa diretta
158	226	612	Nome lavoro	Char(10)	La prima parte del nome lavoro qualificato.
168	236	622	Nome utente lavoro	Char(10)	La seconda parte del nome lavoro qualificato.
178	246	632	Numero lavoro	Zoned(6,0)	La terza parte del nome lavoro qualificato.
184	252	638	Profilo utente	Char(10)	Il profilo utente che ha creato l'emissione.
194	262	648	Coda di emissione	Char(10)	La coda di emissione che contiene il file di spool.[1]
204	272	658	Nome libreria coda di emissione	Char(10)	Il nome della libreria che contiene la coda di emissione.[1]
214	282	668	Nome unità	Char(10)	L'unità in cui è stata stampata l'emissione[2].
224	292	678	Tipo unità	Char(4)	Il tipo di unità stampante[2].
228	296	682	Modello unità	Char(4)	Il modello dell'unità stampante[2].
232	300	686	Nome file unità	Char(10)	Il nome del file unità utilizzato per accedere alla stampante.
242	310	696	Libreria file unità	Char(10)	Il nome della libreria per il file unità.
252	320	706	Nome file di spool	Char(10)	Il nome del file di spool [1]
262	330	716	Numero file di spool breve	Char(4)	Il numero del file di spool [1]. Lasciato vuoto se troppo lungo.
266	334	720	Tipo formato	Char(10)	Il tipo di formato del file di spool.
276	344	730	Dati utente	Char(10)	I dati utente associati al file di spool [1].
286			(Area riservata)	Char(20)	
	354	740	Numero file di spool	Char(6)	Il numero del file di spool.
	360	746	Area riservata	Char(14)	
306	374	760	Sistema remoto	Char(255)	Il nome del sistema remoto a cui è stata inviata la stampa.

Tabella 198. Voci di giornale PO (Printer Output/Emissione di stampa) (Continua). File descrizione campo QASYPOJE/J4/J5

Scost.					
JE	**`J4**	**J5**	**Campo**	**Formato**	**Descrizione**
561	629	1015	Coda di stampa sistema remoto	Char(128)	Il nome della coda di emissione sul sistema remoto.
	757	1143	Nome sistema lavoro file di spool	Char(8)	Il nome del sistema nel quale risiede il file di spool.
	765	1151	Data creazione file di spool	Char (7)	Data di creazione del file di spool (SAAMMGG)
	772	1158	Ora di creazione del file di spool	Char(6)	L'ora della creazione del file di spool (HHMMSS).
		1164	Nome ASP	Char(10)	Nome ASP per la libreria unità
		1174	Numero ASP	Char(5)	Numero ASP per la libreria file unità
		1179	Nome ASP coda di emissione	Char(10)	Nome ASP per la libreria coda di emissione.
		1189	Numero ASP coda di emissione	Char(5)	Numero ASP per la libreria coda di emissione.
		1194	UTC data creazione file di spool	Char(7)	La data di creazione del file di spool in UTC (È la stessa data della Data di creazione file di spool (scostamento 1151) solo in UTC).
		1201	UTC ora di creazione del file di spool	Char(6)	L'ora di creazione del file di spool in UTC (È la stessa ora della Ora di creazione file di spool (scostamento 1158) solo in UTC)

[1] Questo campo è vuoto se il tipo di emissione è stampa diretta.

[2] Questo campo è vuoto se il tipo di emissione è stampa remota.

Voci di giornale PS (Profile Swap/Swap profilo)

Questa tabella fornisce il formato delle voci di giornale PS (Profile Swap/ Swap profilo).

Tabella 199. Voci di giornale PS (Profile Swap/Swap profilo). File descrizione campo QASYPSJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.

Tabella 199. Voci di giornale PS (Profile Swap/Swap profilo) (Continua). File descrizione campo QASYPSJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Swap profilo durante pass-through. **E** Fine lavoro per conto della relazione. **H** Gestione profilo generata dall'API QSYGETPH. **I** Tutti i token del profilo sono stati invalidati **M** Numero massimo di token profilo generati. **P** Token profilo generati per l'utente. **R** Tutti i token profilo per un utente sono stati eliminati. **S** Avvio lavoro per conto della relazione **V** Profilo utente autenticato
157	225	611	Profilo utente	Char(10)	Nome profilo utente.
167	235	621	Ubicazione origine	Char(8)	Ubicazione dell'origine pass-through.
175	243	629	Profilo utente destinazione originale	Char(10)	Profilo utente destinazione pass-through originale.
185	253	639	Profilo utente nuova destinazione	Char(10)	Profilo utente nuova destinazione pass-through
195	263	649	Utente Office	Char(10)	L'utente Office che avvia o termina per conto della relazione.
205	273	659	Per conto dell'utente	Char(10)	Utente per conto del quale l'utente office sta operando.
215	283	669	Tipo token profilo	Char(1)	Il tipo di token profilo generato. **M** Token profilo multiuso **R** Token profilo ricreato multiuso **S** Token profilo a singolo utilizzo
216	284	670	Supero tempo token profilo	Binary (4)	Il numero di secondi in cui il token del profilo è valido.

Voci di giornale PW (Password/Parola d'ordine)

Questa tabella fornisce il formato delle voci di giornale PW (Password/ Parola d'ordine).

Tabella 200. Voci di giornale PW (Password/Parola d'ordine). File descrizione campo QASYPWJE/J4/J5

Scostamento			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo voce violazione	Char(1)	Il tipo di violazione **A** Errore collegamento APPC. **C** L'autenticazione utente con il comando CHKPWD ha avuto esito negativo. **D** Nome ID utente programmi di manutenzione non valido. **E** Parola d'ordine ID utente programmi di manutenzione non valida. **P** Parola d'ordine non valida. **Q** Tentativo di collegamento (autenticazione utente) non riuscito a causa della disabilitazione del profilo utente. **R** Tentativo di collegamento (autenticazione utente) non riuscito a causa della scadenza della parola d'ordine. È possibile che questo record di controllo non si verifichi per alcuni meccanismi di autenticazione utente. Alcuni meccanismi di autenticazione non verificano le parole d'ordine scadute. **S** La parola d'ordine Decodifica SQL non è valida **U** Nome utente non valido. **X** L'ID utente dei programmi di manutenzione è disabilitato **Y** ID utente programmi di manutenzione non valido. **Z** Parola d'ordine ID utente programmi di manutenzione non valida.
157	225	611	Nome utente	Char(10)	Il nome utente lavoro o il nome ID utente dei programmi di manutenzione.
167	235	621	Nome unità	Char(40)	Il nome dell'unità o dell'unità di comunicazioni su cui sono stati immessi la parola d'ordine o l'ID utente. Se il tipo di voce è X, Y o Z, questo campo conterrà il nome del programma di manutenzione a cui si accede.

Tabella 200. Voci di giornale PW (Password/Parola d'ordine) (Continua). File descrizione campo QASYPWJE/J4/J5

Scostamento			Campo	Formato	Descrizione
JE	**J4**	**J5**			
207	275	661	Nome ubicazione remota	Char(8)	Nome dell'ubicazione remota per il collegamento APPC.
215	283	669	Nome ubicazione locale	Char(8)	Nome dell'ubicazione locale per il collegamento APPC.
223	291	677	ID rete	Char(8)	ID rete per il collegamento APPC.
		685[2]	Nome oggetto	Char(10)	Il nome dell'oggetto che viene decodificato.
		695	Libreria oggetto	Char(10)	La libreria per l'oggetto che viene decodificato.
		705	Tipo di oggetto	Char(8)	Il tipo dell'oggetto che viene decodificato.
		713	Nome ASP[1]	Char(10)	Il nome dell'unità ASP
		723	Numero ASP[1]	Char(5)	Il numero dell'unità ASP.

[1] Se l'oggetto è in una libreria, queste sono le informazioni ASP relative alla libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP per l'oggetto.

[2] Se il nome dell'oggetto è *N ed il tipo di violazione è S, l'utente ha tentato di decodificare dati in una variabile host.

Voci di giornale RA (Modifica autorizzazione per oggetto ripristinato)

Questa tabella fornisce il formato delle voci di giornale RA (Modifica autorizzazione per oggetto ripristinato).

Tabella 201. Voci di giornale RA (Modifica autorizzazione per oggetto ripristinato). File descrizione campo QASYRAJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Modifiche all'autorizzazione per oggetto ripristinato
157	225	611	Nome oggetto	Char(10)	Il nome dell'oggetto.
167	235	621	Nome libreria	Char(10)	Il nome della libreria dove è memorizzato l'oggetto.
177	245	631	Tipo di oggetto	Char(8)	Il tipo di oggetto.

Tabella 201. Voci di giornale RA (Modifica autorizzazione per oggetto ripristinato) (Continua). File descrizione campo QASYRAJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
185	253	639	Nome elenco autorizzazioni	Char(10)	Il nome dell'elenco autorizzazioni.
195	263	649	Autorizzaz. pubblica	Char(1)	**Y** Autorizzazione pubblica impostata su *EXCLUDE.
196	264	650	Autorizzazione privata	Char(1)	**Y** Autorizzazione privata eliminata.
197	265	651	AUTL eliminato	Char(1)	**Y** Elenco autorizzazioni eliminato dall'oggetto.
198	266	652	(Area riservata)	Char(20)	
218	286	672	Nome DLO	Char(12)	Il nome del DLO (document library object).
230	298	684	(Area riservata)	Char(8)	
238	306	692	Percorso cartella	Char(63)	La cartella contenente il DLO (document library object).
301			(Area riservata)	Char(20)	
	369	755	(Area riservata)	Char(18)	
	387	773	Lunghezza nome oggetto	Binary (4)	La lunghezza del nome oggetto.
321	389	775	CCSID nome oggetto[1]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
325	393	779	ID paese o regione nome oggetto[1]	Char(2)	L'ID paese o regione per il nome oggetto.
327	395	781	ID lingua nome oggetto[1]	Char(3)	L'ID lingua per il nome oggetto.
330	398	784	(Area riservata)	Char(3)	
333	401	787	ID file principale[1,2]	Char(16)	L'ID file dell'indirizzario principale.
349	417	803	ID file oggetto[1,2]	Char(16)	L'ID file dell'oggetto.
365	433	819	Nome oggetto[1]	Char(512)	Il nome dell'oggetto.
	945	1331	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	961	1347	Nome ASP[5]	Char(10)	Il nome dell'unità ASP
	971	1357	Numero ASP[5]	Char(5)	Il numero dell'unità ASP.
	976	1362	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	980	1366	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.

Tabella 201. Voci di giornale RA (Modifica autorizzazione per oggetto ripristinato) (Continua). File descrizione campo QASYRAJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	982	1368	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	985	1371	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.
	987	1373	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	988	1374	ID file indirizzario relativo[3]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[3]
	1004	1390	Nome percorso[4]	Char(5002)	Il nome percorso dell'oggetto.

[1] Questi campi vengono utilizzati solo per oggetti nei file system "root" (/), QOpenSys e negli UDFS (user-defined file systems).

[2] Un ID con il bit all'estrema sinistra impostato ed il resto dei bit zero indica che l'ID NON è impostato.

[3] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[4] Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza del nome percorso.

[5] Se l'oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.

Voci di giornale RJ (Ripristino descrizione lavoro)

Questa tabella fornisce il formato delle voci di giornale RJ (Ripristino descrizione lavoro).

Tabella 202. Voci di giornale RJ (Ripristino descrizione lavoro). File descrizione campo QASYRJJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Ripristino di una descrizione lavoro con un profilo utente specificato nel parametro USER.
157	225	611	Nome descrizione lavoro	Char(10)	Il nome della descrizione lavoro ripristinata.
167	235	621	Nome libreria	Char(10)	Il nome della libreria in cui è stata ripristinata la descrizione lavoro.
177	245	631	Tipo di oggetto	Char(8)	Il tipo di oggetto.
185	253	639	Nome utente	Char(10)	Il nome del profilo utente specificato nella descrizione lavoro.
		649	Nome ASP	Char(10)	Nome ASP per la libreria JOBD
		659	Numero ASP	Char(5)	Numero ASP per la libreria JOBD

Voci di giornale RO (Modifica proprietà per oggetto ripristinato)

Questa tabella fornisce il formato delle voci di giornale RO (Modifica proprietà per oggetto ripristinato).

Tabella 203. Voci di giornale RO (Modifica proprietà per oggetto ripristinato). File descrizione campo QASYROJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Ripristino i oggetti la cui proprietà è stata modifica durante il ripristino

Tabella 203. Voci di giornale RO (Modifica proprietà per oggetto ripristinato) (Continua). File descrizione campo QASYROJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
157	225	611	Nome oggetto	Char(10)	Il nome dell'oggetto.
167	235	621	Nome libreria	Char(10)	Il nome della libreria in cui si trova l'oggetto.
177	245	631	Tipo di oggetto	Char(8)	Il tipo di oggetto.
185	253	639	Vecchio proprietario	Char(10)	Il nome del proprietario prima della modifica della proprietà.
195	263	649	Nuovo proprietario	Char(10)	Il nome del proprietario dopo che la proprietà è stata modificata.
205	273	659	(Area riservata)	Char(20)	
225	293	679	Nome DLO	Char(12)	Il nome del DLO (document library object).
237	305	691	(Area riservata)	Char(8)	
245	313	699	Percorso cartella	Char(63)	La cartella in cui l'oggetto è stato ripristinato.
308			(Area riservata)	Char(20)	
	376	762	(Area riservata)	Char(18)	
	394	780	Lunghezza nome oggetto[1]	Binary (4)	La lunghezza del nome oggetto.
328	396	782	CCSID nome oggetto[1]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
332	400	786	ID paese o regione nome oggetto[1]	Char(2)	L'ID paese o regione per il nome oggetto.
334	402	788	ID lingua nome oggetto[1]	Char(3)	L'ID lingua per il nome oggetto.
337	405	791	(Area riservata)	Char(3)	
340	408	794	ID file principale[1,2]	Char(16)	L'ID file dell'indirizzario principale.
356	424	810	ID file oggetto[1,2]	Char(16)	L'ID file dell'oggetto.
372	440	826	Nome oggetto[1]	Char(512)	Il nome dell'oggetto.
	952	1338	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	968	1354	Nome ASP[5]	Char(10)	Il nome dell'unità ASP
	978	1364	Numero ASP[5]	Char(5)	Il numero dell'unità ASP.
	983	1369	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	987	1373	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	989	1375	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	992	1378	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.

Tabella 203. Voci di giornale RO (Modifica proprietà per oggetto ripristinato) (Continua). File descrizione campo QASYROJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
	994	1380	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	995	1381	ID file indirizzario relativo[3]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[3]
	1011	1397	Nome percorso[4]	Char(5002)	Il nome percorso dell'oggetto.

[1] Questi campi vengono utilizzati solo per oggetti nei file system "root" (/), QOpenSys e negli UDFS (user-defined file systems).

[2] Un ID con il bit all'estrema sinistra impostato ed il resto dei bit zero indica che l'ID NON è impostato.

[3] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[4] Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza del nome percorso.

[5] Se l'oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.

Voci di giornale RP (Ripristino programmi che adottano l'autorizzazione)

Questa tabella fornisce il formato delle voci di giornale RP (Ripristino programmi che adottano l'autorizzazione).

Tabella 204. Voci di giornale RP (Ripristino programmi che adottano l'autorizzazione). File descrizione campo QASYRPJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.

Tabella 204. Voci di giornale RP (Ripristino programmi che adottano l'autorizzazione) (Continua). File descrizione campo QASYRPJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Ripristino di programmi che adottano l'autorizzazione del proprietario
157	225	611	Nome programma	Char(10)	Il nome del programma
167	235	621	Libreria programma	Char(10)	Il nome della libreria dove è ubicato il programma.
177	245	631	Tipo di oggetto	Char(8)	Il tipo di oggetto
185	253	639	Nome proprietario	Char(10)	Nome del proprietario
	263	649	(Area riservata)	Char(18)	
	281	667	Lunghezza nome oggetto[1]	Binary (4)	La lunghezza del nome oggetto.
	283	669	CCSID nome oggetto[1]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
	287	673	ID paese o regione nome oggetto[1]	Char(2)	L'ID paese o regione per il nome oggetto.
	289	675	ID lingua nome oggetto[1]	Char(3)	L'ID lingua per il nome oggetto.
	292	678	(Area riservata)	Char(3)	
	295	681	ID file principale[1,2]	Char(16)	L'ID file dell'indirizzario principale.
	311	697	ID file oggetto[1,2]	Char(16)	L'ID file dell'oggetto.
	327	713	Nome oggetto[1]	Char(512)	Il nome dell'oggetto.
	839	1225	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	855	1241	Nome ASP[5]	Char(10)	Il nome dell'unità ASP
	865	1251	Numero ASP[5]	Char(5)	Il numero dell'unità ASP.
	870	1256	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	874	1260	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	876	1262	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	879	1265	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.

Tabella 204. Voci di giornale RP (Ripristino programmi che adottano l'autorizzazione) (Continua). File descrizione campo QASYRPJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	881	1267	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	882	1268	ID file indirizzario relativo[3]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[3]
	898	1284	Nome percorso[4]	Char(5002)	Il nome percorso dell'oggetto.

[1] Questi campi vengono utilizzati solo per oggetti nei file system "root" (/), QOpenSys e negli UDFS (user-defined file system).

[2] Se un ID ha il bit all'estrema sinistra impostato ed il resto dei bit hanno valore zero, l'ID non è impostato.

[3] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[4] Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza del nome percorso.

[5] Se l'oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.

Voci di giornale RQ (Ripristino oggetto descrittore richiesta di modifica)

Questa tabella fornisce il formato delle voci di giornale RQ (Ripristino oggetto descrittore richiesta di modifica).

Tabella 205. Voci di giornale RQ (Ripristino oggetto descrittore richiesta di modifica). File descrizione campo QASYRQJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.

Tabella 205. Voci di giornale RQ (Ripristino oggetto descrittore richiesta di modifica) (Continua). File descrizione campo QASYRQJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Ripristino oggetto *CRQD che adotta l'autorizzazione.
157	225	611	Nome oggetto	Char(10)	Il nome del descrittore richiesta di modifica.
167	235	621	Libreria oggetto	Char(10)	Il nome della libreria dove è stato reperito il descrittore richiesta di modifica.
177	245	631	Tipo di oggetto	Char(8)	Il tipo di oggetto.
		639	Nome ASP	Char(10)	Nome ASP per libreria CRQD
		649	Numero ASP	Char(5)	Numero ASP per libreria CRQD

Voci di giornale RU (Ripristino autorizzazione per profilo utente)

Questa tabella fornisce il formato delle voci di giornale RU (Ripristino autorizzazione per profilo utente).

Tabella 206. Voci di giornale RU (Ripristino autorizzazione per profilo utente). File descrizione campo QASYRUJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Ripristino autorizzazione per profili utente
157	225	611	Nome utente	Char(10)	Il nome del profilo utente la cui autorizzazione è stata ripristinata.
167	235	621	Nome libreria	Char(10)	Il nome della libreria.
177	245	631	Tipo di oggetto	Char(8)	Il tipo di oggetto.
	253	639	Autorizzazione ripristinata	Char(1)	Indica se tutte le autorizzazioni sono state ripristinate per l'utente. **A** Tutte le autorizzazioni sono state ripristinate **S** Alcune autorizzazioni non ripristinate

Voci di giornale RZ (Modifica gruppo principale per oggetto ripristinato)

Questa tabella fornisce il formato delle voci di giornale RZ (Modifica gruppo principale per oggetto ripristinato).

Tabella 207. Voci di giornale RZ (Modifica gruppo principale per oggetto ripristinato). File descrizione campo QASYRZJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Gruppo principale modificato.
157	225	611	Nome oggetto	Char(10)	Il nome dell'oggetto.
167	235	621	Libreria oggetto	Char(10)	Il nome della libreria dove è stato reperito l'oggetto.
177	245	631	Tipo di oggetto	Char(8)	Il tipo di oggetto.
185	253	639	Vecchio gruppo principale	Char(10)	Il precedente gruppo principale per l'oggetto.
195	263	649	Nuovo gruppo principale	Char(10)	Il nuovo gruppo principale per l'oggetto.
205	273	659	(Area riservata)	Char(20)	
225	293	679	Nome DLO	Char(12)	Il nome del DLO (document library object).
237	305	691	(Area riservata)	Char(8)	
245	313	699	Percorso cartella	Char(63)	La cartella in cui l'oggetto è stato ripristinato.
308			(Area riservata)	Char(20)	
	376	762	(Area riservata)	Char(18)	
	394	780	Lunghezza nome oggetto[1]	Binary (4)	La lunghezza del nome oggetto.
328	396	782	CCSID nome oggetto[1]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
332	400	786	ID paese o regione nome oggetto[1]	Char(2)	L'ID paese o regione per il nome oggetto.
334	402	788	ID lingua nome oggetto[1]	Char(3)	L'ID lingua per il nome oggetto.

Tabella 207. Voci di giornale RZ (Modifica gruppo principale per oggetto ripristinato) (Continua). File descrizione campo QASYRZJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
337	405	791	(Area riservata)	Char(3)	
340	408	794	ID file principale[1,2]	Char(16)	L'ID file dell'indirizzario principale.
356	424	810	ID file oggetto[1,2]	Char(16)	L'ID file dell'oggetto.
372	440	826	Nome oggetto[1]	Char(512)	Il nome dell'oggetto.
	952	1338	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	968	1354	Nome ASP	Char(10)	Il nome dell'unità ASP
	978	1364	Numero ASP	Char(5)	Il numero dell'unità ASP.
	983	1369	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	987	1373	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	989	1375	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	992	1378	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.
	994	1380	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	995	1381	ID file indirizzario relativo[3]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[3]
	1011	1397	Nome percorso[4]	Char(5002)	Il nome percorso dell'oggetto.

[1] Questi campi vengono utilizzati solo per oggetti nei file system "root" (/), QOpenSys e negli UDFS (user-defined file systems).

[2] Un ID con il bit all'estrema sinistra impostato ed il resto dei bit zero indica che l'ID NON è impostato.

[3] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.

[4] Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza del nome percorso.

Voci di giornale SD (Modifica indirizzario distribuzione sistema)

Questa tabella fornisce il formato delle voci di giornale SD (Modifica indirizzario distribuzione sistema).

Tabella 208. Voci di giornale SD (Modifica indirizzario distribuzione sistema). File descrizione campo QASYSDJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **S** Modifica indirizzario sistema
157	225	611	Tipo di modifica	Char(3)	**ADD** Aggiungere voce indirizzario **CHG** Modificare voce indirizzario **COL** Voce raccoglitore **DSP** Visualizzare voce indirizzario **OUT** Richiesta file di emissione **PRT** Stampare voce indirizzario **RMV** Eliminare voce indirizzario **RNM** Ridenominare voce indirizzario **RTV** Richiamare dettagli **SUP** Voce fornitore
160	228	614	Tipo di record	Char(4)	**DIRE** Indirizzario **DPTD** Dettagli reparto **SHDW** Shadow indirizzario **SRCH** Ricerca indirizzario
164	232	618	Sistema di origine	Char(8)	Il sistema che ha dato origine alla modifica
172	240	626	Profilo utente	Char(10)	Il profilo utente che effettua la modifica
182	250	636	Sistema richiedente	Char(8)	Il sistema che richiede la modifica

Tabella 208. Voci di giornale SD (Modifica indirizzario distribuzione sistema) (Continua). File descrizione campo QASYSDJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
190	258	644	Funzione richiesta	Char(6)	**INIT** Inizializzazione **OFFLIN** Inizializzazione fuori linea **REINIT** Reinizializzazione **SHADOW** Shadow normale **STPSHD** Arresto shadow
196	264	650	ID utente	Char(8)	L'ID utente modificato
204	272	658	Indirizzo	Char(8)	L'indirizzo modificato
212	280	666	ID utente di rete	Char(47)	ID utente di rete modificato

Voci di giornale SE (Modifica della voce di instradamento del sottosistema)

Questa tabella fornisce il formato delle voci di giornale SE (Modifica della voce di instradamento del sottosistema).

Tabella 209. Voci di giornale SE (Modifica della voce di instradamento del sottosistema). File descrizione campo QASYSEJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Voce di instradamento del sottosistema modificata
157	225	611	Nome sottosistema	Char(10)	Il nome dell'oggetto
167	235	621	Nome libreria	Char(10)	Il nome della libreria dove è memorizzato l'oggetto.
177	245	631	Tipo di oggetto	Char(8)	Il tipo di oggetto.
185	253	639	Nome programma	Char(10)	Il nome del programma che ha modificato la voce di instradamento

Tabella 209. Voci di giornale SE (Modifica della voce di instradamento del sottosistema) (Continua). File descrizione campo QASYSEJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
195	263	649	Nome libreria	Char(10)	Il nome della libreria per il programma
205	273	659	Numero di sequenza	Char(4)	Il numero di sequenza
209	277	663	Nome comando	Char(3)	Il tipo di comando utilizzato **ADD** ADDRTGE **CHG** CHGRTGE **RMV** RMVRTGE
		666	Nome ASP per libreria SBSD	Char(10)	Nome ASP per libreria SBSD
		676	Numero ASP per libreria SBSD	Char(5)	Numero ASP per libreria SBSD
		681	Nome ASP per libreria programma	Char(10)	Nome ASP per libreria programma
		691	Numero ASP per libreria programma	Char(5)	Numero ASP per libreria programma

Voci di giornale SF (Operazione su file di spool)

Questa tabella fornisce il formato delle voci di giornale SF (Operazione su file di spool).

Tabella 210. Voci di giornale SF (Operazione su file di spool). File descrizione campo QASYSFJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.

Tabella 210. Voci di giornale SF (Operazione su file di spool) (Continua). File descrizione campo QASYSFJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
156	224	610	Tipo accesso	Char(1)	Il tipo di voce **A** File di spool letto da un utente che non è il proprietario. **C** File di spool creato. **D** File di spool cancellato. **H** File di spool congelato. **I** Creazione di file in linea. **R** File di spool rilasciato. **S** File di spool salvato. **T** File di spool ripristinato. **U** Attributi file di spool rilevante per la sicurezza modificato. **V** Modificati solo attributi file di spool non rilevanti per la sicurezza.
157	225	611	Nome file di database	Char(10)	Il nome del file di database che contiene il file di spool
167	235	621	Nome libreria	Char(10)	Il nome della libreria relativa al file di database
177	245	631	Tipo di oggetto	Char(8)	Il tipo di oggetto del file di database
185	253	639	Area riservata	Char(10)	
195	263	649	Nome membro	Char(10)	Il nome del membro file.
205	273	659	Nome file di spool	Char(10)	Il nome del file di spool [1].
215	283	669	Numero file di spool breve	Char(4)	Il numero del file di spool [1]. Se tale numero è maggiore di 4 byte, questo campo risulterà vuoto e verrà utilizzato il campo Numero file di spool (J5 scostamento 693).
219	287	673	Nome coda di emissione	Char(10)	Il nome della coda di emissione che contiene il file di spool.
229	297	683	Libreria coda di emissione	Char(10)	Il nome della libreria relativa alla coda di emissione.
239			Area riservata	Char(20)	
	307	693	Numero file di spool	Char(6)	Il numero del file di spool.
	313	699	Area riservata	Char(14)	
259	327	713	Vecchie copie	Char(3)	Numero delle vecchie copie del file di spool
262	330	716	Nuove copie	Char(3)	Numero delle nuove copie del file di spool
265	333	719	Vecchia stampante	Char(10)	Vecchia stampante per il file di spool
275	343	729	Nuova stampante	Char(10)	Nuova stampante per il file di spool
285	353	739	Nuova coda di emissione	Char(10)	Nuova coda di emissione per il file di spool

Tabella 210. Voci di giornale SF (Operazione su file di spool) (Continua). File descrizione campo QASYSFJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
295	363	749	Libreria nuova coda di emissione	Char(10)	Libreria per la nuova coda di emissione
305	373	759	Vecchio tipo di formato	Char(10)	Vecchio tipo di formato del file di spool
315	383	769	Nuovo tipo di formato	Char(10)	Nuovo tipo di formato del file di spool
325	393	779	Vecchia pagina di riavvio	Char(8)	Vecchia pagina di riavvio per il file di spool
333	401	787	Nuova pagina di riavvio	Char(8)	Nuova pagina di riavvio per il file di spool
341	409	795	Vecchio inizio intervallo pagine	Char(8)	Vecchio inizio intervallo pagine del file di spool
349	417	803	Nuovo inizio intervallo pagine	Char(8)	Nuovo inizio intervallo pagine del file di spool
357	425	811	Vecchia fine intervallo pagine	Char(8)	Vecchia fine intervallo pagine del file di spool
365	433	819	Nuova fine intervallo pagine	Char(8)	Nuova fine intervallo pagine del file di spool
	441	827	Nome lavoro file di spool	Char(10)	Il nome del lavoro file di spool.
	451	837	Utente lavoro file di spool	Char(10)	L'utente per il lavoro file di spool.
	461	847	Numero lavoro file di spool	Char(6)	Il numero del lavoro file di spool.
	467	853	Vecchio cassetto	Char(8)	Vecchio cassetto origine.
	475	861	Nuovo cassetto	Char(8)	Nuovo cassetto origine.
	483	869	Vecchio nome definizione pagina	Char(10)	Vecchio nome definizione pagina.
	493	879	Libreria vecchia definizione pagina	Char(10)	Nome libreria vecchia definizione pagina.
	503	889	Nuovo nome definizione pagina	Char(10)	Nuovo nome definizione pagina.
	513	899	Libreria nuova definizione pagina	Char(10)	Libreria nuova definizione pagina.
	523	909	Vecchio nome definizione formato	Char(10)	Vecchio nome definizione formato.

Tabella 210. Voci di giornale SF (Operazione su file di spool) (Continua). File descrizione campo QASYSFJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	533	919	Libreria vecchia definizione formato	Char(10)	Nome libreria vecchia definizione formato.
	543	929	Nome della nuova definizione formato	Char(10)	Nome della nuova definizione formato
	553	939	Libreria nuova definizione formato	Char(10)	Nome libreria nuova definizione formato.
	563	949	Vecchia opzione 1 definita dall'utente	Char(10)	Vecchia opzione 1 definita dall'utente.
	573	959	Vecchia opzione 2 definita dall'utente	Char(10)	Vecchia opzione 2 definita dall'utente.
	583	969	Vecchia opzione 3 definita dall'utente	Char(10)	Vecchia opzione 3 definita dall'utente.
	593	979	Vecchia opzione 4 definita dall'utente	Char(10)	Vecchia opzione 4 definita dall'utente.
	603	989	Nuova opzione 1 definita dall'utente	Char(10)	Nuova opzione 1 definita dall'utente.
	613	999	Nuova opzione 2 definita dall'utente	Char(10)	Nuova opzione 2 definita dall'utente.
	623	1009	Nuova opzione 3 definita dall'utente	Char(10)	Nuova opzione 3 definita dall'utente.
	633	1019	Nuova opzione 4 definita dall'utente	Char(10)	Nuova opzione 4 definita dall'utente.
	643	1029	Vecchio oggetto definito dall'utente	Char(10)	Nome vecchio oggetto definito dall'utente.
	653	1039	Vecchia libreria oggetti definita dall'utente	Char(10)	Vecchio nome libreria definita dall'utente.
	663	1049	Vecchio tipo oggetto definito dall'utente	Char(10)	Vecchio tipo oggetto definito dall'utente.

Tabella 210. Voci di giornale SF (Operazione su file di spool) (Continua). File descrizione campo QASYSFJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	673	1059	Nuovo oggetto definito dall'utente	Char(10)	Nuovo oggetto definito dall'utente.
	683	1069	Nuova libreria oggetti definita dall'utente	Char(10)	Nuovo nome libreria oggetti definita dall'utente.
	693	1079	Nuovo tipo oggetto definito dall'utente	Char(10)	Nuovo tipo oggetto definito dall'utente.
	703	1089	Nome sistema lavoro file di spool	Char(8)	Il nome del sistema nel quale risiede il file di spool.
	711	1097	Data creazione file di spool	Char (7)	La data di creazione del file di spool (SAAMMGG).
	718	1104	Ora di creazione del file di spool	Char(6)	L'ora della creazione del file di spool (HHMMSS).
		1110	Nome dei vecchi dati definiti dall'utente	Char(255)	Nome dei vecchi dati definiti dall'utente
		1365	Nome di nuovi dati definiti dall'utente	Char(255)	Nome di nuovi dati definiti dall'utente
		1620	Nome ASP file	Char(10)	Nome ASP per libreria file di database.
		1630	Numero ASP file	Char(5)	Numero ASP per libreria file di database.
		1635	Nome ASP coda di emissione	Char(10)	Nome ASP per la libreria coda di emissione.
		1645	Numero ASP coda di emissione	Char(5)	Numero ASP per la libreria coda di emissione.
		1650	Nome ASP nuova coda di emissione	Char(10)	Nome ASP per la libreria nuova coda di emissione.
		1660	Numero ASP nuova coda di emissione	Char(5)	Numero ASP per la libreria nuova coda di emissione.
		1665	Stato file di spool obsoleto	Char(3)	Stato file di spool obsoleto
		1668	Stato nuovo file di spool	Char(3)	Stato nuovo file di spool
		1671	Data di creazione originale	Char(7)	Data di creazione originale

Tabella 210. Voci di giornale SF (Operazione su file di spool) (Continua). File descrizione campo QASYSFJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
		1678	Ora di creazione originale	Char(6)	Ora di creazione originale
		1684	Data di scadenza file di spool obsoleto	Char(7)	Data di scadenza file di spool obsoleto
		1687	Data di scadenza nuovo file di spool	Char(7)	Data di scadenza nuovo file di spool
		1694	UTC data creazione file di spool	Char(7)	La data di creazione del file di spool in UTC (È la stessa data della Data di creazione file di spool (scostamento 1097) solo in UTC)
		1701	UTC ora di creazione del file di spool	Char(6)	L'ora di creazione del file di spool in UTC (È la stessa ora della Ora di creazione file di spool (scostamento 1104) solo in UTC)

[1] Questo campo è vuoto quando il tipo di voce è I (stampa in linea).

Voci di giornale SG (Segnali asincroni)

Questa tabella fornisce il formato delle voci di giornale SG (Segnali asinmcroni).

Tabella 211. Voci di giornale SG (Segnali asincroni). File descrizione campo QQASYSGJ4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 per l'elenco dei campi.
	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Segnale i5/OS asincrono elaborato **P** Segnale PASE (Private Address Space Environment) asincrono elaborato
	225	611	Numero segnale	Char(4)	Il numero segnale che è stato elaborato.

Tabella 211. Voci di giornale SG (Segnali asincroni) (Continua). File descrizione campo QQASYSGJ4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
	229	615	Azione di gestione	Char(1)	L'azione intrapresa sul segnale. **C** Continuare il processo **E** Eccezione segnale **H** Gestire richiamando la funzione di cattura segnale **S** Arrestare il processo **T** Terminare il processo **U** Terminare la richiesta
	230	616	Origine segnale	Char(1)	L'origine del segnale. **M** Origine macchina **P** Origine processo **Nota:** quando il valore dell'origine segnale è rappresentato da una macchina, i valori lavoro origine sono vuoti.
	231	617	Nome lavoro origine	Char(10)	La prima parte del nome completo del lavoro origine.
	241	627	Nome utente lavoro origine	Char(10)	La seconda parte del nome completo del lavoro origine.
	251	637	Numero lavoro origine	Char(6)	La terza parte del nome completo lavoro origine.
	257	643	Utente corrente lavoro origine	Char(10)	Il profilo utente corrente per il lavoro origine.
	267	653	Registrazione data/ora di creazione	Char(8)	Il formato *DTS dell'ora in cui è stato creato il segnale. **Nota:** è possibile utilizzare l'API QWCCVTDT per convertire una registrazione data/ora *DTS in altri formati.

Voci di giornale SK (Connessioni socket protette)

Questa tabella fornisce il formato delle voci di giornale SK (Connessioni socket protette).

Tabella 212. Voci di giornale SK (Connessioni socket protette). File descrizione campo QASYSKJ4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 per l'elenco dei campi.

Tabella 212. Voci di giornale SK (Connessioni socket protette) (Continua). File descrizione campo QASYSKJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	224	610	Tipo di voce	Char(1)	**A** Accettare **C** Collegarsi **D** Indirizzo DHCP assegnato **F** Posta filtrata **P** Porta non disponibile **R** Respingere posta **U** Indirizzo DHCP non assegnato
	225	611	Indirizzo IP locale[3]	Char(15)	L'indirizzo IP locale.
	240	626	Porta locale	Char(5)	La porta locale.
	245	631	Indirizzo IP remoto[3]	Char(15)	L'indirizzo IP remoto.
	260	646	Porta remota	Char(5)	La porta remota.
	265	651	Descrittore socket	Bin(5)	Il descrittore socket.
	269	655	Descrizione filtro	Char(10)	Il filtro posta specificato.
	279	665	Lunghezza dati filtro	Bin(4)	La lunghezza dei dati filtro.
	281	667	Dati filtro[1]	Char(514)	I dati filtro.
	795	1181	Famiglia indirizzi	Char(10)	La famiglia di indirizzi. ***IPV4** Internet Protocol Versione 4 ***IPV6** Internet Protocol Versione 6
	805	1191	Indirizzo IP locale	Char(46)	L'indirizzo IP locale.
	851	1237	Indirizzo IP remoto [2]	Char(46)	L'indirizzo IP remoto
	897	1283	Indirizzo MAC	Char(32)	L'indirizzo MAC del client richiedente.
	929	1315	Nome host	Char(255)	Il nome host del cliente richiedente.

[1] Questo è un campo a lunghezza variabile. I primi due byte contengono la lunghezza del campo.

[2] Quando il tipo di voce è D, questo campo contiene l'indirizzo IP che il server DHCP ha assegnato al client richiedente.

[3] Questi campi supportano solo indirizzi IPv4.

Voci di giornale SM (Modifica gestione sistemi)

Questa tabella fornisce il formato delle voci di giornale SM (Modifica gestione sistemi).

Tabella 213. Voci di giornale SM (Modifica gestione sistemi). File descrizione campo QASYSMJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Funzione a cui si è avuto accesso **B** Elenco copia di riserva modificato **C** Opzioni di ripulitura automatica **D** DRDA **F** File system HFS **N** Operazione file di rete **O** Opzioni di copia di riserva modificate **P** Pianificazione accensione/spegnimento **S** Elenco risposte di sistema **T** Ore di ripristino del percorso di accesso modificate
157	225	611	Tipo accesso	Char(1)	**A** Aggiunta **C** Modifica **D** Cancellazione **R** Eliminazione **S** Visualizzazione **T** Richiamo o ricezione
158	226	612	Numero di sequenza	Char(4)	Numero di sequenza dell'operazione
162	230	616	ID messaggio	Char (7)	ID messaggio associato all'operazione
169	237	623	Nome database relazionale	Char(18)	Nome del database relazionale
187	255	641	Nome file system	Char(10)	Nome del file system
197	265	651	Opzione copia di riserva modificata	Char(10)	L'opzione copia di riserva che è stata modificata
207	275	661	Modifica elenco copia di riserva	Char(10)	Il nome dell'elenco copia di riserva che è stato modificato
217	285	671	Nome file di rete	Char(10)	Il nome del file di rete che è stato utilizzato

Tabella 213. Voci di giornale SM (Modifica gestione sistemi) (Continua). File descrizione campo QASYSMJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
227	295	681	Membro file di rete	Char(10)	Il nome del membro del file di rete
237	305	691	Numero file di rete	Zoned(6,0)	Il numero del file di rete
243	311	697	Proprietario file di rete	Char(10)	Il nome del profilo utente proprietario del file di rete
253	321	707	Utente che dà origine al file di rete	Char(8)	Il nome del profilo utente che ha dato origine al file di rete
261	329	715	Indirizzo che dà origine al file di rete	Char(8)	L'indirizzo che ha dato origine al file di rete

Voci di giornale SO (Operazioni di informazioni utente sicurezza server)

Questa tabella fornisce il formato delle voci di giornale SO (Operazioni di informazioni utente sicurezza server).

Tabella 214. Voci di giornale SO (Operazioni di informazioni utente sicurezza server). File descrizione campo QASYSOJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce **A** Aggiungere voce **C** Modificare voce **R** Eliminare voce **T** Richiamare voce
157	225	611	Profilo utente	Char(10)	Il nome del profilo utente.
	235	621	Tipo di voce informazioni utente	Char(1)	**N** Tipo di voce non specificato. **U** La voce è una voce di informazioni applicazione utente. **Y** La voce è una voce di autenticazione server.

Tabella 214. Voci di giornale SO (Operazioni di informazioni utente sicurezza server) (Continua). File descrizione campo QASYSOJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	236	622	Parola d'ordine memorizzata	Char(1)	**N** Parola d'ordine non memorizzata **S** Nessuna modifica **Y** La parola d'ordine è stata memorizzata.
	237	623	Nome server	Char(200)	Il nome del server.
	437	823	(Area riservata)	Char(3)	
	440	826	Lunghezza ID utente	Binary (4)	La lunghezza dell'ID utente.
	442	828	(Area riservata)	Char(20)	
	462	848	ID utente	Char(1002)[1]	L'ID per l'utente.

[1] Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza del campo.

Voci di giornale ST (Operazione programmi di manutenzione)

Questa tabella fornisce il formato delle voci di giornale ST (Operazione programmi di manutenzione).

Tabella 215. Voci di giornale ST (Operazione programmi di manutenzione). File descrizione campo QASYSTJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce **A** Record servizio

Tabella 215. Voci di giornale ST (Operazione programmi di manutenzione) (Continua). File descrizione campo QASYSTJE/J4/J5

Scost.			Campo	Formato	Descrizione	
JE	**J4**	**J5**				
157	225	611	Programma di manutenzione	Char(2)	Il tipo di voce.	
					AN	ANZJVM
					AR	Traccia di diagnostica ARM (vedere comando ARMSRV QShell)
					CD	QTACTLDV, QTADMPDV
					CE	QWTCTLTR
					CS	STRCPYSCN
					CT	DMPCLUTRC
					DC	DLTCMNTRC
					DD	DMPDLO
					DF	QWTDMPFR, QWTDMPLF
					DI	QSCDIRD
					DJ	DMPJVM, QPYRTJVM
					DM	DMPMEMINF
					DO	DMPOBJ
					DS	DMPSYSOBJ, QTADMPTS, QTADMPDV, QWTDMPLF
					DU	DMPUSRPRF
					DW	STRDW, ENDDW, ADDDWDFN, RMVDWDFN
					EC	ENDCMNTRC
					ER	ENDRMTSPT
					GS	QSMGSSTD
					HD	QYHCHCOP (DASD)
					HL	QYHCHCOP (LPAR)
					JW	STRJW, ENDJW, ADDJWDFN, RMVJWDFN
					LC	Creato EPT
					LD	Cancellato EPT
					LE	L'EPT per il lavoro è stato modificato
					LF	L'EPT di sistema è stato corretto
					LG	le voci nell'EPT sono state modificate
					LH	EPT confrontato

Tabella 215. Voci di giornale ST (Operazione programmi di manutenzione) (Continua). File descrizione campo QASYSTJE/J4/J5

Scost.			Campo	Formato	Descrizione	
JE	J4	J5				
					LI	Voci EPT visualizzate
					MC	QWTMAINT (modifica)
					MD	QWTMAINT (dump)
					MP	Fine lavoro di sistema
					MQ	Riavvio lavoro di sistema
					OP	Operations console
					PC	PRTCMNTRC
					PE	PRTERRLOG, QTADMPDV
					PI	PRTINTDTA, QTADMPDV
					PS	QP0FPTOS
					SC	STRCMNTRC
					SE	QWTSETTR
					SF	QWCCDSIC, QWVRCSTK (Visualizzazione voce stack interno)
					SJ	STRSRVJOB
					SN	QPZSYNC
					SR	STRRMTSPT
					SS	QFPHPSF
					ST	STRSST
					SV	QSRSRV
					TA	TRCTCPAPP
					TC	TRCCNN (*FORMAT specificato)
					TE	ENDTRC, ENDPEX, TRCJOB(specificato *OFF o *END)
					TI	TRCINT o TRCCNN con SET(*ON), SET(*OFF) o SET(*END)
					TO	QTOBSRV
					TQ	QWCTMQTM
					TS	STRTRC, STRPEX, TRCJOB(*ON specificato)
					UD	QTAUPDDV
					WE	ENDWCH, QSCEWCH
					WS	STRWCH, QSCSWCH
					WT	WRKTRC
					WW	WRKWCH
159	227	613	Nome oggetto	Char(10)	Nome dell'oggetto a cui si è avuto accesso	

Tabella 215. Voci di giornale ST (Operazione programmi di manutenzione) (Continua). File descrizione campo QASYSTJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
169	237	623	Nome libreria	Char(10)	Nome della libreria per l'oggetto
179	247	633	Tipo oggetto	Char(8)	Tipo di oggetto
187	255	641	Nome lavoro	Char(10)	La prima parte del nome lavoro completo
197	265	651	Nome utente lavoro	Char(10)	La seconda parte del nome lavoro completo
207	275	661	Numero lavoro	Zoned(6,0)	La terza parte del nome lavoro completo
213	281	667	Nome oggetto	Char(30)	Nome dell'oggetto per DMPSYSOBJ
243	311	697	Nome libreria	Char(30)	Nome della libreria relativa all'oggetto per DMPSYSOBJ
273	341	727	Tipo oggetto	Char(8)	Tipo dell'oggetto
281	349	735	Nome DLO	Char(12)	Nome del DLO (document library object)
293	361	747	(Area riservata)	Char(8)	
301	369	755	Percorso cartella[8]	Char(63)	La cartella contenente il DLO (document library object)
	432	818	Campo JUID	Char(10)	Il JUID del lavoro di destinazione
	442	828	Operazione traccia iniziale[1]	Char(10)	L'operazione richiesta per la traccia lavoro iniziale ***ON** Traccia iniziale attivata ***OFF** Traccia iniziale disattivata ***RESET** Traccia iniziale disattivata ed informazioni sulla cancellate.
	452	838	Opzione traccia applicazione[2]	Char(1)	L'opzione traccia specificata su TRCTCPAPP. **A**[6] Attivazione **D**[6] Disattivazione **Y**[7] Raccolta delle informazioni di traccia avviata **N**[7] Raccolta di informazioni di traccia arrestata e informazioni di traccia scritte nel file di spool **E**[7] Raccolta di informazioni di traccia terminata e tutte le informazioni di traccia eliminate (nessuna emissione creata)
	453	839	Eseguita traccia della applicazione[2]	Char(10)	Il nome dell'applicazione di cui si è eseguita la traccia.
	463	849	Profilo programmi di manutenzione[3]	Char(10)	Il nome del profilo dei programmi di manutenzione utilizzato per STRSST.
		859	ID nodo origine	Char(8)	ID nodo origine
		867	Utente origine	Char(10)	Utente origine

Tabella 215. Voci di giornale ST (Operazione programmi di manutenzione) (Continua). File descrizione campo QASYSTJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
		877	Nome ASP per libreria oggetto	Char(10)	Nome ASP per libreria oggetto
		887	Numero ASP per libreria oggetto	Char(5)	Numero ASP per libreria oggetto
		892	Nome ASP per libreria oggetto DMPSYSOBJ	Char(10)	Nome ASP per libreria oggetto DMPSYSOBJ
		902	Numero ASP per libreria oggetto DMPSYSOBJ	Char(5)	Numero ASP per libreria oggetto DMPSYSOBJ
		907	Tipo di console [4]	Char(10)	Il tipo di console. Valori possibili sono: • *DIRECT • *LAN • *HMC
		917	Azione della console [4]	Char(10)	L'azione della console. Valori possibili sono: • *RECOVERY • *TAKEOVER
		927	Famiglia di indirizzi [4]	Char(10)	La famiglia di indirizzi. • *IPv4 • *IPv6
		937	Indirizzo IP precedente [4]	Char(46)	L'indirizzo IP dell'unità console precedente per *LAN.
		938	ID dispositivo precedente[4]	Char(10)	L'ID dispositivo dei programmi di manutenzione dell'unità console precedente per *LAN.
		993	Indirizzo IP corrente [4]	Char(46)	L'indirizzo IP dell'unità console corrente per *LAN.
		1039	ID dispositivo corrente [4]	Char(10)	L'ID dispositivo dei programmi di manutenzione dell'unità console corrente per *LAN.
		1049	Sessione di visualizzazione [5]	Char(10)	ID della sessione di visualizzazione.
		1059	Voce[9]	Char(10)	Nome della voce nella tabella del punto di immissione che è stato modificato.

Tabella 215. Voci di giornale ST (Operazione programmi di manutenzione) (Continua). File descrizione campo QASYSTJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
		1069	Oggetto correlato[10]	Char(10)	Nome dell'oggetto correlato. • Per valore LC del programma di manutenzione, questo campo contiene il nome della tabella punto di immissione di base. • Per valore LG del programma di manutenzione, questo campo contiene il nome del programma di sostituzione. • Per valore LH del programma di manutenzione, questo campo contiene il nome della tabella punto di immissione di confronto.
		1079	Libreria oggetti correlati[10]	Char(10)	Nome della libreria oggetti correlati. • Per valore LC del programma di manutenzione, questo campo contiene il nome della libreria tabella punto di immissione di base. • Per valore LG del programma di manutenzione, questo campo contiene il nome della libreria programma di sostituzione. • Per valore LH del programma di manutenzione, questo campo contiene il nome della libreria tabella punto di immissione di confronto.

[1] Questo campo viene utilizzato solo quando il valore del programma di manutenzione (scostamento 611) è CE.

[2] Questo campo viene utilizzato solo quando il valore del programma di manutenzione (scostamento 611) è AR o TA.

[3] Questo campo viene utilizzato solo quando il valore del programma di manutenzione (scostamento 611) è ST o OP.

[4] Questo campo viene utilizzato solo quando il valore del programma di manutenzione (scostamento 611) è OP.

[5] Questo campo viene utilizzato solo quando il valore del programma di manutenzione (scostamento 611) è WS o WE.

[6] Questo campo viene utilizzato solo quando il valore del programma di manutenzione (scostamento 611) è AR.

[7] Questo campo viene utilizzato solo quando il valore del programma di manutenzione (scostamento 611) è TA.

[8] Il Percorso cartella conterrà un nome AAC (comando di analisi avanzata) composto da 30 caratteri quando il valore programma di manutenzione (scostamento 611) è GS.

[9] Questo campo viene utilizzato solo quando il valore del programma di manutenzione (scostamento 611) è LG.

[10] Questo campo viene utilizzato solo quando il valore del programma di manutenzione (scostamento 611) è LC, LG o LH.

Voci di giornale SV (Operazione su valore di sistema)

Questa tabella fornisce il formato delle voci di giornale SV (Operazione su valore di sistema).

Tabella 216. Voci di giornale SV (Operazione su valore di sistema). File descrizione campo QASYSVJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Modificare in valori di sistema **B** Modificare in attributi di sistema **C** Modificare in orologio di sistema **D** Adattamento all'UTC (Coordinated Universal Time) **E** Modificare in opzione **F** Modificare nell'attributo del giornale dell'intero sistema
157	225	611	Valore di sistema o attributo di servizio	Char(10)	**JRNRCVCNT** Valore conteggio ripristino giornale modificato **MAXCCHWAIT** Tempo di attesa massimo memoria cache giornale modificato **QINPIDCO** modificare l'opzione di configurazione disco installazione corrente con L'API QINPIDCO.
167	235	621	Nuovo valore	Char(250)	Il valore nel quale il valore di sistema o l'attributo di servizio è stato modificato
417	485	871	Vecchio valore	Char(250)	Il valore del valore di sistema o dell'attributo di servizio prima che venisse modificato
667	735	1121	Nuovo valore continuato	Char(250)	La continuazione del valore nel quale il valore di sistema o l'attributo di servizio è stato modificato.
917	985	1371	Vecchio valore continuato	Char(250)	Continuazione del valore del valore di sistema o dell'attributo del servizio prima della modifica.
		1621	Estensione nuovo valore continuato	Char(1000)	Seconda continuazione del valore in cui il valore di sistema o l'attributo del servizio sono stati modificati.
		2621	Estensione vecchio valore continuato	Char(1000)	Seconda continuazione del valore del valore di sistema o dell'attributo di servizio prima della modifica.

Voci di giornale VA (Modifica dell'elenco controllo accesso)

Questa tabella fornisce il formato delle voci di giornale VA (Modifica dell'elenco controllo accesso.

Tabella 217. Voci di giornale VA (Modifica dell'elenco controllo accesso). File descrizione campo QASYVAJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Stato	Char(1)	Stato della richiesta. **S** Esito positivo **F** Esito negativo
157	225	611	Nome server	Char(10)	Il nome della descrizione server di rete che ha registrato l'evento.
167	235	621	Data server	Char(6)	La data in cui l'evento è stato registrato sul server di rete.
173	241	627	Ora server	Zoned(6,0)	L'ora in cui l'evento è stato registrato sul server di rete.
179	247	633	Nome computer	Char(8)	Il nome del computer che emette la richiesta di modifica dell'elenco controllo accesso.
187	255	641	Nome richiedente	Char(10)	Il nome dell'utente che emette la richiesta.
197	265	651	Operazione eseguita	Char(1)	L'operazione eseguita sul profilo controllo accesso: **A** Aggiunta **C** Modifica **D** Cancellazione
198	266	652	Nome risorsa	Char(260)	Il nome della risorsa da modificare.

Voci di giornale VC (Avvio e fine collegamento)

Questa tabella fornisce il formato delle voci di giornale VC (Avvio e fine collegamento).

Tabella 218. Voci di giornale VC (Avvio e fine collegamento). File descrizione campo QASYVCJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Operazione di collegamento.	Char(1)	L'operazione di collegamento che si è verificata. **S** Avvio **E** Fine **R** Respingere
157	225	611	Nome server	Char(10)	Il nome della descrizione server di rete che ha registrato l'evento.
167	235	621	Data server	Char(6)	La data in cui l'evento è stato registrato sul server di rete.
173	241	627	Ora server	Zoned(6,0)	L'ora in cui l'evento è stato registrato sul server di rete.
179	247	633	Nome computer	Char(8)	Il nome del computer associato alla richiesta di collegamento.
187	255	641	Utente collegamento	Char(10)	Il nome dell'utente associato alla richiesta di collegamento.
197	265	651	ID collegamento	Char(5)	L'ID di avvio e fine collegamento.
202	270	656	Motivo del rifiuto	Char(1)	La ragione per cui è stato respinto il collegamento: **A** Scollegamento automatico (supero tempo), condivisione eliminata o mancanza delle autorizzazione di gestione **E** Errore, scollegamento sessione o parola d'ordine non corretta **N** Normale scollegamento o limite nome utente **P** Nessuna autorizzazione all'accesso per la risorsa condivisa
203	271	657	Nome rete	Char(12)	Il nome rete associato al collegamento.

Voci di giornale VF (Chiusura dei file server)

Questa tabella fornisce il formato delle voci di giornale VF (Chiusura dei file server).

Tabella 219. Voci di giornale VF (Chiusura dei file server). File descrizione campo QASYVFJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Motivo della chiusura	Char(1)	Il motivo per cui è stato chiuso il file. **A** Scollegamento di gestione **N** Scollegamento client normale **S** Scollegamento di gestione
157	225	611	Nome server	Char(10)	Il nome della descrizione server di rete che ha registrato l'evento.
167	235	621	Data server	Char(6)	La data in cui l'evento è stato registrato sul server di rete.
173	241	627	Ora server	Zoned(6,0)	L'ora in cui l'evento è stato registrato sul server di rete.
179	247	633	Nome computer	Char(8)	Il nome del computer che richiede la chiusura.
187	255	641	Utente collegamento	Char(10)	Il nome dell'utente che richiede la chiusura.
197	265	651	ID file	Char(5)	L'ID del file in fase di chiusura.
202	270	656	Durata	Char(6)	Il numero di secondi in cui il file è rimasto aperto.
208	276	662	Nome risorsa	Char(260)	Il nome della risorsa che possiede il file a cui si è avuto accesso.

Voci di giornale VL (Limite account superato)

Questa tabella fornisce il formato delle voci di giornale VL (Limite account superato).

Tabella 220. Voci di giornale VL (Limite account superato). File descrizione campo QASYVLJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.

Tabella 220. Voci di giornale VL (Limite account superato) (Continua). File descrizione campo QASYVLJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
156	224	610	Causa	Char(1)	Il motivo per cui è stato superato il limite. **A** Account scaduto **D** Account disabilitato **L** Ore di collegamento superate **U** Sconosciuto o non disponibile **W** Stazione di lavoro non valida
157	225	611	Nome server	Char(10)	Il nome della descrizione server di rete che ha registrato l'evento.
167	235	621	Data server	Char(6)	La data in cui l'evento è stato registrato sul server di rete.
173	241	627	Ora server	Zoned(6,0)	L'ora in cui l'evento è stato registrato sul server di rete.
179	247	633	Nome computer	Char(8)	Il nome del computer con la violazione del limite account.
187	255	641	Profilo	Char(10)	Il nome dell'utente con la violazione limite account.
197	265	651	Nome risorsa	Char(260)	Il nome della risorsa che viene utilizzata.

Voci di giornale VN (Collegamento e scollegamento rete)

Questa tabella fornisce il formato delle voci di giornale VN (Collegamneto e scollegamento rete).

Tabella 221. Voci di giornale VN (Collegamento e scollegamento rete). File descrizione campo QASYVNJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo registrazione	Char(1)	Il tipo di evento che si è verificato: **F** Scollegamento richiesto **O** Collegamento richiesto **R** Collegamento rifiutato
157	225	611	Nome server	Char(10)	Il nome della descrizione server di rete che ha registrato l'evento.
167	235	621	Data server	Char(6)	La data in cui l'evento è stato registrato sul server di rete.
173	241	627	Ora server	Zoned(6,0)	L'ora in cui l'evento è stato registrato sul server di rete.

Tabella 221. Voci di giornale VN (Collegamento e scollegamento rete) (Continua). File descrizione campo QASYVNJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
179	247	633	Nome computer	Char(8)	Il nome del computer per l'evento.
187	255	641	Profilo	Char(10)	L'utente che si è collegato o scollegato.
197	265	651	Privilegio utente	Char(1)	Privilegio dell'utente che effettua il collegamento: **A** Amministratore **G** Ospite **U** Profilo
198	266	652	Motivo del rifiuto	Char(1)	La ragione per cui è stato respinto il tentativo di collegamento: **A** Accesso negato **F** Scollegamento forzato a causa di limite collegamento **P** Parola d'ordine non corretta
199	267	653	Ulteriore motivazione	Char(1)	Dettagli sul perché è stato negato l'accesso: **A** Account scaduto **D** Account disabilitato **L** Ore di collegamento non valide **R** ID richiedente non valido **U** Sconosciuto o non disponibile

Voci di giornale VO (Elenco di convalida)

Questa tabella fornisce il formato delle voci di giornale VO (Elenco di convalida).

Tabella 222. Voci di giornale VO (Elenco di convalida). File descrizione campo QASYVOJ4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 per l'elenco dei campi.

Tabella 222. Voci di giornale VO (Elenco di convalida) (Continua). File descrizione campo QASYVOJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	224	610	Tipo di voce	Char(1)	Il tipo di voce. **A** Aggiunta voce elenco di convalida **C** Modifica voce elenco di convalida **F** Individuazione voce elenco di convalida **R** Eliminazione voce elenco di convalida **U** Verifica con esito negativo di una voce elenco di convalida **V** Verifica con esito positivo di una voce elenco di convalida
	225	611	Tipo di esito negativo	Char(1)	Tipo di verifica con esito negativo. **E** I dati codificati non sono corretti **I** L'ID voce non è stato trovato **V** L'elenco di convalida non è stato trovato
	226	612	Elenco di convalida	Char(10)	Il nome dell'elenco di convalida.
	236	622	Nome libreria	Char(10)	Il nome della libreria in cui si trova l'elenco di convalida.
	246	632	Dati codificati	Char(1)	Valore dei dati da codificare **Y** I dati da codificare sono stati specificati nella richiesta. **N** I dati da codificare non sono stati specificati nella richiesta
	247	633	Dati voce	Char(1)	Valori dati voce **Y** I dati voce sono stati specificati nella richiesta. **N** I dati voce non sono stati specificati nella richiesta
	248	634	Lunghezza ID voce	Binary (4)	La lunghezza dell'ID voce.
	250	636	Lunghezza dati	Binary (4)	La lunghezza dei dati della voce.
	252	638	Attributo dati codificati	Char(1)	Dati codificati. **' '** L'attributo dati codificato non è stato specificato. **0** I dati da codificare possono essere solo utilizzati per verificare una voce. Questa è l'impostazione predefinita. **1** I dati da codificare possono essere utilizzati per verificare una voce ed i dati possono essere restituiti in un'operazione di ricerca.
	253	639	Attributo Certificato X.509	Char(1)	Certificato X.509.

Tabella 222. Voci di giornale VO (Elenco di convalida) (Continua). File descrizione campo QASYVOJ4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
	254	640	(Area riservata)	Char (28)	
	282	668	ID voce	Byte(100)	L'ID voce.
	382	768	Dati voce	Byte(1000)	I dati della voce.
		1768	Nome ASP per libreria elenco di convalida	Char(10)	Nome ASP per libreria elenco di convalida
		1778	Numero ASP per libreria elenco di convalida	Char(5)	Numero ASP per libreria elenco di convalida

Voci di giornale VP (Errore parola d'ordine di rete)

Questa tabella fornisce il formato delle voci di giornale VP (Errore parola d'ordine di rete).

Tabella 223. Voci di giornale VP (Errore parola d'ordine di rete). File descrizione campo QASYVPJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di errore	Char(1)	Il tipo di errore che si è verificato. **P** Errore parola d'ordine
157	225	611	Nome server	Char(10)	Il nome della descrizione server di rete che ha registrato l'evento.
167	235	621	Data server	Char(6)	La data in cui l'evento è stato registrato sul server di rete.
173	241	627	Ora server	Zoned(6,0)	L'ora in cui l'evento è stato registrato sul server di rete.
179	247	633	Nome computer	Char(8)	Il nome del computer che ha iniziato la richiesta.
187	255	641	Profilo	Char(10)	Il nome dell'utente che ha tentato il collegamento.

Voci di giornale VR (Accesso risorsa di rete)

Questa tabella fornisce il formato delle voci di giornale VR (Accesso risorsa di rete).

Tabella 224. Voci di giornale VR (Accesso risorsa di rete). File descrizione campo QASYVRJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Stato	Char(1)	Lo stato dell'accesso. **F** Accesso alla risorsa non riuscito **S** Accesso alla risorsa riuscito
157	225	611	Nome server	Char(10)	Il nome della descrizione server di rete che ha registrato l'evento.
167	235	621	Data server	Char(6)	La data in cui l'evento è stato registrato sul server di rete.
173	241	627	Ora server	Zoned(6,0)	L'ora in cui l'evento è stato registrato sul server di rete.
179	247	633	Nome computer	Char(8)	Il nome del computer che richiede la risorsa.
187	255	641	Profilo	Char(10)	Il nome dell'utente che richiede la risorsa.
197	265	651	Tipo di operazione	Char(1)	Il tipo di operazione che viene eseguita: **A** Attributi risorsa modificati **C** Istanza della risorsa creata **D** Risorsa cancellata **P** Autorizzazioni della risorsa modificate **R** Dati letti o scritti da una risorsa **W** Dati scritti in una risorsa **X** Risorsa eseguita
198	266	652	Codice di errore	Char(4)	Il codice di errore ricevuto se è stato concesso l'accesso alla risorsa.
202	270	656	Messaggio server	Char(4)	Il codice messaggio inviato quando si concede l'accesso.
206	274	660	ID file	Char(5)	L'ID del file a cui si accede.
211	279	665	Nome risorsa	Char(260)	Il nome della risorsa che viene utilizzata.

Voci di giornale VS (Sessione server)

Questa tabella fornisce il formato delle voci di giornale VS (Sessione server).

Tabella 225. Voci di giornale VS (Sessione server). File descrizione campo QASYVSJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Operazione sessione	Char(1)	L'operazione sessione che si è verificata. **E** Fine sessione **S** Avvio sessione
157	225	611	Nome server	Char(10)	Il nome della descrizione server di rete che ha registrato l'evento.
167	235	621	Data server	Char(6)	La data in cui l'evento è stato registrato sul server di rete.
173	241	627	Ora server	Zoned(6,0)	L'ora in cui l'evento è stato registrato sul server di rete.
179	247	633	Nome computer	Char(8)	Il nome del computer che richiede la sessione.
187	255	641	Profilo	Char(10)	Il nome dell'utente che richiede la sessione.
197	265	651	Privilegio utente	Char(1)	Il livello di privilegio dell'utente per l'avvio di sessione: **A** Amministratore **G** Ospite **U** Profilo
198	266	652	Codice di errore	Char(1)	Il codice di errore per la fine della sessione. **A** Scollegamento amministratore **D** Scollegamento automatico (supero tempo), condivisione eliminata o mancanza delle autorizzazione di gestione **E** Errore, scollegamento sessione o parola d'ordine non corretta **N** Normale scollegamento o limite nome utente **R** Limitazione account

Voci di giornale VU (Modifica profilo di rete)

Questa tabella fornisce il formato delle voci di giornale VU (Modifica profilo di rete).

Tabella 226. Voci di giornale VU (Modifica profilo di rete). File descrizione campo QASYVUJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo	Char(1)	Il tipo di record che è stato modificato. **G** Record gruppo **U** Record profilo utente **M** Informazioni globali profilo utente
157	225	611	Nome server	Char(10)	Il nome della descrizione server di rete che ha registrato l'evento.
167	235	621	Data server	Char(6)	La data in cui l'evento è stato registrato sul server di rete.
173	241	627	Ora server	Zoned(6,0)	L'ora in cui l'evento è stato registrato sul server di rete.
179	247	633	Nome computer	Char(8)	Il nome del computer che richiede la modifica del profilo utente.
187	255	641	Profilo	Char(10)	Il nome dell'utente che richiede la modifica del profilo utente.
197	265	651	Operazione	Char(1)	Operazione richiesta: **A** Aggiunta **C** Modifica **D** Cancellazione **P** Parola d'ordine non corretta
198	266	652	Nome risorsa	Char(260)	Nome della risorsa.

Voci di giornale VV (Modifica stato servizio)

Questa tabella fornisce il formato delle voci di giornale VV (Modifica stato servizio).

Tabella 227. Voci di giornale VV (Modifica stato servizio). File descrizione campo QASYVVJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Il tipo di voce: **C** Stato del servizio modificato **E** Server arrestato **P** Server in pausa **R** Server riavviato **S** Server avviato
157	225	611	Nome server	Char(10)	Il nome della descrizione server di rete che ha registrato l'evento.
167	235	621	Data server	Char(6)	La data in cui l'evento è stato registrato sul server di rete.
173	241	627	Ora server	Zoned(6,0)	L'ora in cui l'evento è stato registrato sul server di rete.
179	247	633	Nome computer	Char(8)	Il nome del computer che richiede la modifica.
187	255	641	Profilo	Char(10)	Il nome dell'utente che richiede la modifica.
197	265	651	Stato	Char(1)	Stato della richiesta del servizio: **A** Servizio attivo **B** Avvio servizio in sospeso **C** Proseguimento servizio in pausa **E** Arresto sospensione per il servizio **H** Servizio in pausa **I** Servizio interrotto **S** Servizio arrestato
198	266	652	Codice servizio	Char(8)	Il codice del servizio richiesto.
206	274	660	Testo impostato	Char(80)	Il testo che viene impostato dalla richiesta del servizio.
286	354	740	Valore di ritorno	Char(4)	Il valore di ritorno dall'operazione di modifica.
290	358	744	Servizio	Char(20)	Il servizio che è stato modificato.

Voci di giornale X0 (Autenticazione di rete)

Questa tabella fornisce il formato delle voci di giornale X0 (Autenticazione di rete).

Tabella 228. Voci di giornale X0 (Autenticazione di rete). File descrizione campo QASYX0JE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.

Tabella 228. Voci di giornale X0 (Autenticazione di rete) (Continua). File descrizione campo QASYX0JE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
156	224	610	Tipo di voce	Char(1)	Il tipo di voce: **1** Certificato di servizio valido **2** Principal del servizio non corrispondenti **3** Principal del client non corrispondenti **4** Mancata corrispondenza indirizzo IP certificato **5** Decodifica del certificato non riuscita **6** Decodifica del programma di autenticazione non riuscita **7** Il dominio non è contenuto nei domini locali del client **8** Il certificato Þ un tentativo di ripetizione **9** Certificato non ancora valido **A** Decodifica dell'errore di checksum KRB_AP_PRIV o KRB_AP_SAFE **B** Mancata corrispondenza indirizzo IP remoto **C** Mancata corrispondenza indirizzo IP locale **D** Errore registrazione data/ora KRB_AP_PRIV o KRB_AP_SAFE **E** Errore ripetizione KRB_AP_PRIV o KRB_AP_SAFE **F** Errore ordine di sequenza KRB_AP_PRIV o KRB_AP_SAFE **K** Accettazione GSS — credenziale scaduta **L** Accettazione GSS — errore di checksum **M** Accettazione GSS — collegamenti canale **N** Unwrap GSS o contesto verifica GSS scaduta **O** Unwrap GSS o decrittografia/decodifica verifica GSS **P** Unwrap GSS o errore checksum verifica GSS **Q** Unwrap GSS o errore di sequenza verifica GSS
	225	611	Codice di stato	Char(8)	Lo stato della richiesta
	233	619	Valore stato GSS	Char(8)	Valore stato GSS
	241	627	Indirizzo IP remoto	Char(21)	Indirizzo IP remoto

Tabella 228. Voci di giornale X0 (Autenticazione di rete) (Continua). File descrizione campo QASYX0JE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	262	648	Indirizzo IP locale	Char(21)	Indirizzo IP locale
	283	669	Indirizzi codificati	Char(256)	Indirizzi IP codificati
	539	925	Indicatore indirizzi codificati	Char(1)	Indicatore indirizzi IP codificati **Y** tutti gli indirizzi inclusi **N** non tutti gli indirizzi inclusi **X** non fornito
	540	926	Indicatori certificato	Char(8)	Indicatori certificato
	548	934	Ora autenticazione certificato	Char(8)	Ora autenticazione certificato
	556	942	Ora di avvio del certificato	Char(8)	Ora di avvio del certificato
	564	950	Ora di fine del certificato	Char(8)	Ora di fine del certificato
	572	958	Ora rinnovo certificato	Char(8)	Ora rinnovo certificato fino a
	580	966	Registrazione data/ora messaggio	Char(8)	Registrazione data/ora X0E
	588	974	Registrazione data/ora scadenza GSS	Char(8)	Registrazione data/ora scadenza credenziale GSS o registrazione data/ora scadenza contesto
	596	982	CCSID principal server	Binary(5)	CCSID principal server (da certificato)
	600	986	Lunghezza principal server	Binary (4)	Lunghezza principal server (da certificato)
	602	988	Indicatore principal server	Char(1)	Indicatore principal server (da certificato) **Y** principal server completo **N** principal server non completo **X** non fornito
	603	989	Principal server	Char(512)	Principal server (da certificato)
	1115	1501	CCSID parametro principal server	Binary(5)	CCSID parametro principal server (da certificato)
	1119	1505	Lunghezza parametro principal server	Binary (4)	Lunghezza parametro principal server (da certificato)

Tabella 228. Voci di giornale X0 (Autenticazione di rete) (Continua). File descrizione campo QASYX0JE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	1121	1507	Indicatore parametro principal server	Char(1)	Indicatore parametro principal server (da certificato) **Y** principal server completo **N** principal server non completo **X** non fornito
	1122	1508	Parametro principal server	Char(512)	Parametro del principal server a cui il certificato deve corrispondere
	1634	2020	CCSID principal client	Binary(5)	CCSID principal client (da programma di autenticazione)
	1638	2024	Lunghezza principal client	Binary (4)	Lunghezza principal client (da programma di autenticazione)
	1640	2026	Indicatore principal client	Char(1)	Indicatore principal client (da programma di autenticazione) **Y** principal client completo **N** principal client non completo **X** non fornito
	1641	2027	Principal client	Char(512)	Principal client da programma di autenticazione
	2153	2539	CCSID principal client	Binary(5)	CCSID principal client (da certificato)
	2157	2543	Lunghezza principal client	Binary (4)	Lunghezza principal client (da certificato)
	2159	2545	Indicatore principal client	Char(1)	Indicatore principal client (da certificato) **Y** principal client completo **N** principal client non completo **X** non fornito
	2160	2546	Principal client	Char(512)	Principal client da certificato
	2672	3058	CCSID principal server GSS	Binary(5)	CCSID principal server (da credenziale GSS)
	2676	3062	Lunghezza principal server GSS	Binary (4)	Lunghezza principal server (da credenziale GSS)
	2678	3064	Indicatore principal server GSS	Char(1)	Indicatore principal server (da credenziale GSS) **Y** principal server completo **N** principal server non completo **X** non fornito
	2679	3065	Principal server GSS	Char(512)	Principal server da credenziale GSS
	3191	3577	CCSID principal locale GSS	Binary(5)	CCSID nome principal locale GSS

Tabella 228. Voci di giornale X0 (Autenticazione di rete) (Continua). File descrizione campo QASYX0JE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
	3195	3581	Lunghezza principal locale GSS	Binary (4)	Lunghezza nome principal locale GSS
	3197	3583	Indicatore principal locale GSS	Char(1)	Indicatore nome principal locale GSS **Y** principal locale completo **N** principal locale non completo **X** non fornito
	3198	3584	Principal locale GSS	Char(512)	Principal locale GSS
	3710	4096	CCSID principal remoto GSS	Binary(5)	CCSID nome principal remoto GSS
	3714	4100	Lunghezza principal remoto GSS	Binary (4)	Lunghezza nome principal remoto GSS
	3716	4102	Indicatore principal remoto GSS	Char(1)	Indicatore nome principal remoto GSS **Y** principal remoto completo **N** principal remoto non completo **X** non fornito
	3717	4103	Principal remoto GSS	Char(512)	Principal remoto GSS

Voci di giornale X1 (Token identità)

Questa tabella fornisce il formato delle voci di giornale X1 (Token identità).

Tabella 229. Voci di giornale X1 (Token identità). File descrizione campo QASYX1JE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
		1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.

Tabella 229. Voci di giornale X1 (Token identità) (Continua). File descrizione campo QASYX1JE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
		610	Tipo di voce	Char(1)	Il tipo di voce: **D** La delega del token identità ha avuto esito positivo **F** La delega del token identità ha avuto esito negativo **G** Il richiamo dell'utente dal token identità ha avuto esito positivo **U** Il richiamo dell'utente dal token identità ha avuto esito negativo
		611	Codice di errore	Binary(5)	Codice di errore per la richiesta non riuscita: **9** Mancata corrispondenza lunghezza token **10** Mancata corrispondenza identificativo EIM **11** Mancata corrispondenza ID istanza applicazione **12** Firma token non valida **13** Token identità non valido **14** Utente di destinazione non trovato **16** Gestione chiave non valida **17** Versione token non supportata **18** Chiave pubblica non trovata **Nota:** in caso di errore, solo le informazioni che sono state convalidate fino al punto in cui è intervenuto l'errore verranno inserite nei campi testo.
		615	Riservato	Char (7)	Riservato
		622	CCSID dati	Binary(5)	Il CCSID dei dati nei campi testo
		626	Lunghezza ricevente	Binary(5)	La lunghezza dei dati nel campo del ricevente.
		630	Ricevitore	Char(508)	Il ricevente del token identità la cui richiesta ha avuto esito negativo o positivo. I dati in questo campo saranno nel formato: <EIMID>receiver_eimID </EIMID> <APPID>RECEIVER_appID </APPID> <TIMESTAMP>receiver_timestamp </TIMESTAMP>. La registrazione data/ora verrà inclusa solo nelle richieste con delega.
		1138	Lunghezza mittente	Binary(5)	La lunghezza dei dati nel campo del mittente.
		1142		Char(508)	L'ultimo mittente del token identità la cui richiesta ha avuto esito negativo o positivo. I dati in questo campo saranno nel formato I dati in questo campo saranno nel formato: <EIMID>sender_eimID</EIMID> <APPID>sender_appID</APPID> <TIMESTAMP>sender_timestamp</TIMESTAMP>
		1650	Lunghezza origine	Binary(5)	La lunghezza dei dati nel campo origine.

Tabella 229. Voci di giornale X1 (Token identità) (Continua). File descrizione campo QASYX1JE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
		1654	Origine	Char(508)	L'origine della richiesta token identità. Se mittente e origine sono uguali, il campo lunghezza origine corrisponderà a 0. I dati in questo campo saranno nel formato: <EIMID>initiator_eimID</EIMID> <APPID>initiator_appID</APPID> <TIMESTAMP>initiator_timestamp</TIMESTAMP>
		2162	Lunghezza concatenam.	Binary(5)	La lunghezza dei dati nel campo concatenamento.
		2166	Concatenam.	Char(2036)	Il concatenamento di mittenti tra l'origine e l'ultimo mittente. Il concatenamento andrà dal più recente al meno recente. Se non vi sono altri mittenti, allora il campo lunghezza concatenamento corrisponderà a 0. Questo campo potrebbe venire troncato se la catena supera la lunghezza del campo stesso. I dati in questo campo saranno nel formato: <SNDRz><EIMID>sndrz_eimID</EIMID> <APPID>sndrz_appID</APPID> <TIMESTAMP>sndrz_timestamp </TIMESTAMP> </SNDRz> <SNDRy>...</SNDRy>...
		4202	Voci concatenam.	Binary(5)	Il numero di voci nel campo relativo al concatenamento.
		4206	Voci concatenam. disponibili	Binary(5)	Numero di voci disponibili per il concatenamento di mittenti. Questo numero può essere maggiore del numero di voci presenti nel campo se il campo del concatenamento è stato troncato.
		4210	Lunghezza registro origine	Binary(5)	La lunghezza dei dati nel campo registro origine.
		4214	Registro origine	Char(508)	Il registro origine specificato nel token identità.
		4722	Lunghezza utente registro origine	Binary(5)	La lunghezza dei dati nel campo utente registro origine.
		4726	Utente registro origine	Char(508)	L'utente registro origine specificato nel token identità.
		5234	Lunghezza registro destinazione	Binary(5)	La lunghezza dei dati nel campo registro destinazione.
		5238	Registro destinazione	Char(508)	Il registro destinazione specificato.
		5746	Lunghezza utente registro destinazione	Binary(5)	La lunghezza dei dati nel campo utente registro destinazione.
		5750	Utente registro destinazione	Char(508)	L'utente registro destinazione con il quale il token identità è in corrispondenza.

Voci di giornale XD (Estensione server indirizzario)

Questa tabella fornisce il formato delle voci di giornale XD (Estensione server indirizzario).

Tabella 230. Voci di giornale XD (Estensione server indirizzario). File descrizione campo QASYXDJ5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
		1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
		610	Tipo di voce	Char(1)	Il tipo di voce: **G** Nomi gruppo. I campi da 1 a 5 contengono nomi gruppo.
		611	Riferimenti incrociati	Char(36)	Stringa riferimenti incrociati utilizzata per mettere in correlazione questa voce con la voce DI utilizzando questi gruppi. Più si una voce DI può far riferimento a questa voce XD se più richieste LDAP utilizzano la stessa serie di gruppi.
		647	Riservato	Char(100)	
		747	CCSID campo 1	Bin(5)	Il valore CCSID per il campo 1.
		751	Lunghezza campo 1	Bin(4)	La lunghezza dei dati nel campo 1.
		753	Campo 1	Char(2002)	Dati campo 1 Per il tipo di voce G, questo campo conterrà un nome gruppo da un'asserzione di appartenenza al gruppo.
		2755	CCSID campo 2	Bin(5)	Il valore CCSID per il campo 2.
		2759	Lunghezza campo 2	Bin(4)	La lunghezza dei dati nel campo 2.
		2761	Campo 2	Char(2002)	Dati campo 2 Per il tipo di voce G, questo campo conterrà un nome gruppo da un'asserzione di appartenenza al gruppo.
		4763	CCSID campo 3	Bin(5)	Il valore CCSID per il campo 3.
		4767	Lunghezza campo 3	Bin(4)	La lunghezza dei dati nel campo 3.
		4769	Campo 3	Char(2002)	dati campo 3 Per il tipo di voce G, questo campo conterrà un nome gruppo da un'asserzione di appartenenza al gruppo.
		6771	CCSID campo 4	Bin(5)	Il valore CCSID per il campo 4.
		6775	Lunghezza campo 4	Bin(4)	La lunghezza dei dati nel campo 4.

Tabella 230. Voci di giornale XD (Estensione server indirizzario) (Continua). File descrizione campo QASYXDJ5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
		6777	Campo 4	Char(2002)	Dati campo 4 Per il tipo di voce G, questo campo conterrà un nome gruppo da un'asserzione di appartenenza al gruppo.
		8779	CCSID campo 5	Bin(5)	Il valore CCSID per il campo 5.
		8783	Lunghezza campo 5	Bin(4)	La lunghezza dei dati nel campo 5.
		8785	Campo 5	Char(2002)	Dati campo 5 Per il tipo di voce G, questo campo conterrà un nome gruppo da un'asserzione di appartenenza al gruppo.

Voci di giornale YC (Modifica in oggetto DLO)

Questa tabella fornisce il formato delle voci di giornale YC (Modifica in oggetto DLO).

Tabella 231. Voci di giornale YC (Modifica in oggetto DLO). File descrizione campo QASYYCJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Accesso oggetto **C** Modifica in un oggetto DLO
157	225	611	Nome oggetto	Char(10)	Nome dell'oggetto
167	235	621	Nome libreria	Char(10)	Nome della libreria
177	245	631	Tipo oggetto	Char(8)	Tipo di oggetto
185	253	639	Utente Office	Char(10)	Profilo utente dell'utente office
195	263	649	Nome cartella o documento	Char(12)	Nome del documento o della cartella
207	275	661	(Area riservata)	Char(8)	
215	283	669	Percorso cartella	Char(63)	La cartella contenente il DLO (document library object)
278	346	732	Per conto dell'utente	Char(10)	Utente che opera per conto di un altro utente
288	356	742	Tipo accesso	Packed(5,0)	Tipo di accesso [1]

[1] Consultare la "Codici numerici per tipi di accesso" a pagina 748 per un elenco di codici relativi ai tipi di accesso.

Voci di giornale YR (Lettura di oggetto DLO)

Questa tabella fornisce il formato delle voci di giornale YR (Lettura di oggetto DLO).

Tabella 232. Voci di giornale YR (Lettura di oggetto DLO). File descrizione campo QASYYRJE/J4/J5

Scostamenti			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Accesso oggetto **R** Lettura di un oggetto DLO
157	225	611	Nome oggetto	Char(10)	Nome dell'oggetto
167	235	621	Nome libreria	Char(10)	Nome della libreria
177	245	631	Tipo oggetto	Char(8)	Tipo di oggetto
185	253	639	Utente Office	Char(10)	Profilo utente dell'utente office
195	263	649	Nome cartella o documento	Char(12)	Nome del DLO (document library object)
207	275	661	(Area riservata)	Char(8)	
215	283	669	Percorso cartella	Char(63)	La cartella contenente il DLO (document library object)
278	346	732	Per conto dell'utente	Char(10)	Utente che opera per conto di un altro utente
288	356	742	Tipo accesso	Packed(5,0)	Tipo di accesso [1]

[1] Consultare la "Codici numerici per tipi di accesso" a pagina 748 per un elenco di codici relativi ai tipi di accesso.

Voci di giornale ZC (Modifica in oggetto)

Questa tabella fornisce il formato delle voci di giornale ZC (Modifica in oggetto).

Tabella 233. Voci di giornale ZC (Modifica in oggetto). File descrizione campo QASYZCJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.

Tabella 233. Voci di giornale ZC (Modifica in oggetto) (Continua). File descrizione campo QASYZCJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
156	224	610	Tipo di voce	Char(1)	Accesso oggetto **C** Modifica di un oggetto **U** Aggiornamento dell'accesso aperto ad un oggetto
157	225	611	Nome oggetto	Char(10)	Nome dell'oggetto
167	235	621	Nome libreria	Char(10)	Nome della libreria in cui è ubicato l'oggetto
177	245	631	Tipo oggetto	Char(8)	Tipo di oggetto
185	253	639	Tipo accesso	Packed(5,0)	Tipo di accesso [1]

Tabella 233. Voci di giornale ZC (Modifica in oggetto) (Continua). File descrizione campo QASYZCJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
188	256	642	Dati specifici per l'accesso	Char(50)	Dati specifici sull'accesso Quando il tipo oggetto è *IMGCLG, questo campo contiene il seguente formato: **Char 3** Numero indice della voce catalogo immagini. **Spazio vuoto** Indica che l'operazione è fatta su un catalogo immagini. **Char 32** ID volume della voce catalogo immagini. **Spazio vuoto** Indica che l'operazione è fatta su un catalogo immagini. **Char 1** Tipo di accesso per la voce. I possibili valori sono riportati sotto. **Spazio vuoto** Indica che l'operazione è fatta su un catalogo immagini. **R** Il file con la voce catalogo immagini è di sola lettura. **W** Il file con la voce catalogo immagini ha capacità di lettura/scrittura. **Char 1** La protezione di scrittura per la voce. **Spazio vuoto** Indica che l'operazione è fatta su un catalogo immagini. **Y** Il file con la voce catalogo immagini è protetto da scrittura. **N** Il file con la voce catalogo immagini non è protetto da scrittura. **Char 10** Il nome dell'unità virtuale. **Spazio vuoto** Indica che l'operazione è fatta su un catalogo immagini o il catalogo non si trova nello stato Pronto. **Char 3** Non usato. Se il tipo oggetto è IFS (integrated file system), il campo contiene altre informazioni che identificano la richiesta di modifica. Vedere il file di inclusione QSYSINC, QP0LJRNL.H per i valori.

Tabella 233. Voci di giornale ZC (Modifica in oggetto) (Continua). File descrizione campo QASYZCJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
238			(Area riservata)	Char(20)	
	306	692	(Area riservata)	Char(18)	
	324	710	Lunghezza nome oggetto [2]	Binary (4)	La lunghezza del nome oggetto.
258	326	712	CCSID nome oggetto[2]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
262	330	716	ID paese o regione nome oggetto[2]	Char(2)	L'ID paese o regione per il nome oggetto.
264	332	718	ID lingua nome oggetto[2]	Char(3)	L'ID lingua per il nome oggetto.
267	335	721	(Area riservata)	Char(3)	
270	338	724	ID file principale[2, 3]	Char(16)	L'ID file dell'indirizzario principale.
286	354	740	ID file oggetto[2, 3]	Char(16)	L'ID file dell'oggetto.
302	370	756	Nome oggetto[2]	Char(512)	Il nome dell'oggetto.
	882	1268	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	898	1284	Nome ASP[6]	Char(10)	Il nome dell'unità ASP
	908	1294	Numero ASP[6]	Char(5)	Il numero dell'unità ASP.
	913	1299	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	917	1303	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	919	1305	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	922	1308	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.
	924	1310	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	925	1311	ID file indirizzario relativo[4]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[4]
	941	1327	Nome percorso[5]	Char(5002)	Il nome percorso dell'oggetto.

Tabella 233. Voci di giornale ZC (Modifica in oggetto) (Continua). File descrizione campo QASYZCJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
[1] Consultare la "Codici numerici per tipi di accesso" a pagina 748 per un elenco di codici relativi ai tipi di accesso.					
[2] Questi campi vengono utilizzati solo per oggetti nei file system "root" (/), QOpenSys e negli UDFS (user-defined file systems).					
[3] Un ID con il bit all'estrema sinistra impostato ed il resto dei bit zero indica che l'ID NON è impostato.					
[4] Se il campo Indicatore nome percorso è N, ma l'ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.					
[5] Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza del nome percorso.					
[6] Se l'oggetto è in una libreria, queste sono le informazioni ASP della libreria dell'oggetto. Se l'oggetto non è in una libreria, queste sono le informazioni ASP dell'oggetto.					

Voci di giornale ZR (Lettura di oggetto)

Questa tabella fornisce il formato delle voci di giornale ZR (Lettura di oggetto).

Tabella 234. Voci di giornale ZR (Lettura di oggetto). File descrizione campo QASYZRJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	**J4**	**J5**			
1	1	1			Campi intestazione comuni a tutti i tipi di voce Consultare la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE5 (*TYPE5)" a pagina 596, la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE4 (*TYPE4)" a pagina 598 e la "Campi intestazione standard per voci giornale di controllo. Formato record QJORDJE2 (*TYPE2)" a pagina 599 per un elenco dei campi.
156	224	610	Tipo di voce	Char(1)	Accesso oggetto **R** Lettura di un oggetto
157	225	611	Nome oggetto	Char(10)	Nome dell'oggetto
167	235	621	Nome libreria	Char(10)	Nome della libreria in cui è ubicato l'oggetto
177	245	631	Tipo oggetto	Char(8)	Tipo di oggetto
185	253	639	Tipo accesso	Packed(5,0)	Tipo di accesso [1]

Tabella 234. Voci di giornale ZR (Lettura di oggetto) (Continua). File descrizione campo QASYZRJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
188	256	642	Dati specifici per l'accesso	Char(50)	Dati specifici sull'accesso. Quando il tipo di oggetto è *IMGCLG, questo campo contiene il seguente formato: **Char 3** Numero indice della voce catalogo immagini. **Spazio vuoto** Indica che l'operazione è stata effettuata rispetto ad un catalogo immagini. **Char 32** ID volume della voce catalogo immagini. **Spazio vuoto** Indica che l'operazione è stata effettuata rispetto ad un catalogo immagini. **Char 1** Tipo di accesso per la voce. I possibili valori sono riportati sotto. **Spazio vuoto** Indica che l'operazione è stata effettuata rispetto ad un catalogo immagini. **R** Il file che contiene la voce del catalogo immagini è di sola lettura. **W** Il file che contiene la voce del catalogo immagini ha capacità di lettura/scrittura. **Char 1** La protezione di scrittura per la voce. **Spazio vuoto** Indica che l'operazione è stata effettuata rispetto ad un catalogo immagini. **Y** Il file che contiene la voce del catalogo immagini è protetto per la scrittura. **N** Il file che contiene la voce del catalogo immagini non è protetto per la scrittura. **Char 10** Il nome dell'unità virtuale. **Spazio vuoto** Indica che l'operazione è stata effettuata rispetto ad un catalogo immagini o che il catalogo immagini non si trova nello stato di Pronto. **Char 3** Non utilizzato.

Tabella 234. Voci di giornale ZR (Lettura di oggetto) (Continua). File descrizione campo QASYZRJE/J4/J5

Scost.					
JE	**J4**	**J5**	**Campo**	**Formato**	**Descrizione**
238			(Area riservata)	Char(20)	
	306	692	(Area riservata)	Char(18)	
	324	710	Lunghezza nome oggetto [2]	Binary (4)	La lunghezza del nome oggetto.
258	326	712	CCSID nome oggetto[2]	Binary(5)	Il CCSID (coded character set identifier) per il nome oggetto.
262	330	716	ID paese o regione nome oggetto[2]	Char(2)	L'ID paese o regione per il nome oggetto.
264	332	718	ID lingua nome oggetto[2]	Char(3)	L'ID lingua per il nome oggetto.
267	335	721	(Area riservata)	Char(3)	
270	338	724	ID file principale[2,3]	Char(16)	L'ID file dell'indirizzario principale.
286	354	740	ID file oggetto[2,3]	Char(16)	L'ID file dell'oggetto.
302	370	756	Nome oggetto[2]	Char(512)	Il nome dell'oggetto.
	882	1268	ID file oggetto	Char(16)	L'ID file dell'oggetto.
	898	1284	Nome ASP	Char(10)	Il nome dell'unità ASP
	908	1294	Numero ASP	Char(5)	Il numero dell'unità ASP.
	913	1299	CCSID nome percorso	Binary(5)	Il CCSID (coded character set identifier) per il nome percorso.
	917	1303	ID paese o regione nome percorso	Char(2)	L'ID paese o regione per il nome percorso.
	919	1305	ID lingua nome percorso	Char(3)	L'ID lingua per il nome percorso.
	922	1308	Lunghezza nome percorso	Binary (4)	La lunghezza del nome percorso.
	924	1310	Indicatore nome percorso	Char(1)	Indicatore nome percorso: **Y** Il campo Nome percorso contiene il nome percorso assoluto completo per l'oggetto. **N** Il campo Nome percorso non contiene un nome percorso assoluto per l'oggetto, ma un nome percorso relativo. Il campo ID file indirizzario relativo è valido e può essere utilizzato per formare un nome percorso assoluto con questo nome percorso relativo.
	925	1311	ID file indirizzario relativo[4]	Char(16)	Quando il campo Indicatore nome percorso è N, questo campo contiene l'ID file dell'indirizzario che contiene l'oggetto identificato nel campo Nome percorso. Altrimenti, contiene zero esa.[4]
	941	1327	Nome percorso[5]	Char(5002)	Il nome percorso dell'oggetto.

Tabella 234. Voci di giornale ZR (Lettura di oggetto) (Continua). File descrizione campo QASYZRJE/J4/J5

Scost.			Campo	Formato	Descrizione
JE	J4	J5			
[1]	Consultare la “Codici numerici per tipi di accesso” per un elenco di codici relativi ai tipi di accesso.				
[2]	Questi campi vengono utilizzati solo per oggetti nei file system ″root″ (/), QOpenSys e negli UDFS (user-defined file systems).				
[3]	Un ID con il bit all’estrema sinistra impostato ed il resto dei bit zero indica che l’ID NON è impostato.				
[4]	Se il campo Indicatore nome percorso è N, ma l’ID file indirizzario relativo è zero esa, si è verificato un errore nello stabilire le informazioni sul nome percorso.				
[5]	Questo è un campo a lunghezza variabile. I primi 2 byte contengono la lunghezza del nome percorso.				

Codici numerici per tipi di accesso

Questa tabella elenca i codici di acceso utilizzati per le voci di giornale di controllo oggetti nei file QASYYCJE/J4/J5, QASYYRJE/J4/J5, QASYZCJE/J4/J5 e QASYZRJE/J4/J5.

Tabella 235. Codici numerici per tipi di accesso

Codice	Tipo accesso	Codice	Tipo accesso	Codice	Tipo accesso
1	Aggiunta	26	Caricamento	51	Invio
2	Attivazione programma	27	Elenco	52	Avvio
3	Analisi	28	Spostamento	53	Trasferimento
4	Applicazione	29	Unione	54	Traccia
5	Chiamata o TFRCTL	30	Apertura	55	Verifica
6	Configurazione	31	Stampa	56	Variazione
7	Modifica	32	Query	57	Lavoro
8	Controllo	33	Riacquisizione	58	Lettura/Modifica attributo DLO
9	Chiusura	34	Ricezione	59	Lettura/Modifica sicurezza DLO
10	Eliminazione contenuto	35	Lettura	60	Lettura/Modifica contenuto DLO
11	Confronto	36	Riorganizzazione	61	Lettura/Modifica di tutte le parti DLO
12	Annullamento	37	Rilascio	62	Aggiunta vincolo
13	Copia	38	Eliminazione	63	Modifica vincolo
14	Creazione	39	Ridenominazione	64	Eliminazione vincolo
15	Conversione	40	Sostituzione	65	Avvio procedura
16	Debug	41	Ripresa	66	Accesso a **OOPOOL
17	Cancellazione	42	Ripristino	67	Firma oggetto
18	Dump	43	Richiamo	68	Eliminazione di tutte le firme

Tabella 235. Codici numerici per tipi di accesso (Continua)

Codice	Tipo accesso	Codice	Tipo accesso	Codice	Tipo accesso
19	Visualizzazione	44	Esecuzione	69	Eliminazione del contenuto di un oggetto firmato
20	Editazione	45	Revoca	70	MOUNT
21	Fine	46	Salvataggio	71	Scaricamento
22	File	47	Salvataggio con memoria libera	72	Fine rollback
23	Concessione	48	Salvataggio e cancellazione		
24	Congelamento	49	Inoltro		
25	Inizializzazione	50	Impostazione		

Appendice G. Comandi e menu per i comandi di sicurezza

Il menu SECTOOLS (Strumenti di sicurezza), il menu SECBATCH (Inoltro o Pianificazione documentazioni di sicurezza in batch), i comandi CFGSYSSEC (Configurazione sicurezza sistema) e RVKPUBAUT (Revoca autorizzazione pubblica) sono quattro strumenti di sicurezza che è possibile utilizzare per configurare la sicurezza del sistema

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 sul menu Strumenti di sicurezza

È possibile utilizzare il menu SECTOOLS (Strumenti di sicurezza) per semplificare la gestione e il controllo della sicurezza sul sistema con numerose opzioni e comandi da esso forniti.

Questa figura mostra la parte del menu SECTOOLS correlata ai profili utente.

Per accedere a questo menu, immettere `GO SECTOOLS`.

```
SECTOOLS                       Strumenti sicurezza

Selezionare una delle seguenti opzioni:

  Gestione profili
     1. Analisi parole d'ordine predefinite

     2. Visualizzazione elenco profili attivi
     3. Modifica elenco profili attivi
     4. Analisi attività profilo

     5. Visualizzazione pianificazione attivazione
     6. Modifica voce Scd di attivazione

     7. Visualizzazione pianificazione di scadenza
     8. Modifica scadenza voce di pianificazione
     9. Stampa valori interni profilo
```

La Tabella 236 descrive tali opzioni di menu e i comandi associati:

Tabella 236. Comandi strumenti per profili utente

Opzione[1] menu	**Nome comando**	**Descrizione**	**File 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]

Tabella 236. Comandi strumenti per profili utente (Continua)

Opzione[1] menu	Nome comando	Descrizione	File database utilizzato
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. È 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 l'accesso 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	DSPEXPSCDE	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 236. Comandi strumenti per profili utente (Continua)

Opzione[1] menu	Nome comando	Descrizione	File database utilizzato
8	CHGEXPSCDE	Utilizzare il comando Modifica voce Scd di scadenza per pianificare la rimozione di un profilo utente. È 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 relative ai valori interni sul numero di voci contenute in un oggetto profilo utente (*USRPRF).	

Note:

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

È possibile utilizzare il tasto pagina giù sul menu per visualizzare opzioni aggiuntive. La Tabella 237 descrive le opzioni di menu e i comandi associati per il controllo sicurezza:

Tabella 237. Comandi strumenti per controllo sicurezza

Opzione[1] menu	Nome comando	Descrizione	File database utilizzato
10	CHGSECAUD	Utilizzare il comando Modifica controllo sicurezza 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 QAUDLVL2 (estensione livello di controllo). È 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 237. Comandi strumenti per controllo sicurezza (Continua)

Opzione[1] menu	Nome comando	Descrizione	File database utilizzato
11	DSPSECAUD	Utilizzare il comando Visualizzazione controllo sicurezza per visualizzare informazioni relative al giornale di controllo sicurezza e i valori di sistema che controllano tale controllo.	
12	CPYAUDJRNE	Utilizzare il comando di copia delle voci dal giornale di controllo per copiare le voci dal suddetto giornale a un file di emissione.	QASYxxJ5[2]

[1] Le opzioni derivano dal menu SECTOOLS.

[2] xx è il tipo di voce di giornale di due caratteri. Ad esempio, il file di emissione modello per le voci del giornali AE è QSYS/QASYAEJ5. I file di emissione del modello vengono descritti in Appendice F, "Layout di voci di giornale di controllo", a pagina 595 di questa raccolta di argomenti.

Come utilizzare il menu batch di sicurezza

È possibile utilizzare il menu batch di sicurezza per inoltrare uno o più prospetti degli Strumenti di sicurezza a una coda lavori da eseguire in seguito come lavoro in batch. È inoltre possibile scegliere di pianificare uno qualsiasi dei prospetti degli Strumenti di sicurezza come lavoro in batch da inoltrare in una sola soluzione o a intervalli regolari. Gli esempi riportati in questo argomento dimostrano come utilizzare il menu batch di sicurezza.

Di seguito è riportata la prima parte del menu SECBATCH:

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

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

Quando si seleziona un'opzione da tale menu, viene visualizzato il pannello Inoltro lavoro (SBMJOB), come riportato nel seguente esempio:

```
                              Inoltro lavoro (SBMJOB)
Immettere le scelte e premere Invio.

Comando da eseguire . . . . . > PRTADPOBJ USRPRF(*ALL)
_____________________________________________
_____________________________________________
_____________________________________________...
Nome lavoro. . . . . .   *JOBD          Nome, *JOBD
Descrizione lavoro. . . . . .   *USRPRF       Nome, *USRPRF
  Libreria. . . . . .                  Nome, *LIBL, *CURLIB
Coda lavori. . . . . .   *JOBD         Nome, *JOBD
  Libreria. . . . . .    __            Nome, *LIBL, *CURLIB
Priorità lavoro (su JOBQ) . . . . .   *JOBD          1-9, *JOBD
Priorità emissione (su OUTQ) . .   *JOBD         1-9, *JOBD
Unità di stampa. . . . . .   *CURRENT      Nome, *CURRENT, *USRPRF...
```

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.

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

    28. Oggetti utente
    29. Informazioni profilo utente
    30. Valori interni profilo utente
    31. Controllo integrità oggetto

  Pianificazione prospetti batch
    40. Adozione oggetti
    41. Controllo voci giornale
    42. Autorizzazioni elenchi di autorizzazioni
    43. Autorizzazione comandi
    44. Autorizzazione privata comandi
    45. Sicurezza delle comunicazioni
    46. Autorizzazione indirizzario
```

È 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):

```
                       Aggiunta specifica
schedulazione lavori (ADDJOBSCDE)

Immettere le scelte e premere Invio.

Nome lavoro. . . . . .  _____                  Nome, *JOBD
Comando da eseguire . . . . . > PRTADPOBJ USRPRF(*ALL)
_____________________________________________
_____________________________________________
_____________________________________________
_____________________________________________...
Frequenza  . . . . . .  _____  *ONCE, *WEEKLY, *MONTHLY
Data di pianificazione o  . . . . . .  *CURRENT      Data, *CURRENT, *MONTHST
Pianificazione giorno. . . . . .  *NONE         *NONE, *ALL, *MON, *TUE.
+ per altri valori
Ora pianificazione. . . . . .  *CURRENT      Ora, *CURRENT
```

È 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 sul menu batch di sicurezza

Questa tabella descrive le opzioni di menu e i comandi associati per i prospetti 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 238. Comandi per prospetti di sicurezza

Opzione[1] menu	**Nome comando**	**Descrizione**	**File 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. È 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[6]	Utilizzare il comando Visualizzazione voci giornale di controllo per visualizzare o stampare informazioni relative alle voci nel giornale di controllo sicurezza. È possibile selezionare tipi di voci specifici, utenti specifici e un periodo di tempo.	QASYxxJ5[3]

Tabella 238. Comandi per prospetti di sicurezza (Continua)

Opzione[1] menu	Nome comando	Descrizione	File 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 sicurezza 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, programmi di controllo e descrizioni unità. Ciascuna di tali documentazioni ha una versione completa e una versione modificata.	QSECCMNOLD[2]

Tabella 238. Comandi per prospetti di sicurezza (Continua)

Opzione[1] menu	Nome comando	Descrizione	File 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 la nota 4.	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 238. Comandi per prospetti di sicurezza (Continua)

Opzione[1] menu	Nome comando	Descrizione	File 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 lavori 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 sicurezza 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 238. Comandi per prospetti di sicurezza (Continua)

Opzione[1] menu	Nome comando	Descrizione	File 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. È 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. È possibile selezionare i profili utente sulla base di autorizzazioni speciali, classe utente o mancata corrispondenza tra autorizzazioni speciali e classe utente. È possibile stampare le informazioni sull'autorizzazione, le informazioni sull'ambiente o sulla parola d'ordine.	
30, 69	PRTPRFINT	Utilizzare il comando Stampa valori interni profilo per stampare una documentazione contenente informazioni relative ai valori interni sul numero di voci contenute in un oggetto profilo utente (*USRPRF).	
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.	

Tabella 238. Comandi per prospetti di sicurezza (Continua)

Opzione[1] menu	Nome comando	Descrizione	File database utilizzato
[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 del giornali AE è QSYS/QASYAEJ5. I file di emissione del modello vengono descritti in Appendice F, "Layout di voci di giornale di controllo", a pagina 595 di questa raccolta di argomenti.			
[4] Il menu SECTOOLS contiene le opzioni per i tipi di oggetti che sono normalmente di interesse degli amministratori 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. Utilizzare le opzioni 12 e 51 per eseguire il comando PRTPVTAUT sugli oggetti *FILE. Utilizzare le opzioni generali (19 e 58) per specificare il tipo di oggetto.			
[5] 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.			
[6] Il comando DSPAUDJRNE non può elaborare tutti i tipi di record di controllo sicurezza e non fornisce un elenco di tutti i campi per i record da esso supportati.			

Comandi per la personalizzazione della sicurezza

Questa tabella descrive i comandi, presenti sul menu SECTOOLS, che è possibile utilizzare per personalizzare la sicurezza sul sistema.

Tabella 239. Comandi per la personalizzazione del sistema

Opzione[1] menu	Nome comando	Descrizione	File database utilizzato
60	CFGSYSSEC	Utilizzare il comando Configurazione sicurezza 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 sicurezza sistema" descrive le attività del comando.	
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 764 elenca le azioni eseguite dal comando RVKPUBAUT.	
[1] Le opzioni derivano dal menu SECTOOLS.			

Valori impostati dal comando Configurazione sicurezza sistema

Questa tabella elenca i valori di sistema impostati quando si esegue il comando CFGSYSSEC (Configurazione sicurezza sistema) che esegue un programma denominato QSYS/QSECCFGS.

Tabella 240. Valori impostati dal comando CFGSYSSEC

Nome valore di sistema	Impostazione	Descrizione valore di sistema
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.
QALWOBJRST	*NONE	Se è possibile il ripristino di programmi di stato del sistema e di programmi che adottano l'autorizzazione
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
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.
QPWDEXPITV	60	Con quale frequenza gli utenti devono modificare le parole d'ordine
QPWDMINLEN	6 (vedere nota 3 e 5)	Lunghezza minima per le parole d'ordine
QPWDMAXLEN	8 (vedere nota 4 e 5)	Lunghezza massima per le parole d'ordine
QPWDPOSDIF	1 (Sì) (vedere nota 5)	Se ogni posizione in una nuova parola d'ordine deve essere differente dalla stessa posizione nell'ultima parola d'ordine
QPWDLMTCHR	Vedere nota 2 e 5	Caratteri non consentiti nelle parole d'ordine
QPWDLMTAJC	1 (Sì) (vedere nota 5)	Se numeri adiacenti sono proibiti nelle parole d'ordine
QPWDLMTREP	2 (Non possono essere ripetuti consecutivamente) (vedere nota 5)	Se caratteri che si ripetono sono proibiti nelle parole d'ordine
QPWDRQDDGT	1 (Sì) (vedere nota 5)	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

Tabella 240. Valori impostati dal comando CFGSYSSEC (Continua)

Nome valore di sistema	Impostazione	Descrizione valore di sistema
QPWDRULES	• *MINLEN6 • *MAXLEN10 • *LMTSAMPOS • *LMTPRFNAME • *DGTMIN1 • *CHRLMTAJC • *DGTLMTAJC • *DGTLMTFST • *DGTLMTLST • *SPCCHRLMTAJC • *SPCCHRLMTFST • *SPCCHRLMTLST (vedere nota 6)	Regoler per creare una parola d'ordine valida.
QPWDVLDPGM	*NONE	Il programma di uscita utente che il sistema richiama per convalidare le parole d'ordine
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	50	Il livello di sicurezza applicato
QVFYOBJRST	3	Verificare l'oggetto al ripristino

Note:

1. Se si sta attualmente eseguendo un valore QSECURITY di 30 o inferiore, accertarsi di rivedere le informazioni contenute nel Capitolo 2, "Valore del valore di sistema Sicurezza sistema (QSecurity)", a pagina 9 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@$#. È possibile utilizzare il comando Modifica descrizione messaggio (CHGMSGD) per modificare i caratteri limitati.
3. Se la lunghezza minima per le parola d'ordine è maggiore di 6, il valore di sistema QPWDMINLEN non verrà modificato.
4. Se la lunghezza massima per le parole d'ordine è maggiore di 8, il valore di sistema QPWDMAXLEN non verrà modificato.
5. Questo valore di sistema viene modificato solo se il valore di sistema QPWDRULES attualmente specifica un valore di *PWDSYSVAL.
6. Questo valore di sistema non viene modificato se il valore corrente è *PWDSYSVAL.

Inoltre, il comando CFGSYSSEC 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 della sicurezza in base ai valori specificati utilizzando il comando CHGSECAUD (Modifica controllo sicurezza).

Modifica del programma

Se alcuni valori di sistema delle impostazioni non sono appropriate per la propria installazione, è possibile creare la propria versione del programma che elabora il comando CFGSYSSEC (Configurazione sicurezza sistema).

Per modificare il programma, attenersi alla seguente procedura:

1. Utilizzare il comando RTVCLSRC (Richiamo origine CL) per copiare l'origine del programma in esecuzione quando si utilizza il comando CFGSYSSEC. Il programma da richiamare è QSYS/QSECCFGS. Una volta richiamato, assegnargli un nome differente.
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.
3. Utilizzare il comando CHGCMD (Modifica comando) 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, è necessario immettere il seguente comando:

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

   Note:

   a. 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.

   b. Se si modifica il comando RVKPUBAUT per utilizzare un programma di elaborazione comandi differente, la firma digitale di tale comando non sarà più valida.

Funzioni del comando Revoca autorizzazione pubblica

È possibile utilizzare il comando RVKPUBAUT (Revoca autorizzazione pubblica) 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 241 a pagina 765 e le API (application programming interface) elencate nella Tabella 242 a pagina 765. All'arrivo del sistema, questi comandi ed API hanno l'autorizzazione pubblica impostata su *USE.

I comandi elencati nella Tabella 241 a pagina 765 e le API elencate nella Tabella 242 a pagina 765 eseguono tutti delle funzioni nel sistema tali da fornire l'opportunità di un uso illecito. Come amministratore 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 241. 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	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

Le API nella Tabella 242 si trovano tutte nella libreria QSYS:

Tabella 242. Programmi la cui autorizzazione pubblica è impostata dal comando RVKPUBAUT

QTIENDSUP		
QTISTRSUP		
QWTCTLTR		
QWTSETTR		
QY2FTML		

A partire da V3R7, quando si esegue il comando RVKPUBAUT, il sistema imposta l'autorizzazione pubblica per l'indirizzario principale su *USE (a meno che non sia già *USE o inferiore).

Modifica del programma

Se alcune impostazioni non sono appropriate per la propria installazione, è possibile creare la propria versione del programma che elabora il comando RVKPUBAUT (Revoca autorizzazione pubblica).

Per modificare il programma, attenersi alla seguente procedura:

1. Utilizzare il comando RTVCLSRC (Richiamo origine CL) per copiare l'origine del programma in esecuzione quando si utilizza il comando RVKPUBAUT. Il programma da reperire è QSYS/QSECRVKP. Una volta reperito, assegnargli un *nome differente*.
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.
3. Utilizzare il comando CHGCMD (Modifica comando) 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, è necessario immettere il seguente comando:

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

   Note:

   a. 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.
   b. Se si modifica il comando RVJPUDAUT per utilizzare un programma di elaborazione comandi differente, la firma digitale di questo comando non sarà più valida.

Appendice H. Informazioni correlate per i riferimenti alla sicurezza i5/OS

Di seguito vengono elencati i manuali del prodotto e gli IBM Redbooks (in formato PDF), i siti Web e gli argomenti dell'Information Center relativi all'argomento della sicurezza. È possibile visualizzare o stampare questi PDF.

Manuali

- Recovering your system (circa 8.42 MB), fornisce informazioni sulla pianificazione di una strategia di copia di riserva e ripristino, sul salvataggio delle informazioni dal sistema e sul ripristino del sistema, sugli ASP (auxiliary storage pools) e sulle opzioni per la protezione disco.
- Installing, upgrading, or deleting i5/OS and related software (3,053 KB), fornisce procedure dettagliate per l'installazione iniziale, l'installazione di programmi su licenza, di PTF (program temporary fix) e lingue secondarie da IBM.
- Remote Workstation Support  (1,636 KB), fornisce informazioni su come impostare e utilizzare il supporto stazione di lavoro, come ad esempio il pass-through della stazione video, la funzione comando host distribuito e il collegamento remoto 3270.
- Cryptographic Support/400  (448 KB), descrive le funzioni per la riservatezza dei dati del programma su licenza Cryptographic Facility. Spiega come utilizzare la funzione e fornisce informazioni di riferimento per i programmatori.
- Local Device Configuration  (763 KB), fornisce informazioni su come effettuare una configurazione iniziale e su come modificare tale configurazione. Contiene inoltre informazioni concettuali sulla configurazione dell'unità.
- *SNA Distribution Services*, SC41-5410 (2,259 KB), fornisce informazioni sulla configurazione di una rete per gli SNADS (Systems Network Architecture distribution service) ed il bridge VM/MVS (Virtual Machine/Multiple Virtual Storage). Inoltre, vengono trattati funzioni di distribuzione oggetto, servizi libreria documenti e servizi indirizzario distribuzione sistema. (Questo manuale non è incluso in questo release di i5/OS Information Center. Tuttavia, potrebbe essere un riferimento utile. Il manuale è disponibile dall'IBM Publications Center come una copia stampata in formato cartaceo che è possibile ordinare o in un formato in linea che può essere scaricato senza alcun costo).
- *ADTS for AS/400: Source Entry Utility*, SC09-2605 (460 KB), fornisce informazioni sull'utilizzo di SEU (source entry utility) Application Development Tools per creare e modificare membri origine. Il manuale spiega come avviare e terminare una sessione SEU e come utilizzare le molte funzioni di questo editor di testo a schermo pieno. Il manuale contiene esempi per aiutare sia gli utenti inesperti che quelli con maggior esperienza a realizzare varie attività di editazione, dai più semplici comandi di riga all'utilizzo di richieste predefinite per formati dati e linguaggi ad alto livello. (Questo manuale non è incluso in questo release di i5/OS Information Center. Tuttavia, potrebbe essere un riferimento utile. Il manuale è disponibile dall'IBM Publications Center come una copia stampata in formato cartaceo che è possibile ordinare o in un formato in linea che può essere scaricato senza alcun costo).

IBM Redbooks

- AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet  (2.1 MB) Questo IBM Redbook descrive questioni relative alla sicurezza e ai rischi associati al collegamento del proprio prodotto System i ad Internet. Fornisce esempi, consigli, suggerimenti e tecniche per le applicazioni.
- Cool Title About the AS/400 and Internet  (7.36 MB) Questo IBM Redbook può essere utile per comprendere ed utilizzare Internet (o la propria intranet) dal proprio prodotto System i. Serve anche a

comprendere come utilizzare le funzioni e le caratteristiche. Questo manuale aiuta ad avere un'introduzione rapida all'utilizzo dell'e-mail, del trasferimento file, dell'emulazione del terminale, di gopher, HTTP e di 5250 ad HTML Gateway.

Siti web

- Lotus Documentation (http://www-10.lotus.com/ldd/doc)

  Questo sito Web fornisce informazioni su Lotus Notes, Domino e IBM Domino for i5/OS. Da questo sito Web, è possibile scaricare informazioni nel formato database Domino (.NSF) e Adobe Acrobat (.PDF), ricercare database e scoprire come si possono ottenere manuali stampati.

Altre informazioni

- Planning and setting up system security fornisce una serie di suggerimenti pratici per l'utilizzo delle funzioni di sicurezza di iSeries e per stabilire le procedure operative relative alla sicurezza. Questo manuale descrive anche come configurare ed utilizzare gli strumenti di sicurezza che fanno parte di i5/OS.
- *Implementing AS/400 Security, 4th Edition* (15 ottobre 2000) a cura di Wayne Madden e Carol Woodbury. Loveland, Colorado: 29th Street Press. Fornisce supporto e suggerimenti pratici per la pianificazione, l'impostazione e la gestione della sicurezza della sicurezza del sistema.

  Numero ordine ISBN
  1583040730
- System i Access per Windows fornisce informazioni tecniche sui programmi System i Access per Windows per tutte le versioni di System i Access per Windows
- TCP/IP setup fornisce informazioni che descrivono come utilizzare e configurare TCP/IP.
- Applicazioni TCP/IP, protocolli e servizi fornisce informazioni che descrivono come utilizzare le applicazioni TCP/IP, come FTP, SMTP e TELNET.
- Operazioni di base di sistema fornisce informazioni su come avviare e arrestare il sistema e gestire i problemi del sistema.
- Integrated file system fornisce una panoramica dell'IFS (integrated file system) inclusa la sua definizione, le possibili modalità di utilizzo e le interfacce disponibili.
- iSeries and Internet security aiuta ad affrontare preoccupazioni relative alla sicurezza che potrebbero insorgere quando si collega iSeries ad Internet. Per ulteriori informazioni, visitare la seguente home page IBM I/T (Information Technology) Security: http://www.ibm.com/security. Optical storage fornisce informazioni sulle funzioni univoche per *Supporto ottico*. Contiene inoltre informazioni utili per l'utilizzo e la comprensione di; Unità CD, Unità libreria supporti magnetici unità ottica direttamente collegati e Unità libreria supporti magnetici unità ottica collegati alla LAN.
- Stampa fornisce informazioni sugli elementi e i concetti del sistema relativi alla stampa, i file di stampa ed il supporto spool di stampa per le operazioni di stampa e la connessione della stampante.
- Control language fornisce un'ampia esposizione di argomenti di di programmazione, inclusa una discussione generale relativa ad oggetti e librerie, programmazione CL, controllo delle flusso e delle comunicazioni tra programmi, gestione di oggetti nei programmi CL e creazione dei programmi CL. Altri argomenti includono messaggi predefiniti ed estemporanei e gestione messaggi, definizione e creazione di comandi e menu definiti dall'utente, verifica delle applicazioni, compresi modalità debug, punti di interruzione, tracce e funzioni di pannello.

  Esso fornisce anche una descrizione di tutto il CL (control language) iSeries ed i relativi comandi i5/OS. I comandi i5/OS vengono utilizzati per richiedere funzioni del programma su licenza i5/OS (5722-SS1). Tutti i comandi CL non-i5/OS—quelli associati con gli altri programmi su licenza, inclusi tutti i vari linguaggi e programmi di utilità—sono descritti in altri manuali che supportano tali programmi su licenza.
- Programmazione fornisce informazioni su molti dei linguaggi e dei programmi di utilità disponibili in iSeries. Contiene riepiloghi di:

  - Tutti i comandi CL iSeries (nel programma i5/OS e in tutti gli altri programmi su licenza), in vari formati.
  - Informazioni relative ai comandi CL, come ad esempio messaggi di errore che è possibile monitorare per ogni comando ed i file forniti da IBM che sono utilizzati da alcuni comandi.
  - Oggetti forniti da IBM, incluse le librerie.
  - Valori di sistema forniti da IBM.
  - Parole chiave DDS per file fisici, logici, video, di stampa e ICF.
  - Istruzioni REXX e funzioni incorporate.
  - Altri linguaggi (come RPG) e programmi di utilità (come SEU e SDA).
- Gestione sistemi include informazioni sulla raccolta di dati delle prestazioni, gestione dei valori di sistema e gestione della memoria.
- Database file concepts fornisce una panoramica delle modalità di progettazione, scrittura, esecuzione e verifica delle istruzioni di DB2 Query Manger e SQL Development Kit per i5/OS. Descrive anche SQL interattivo (Structured Query Language) e fornisce esempi di come scrivere istruzioni SQL in COBOL, RPG, C, FORTRAN e programmi PL/I. Fornisce anche informazioni relativamente alla modalità di:
  - Creare, conservare ed eseguire query SQL
  - Creare prospetti che spaziano dal semplice al complesso
  - Creare, aggiornare, gestire, query e prospetti su tabelle di database utilizzando un'interfaccia basata sui moduli
  - Definire e creare un prototipo di query e prospetti SQL per l'inclusione in programmi dell'applicazione

Salvataggio dei file PDF

Per salvare un file PDF sulla propria stazione di lavoro per poterlo poi visualizzare o stampare:

1. Fare clic con il tastino destro del mouse sul PDF nel browser (fare clic sul collegamento precedente).
2. Fare clic sull'opzione che salva il PDF in locale.
3. Andare all'indirizzario in cui si desidera salvare il PDF.
4. Fare clic su **Salva**.

Come scaricare Adobe Reader

È necessario Adobe Reader per visualizzare o stampare questi PDF. È possibile scaricare una copia gratuita dal sito sito Web Adobe (www.adobe.com/products/acrobat/readstep.html) .

Appendice I. Informazioni particolari

Queste informazioni sono state progettate per prodotti e servizi offerti negli Stati Uniti.

IBM potrebbe non fornire ad altri paesi prodotti, servizi o funzioni discussi in questo documento. Contattare il rappresentante IBM locale per informazioni sui prodotti e servizi correntemente disponibili nella propria area. Qualsiasi riferimento ad un prodotto, programma o servizio IBM non implica o intende dichiarare che solo quel prodotto, programma o servizio IBM può essere utilizzato. Qualsiasi prodotto funzionalmente equivalente al prodotto, programma o servizio che non violi alcun diritto di proprietà intellettuale IBM può essere utilizzato. Tuttavia la valutazione e la verifica dell'uso di prodotti o servizi non IBM ricadono esclusivamente sotto la responsabilità dell'utente.

IBM può avere brevetti o domande di brevetto in corso relativi a quanto trattato nel presente documento. La fornitura del presente documento non garantisce alcuna licenza a tali brevetti. Chi desiderasse ricevere informazioni relative a licenza può rivolgersi per iscritto a:

IBM Director of Commercial Relations
IBM Europe
Schoenaicher Str. 220
D-7030 Boeblingen,
Deutschland

Per richieste di licenze relative ad informazioni double-byte (DBCS), contattare il Dipartimento di Proprietà Intellettuale IBM nel proprio paese o inviare richieste per iscritto a:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Giappone

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: IBM FORNISCE QUESTA PUBBLICAZIONE "COSÌ COM'È" 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. Le modifiche alle presenti informazioni vengono effettuate periodicamente; tali modifiche saranno incorporate nelle nuove pubblicazioni della pubblicazione. 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.

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:

IBM Europe

Software Interoperability Coordinator, Department YBWA
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 da IBM nei termini dell'IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code o qualsiasi altro accordo equivalente tra le parti.

Tutti i dati relativi alle prestazioni contenuti in questa pubblicazione sono stati determinati in un ambiente controllato. Pertanto, i risultati ottenuti in ambienti operativi diversi possono variare in modo considerevole. È 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, è possibile che alcune misurazioni siano state calcolate mediante estrapolazione. I risultati possono quindi variare. Gli utenti di questa pubblicazione devono verificare che i dati siano applicabili al loro specifico ambiente.

Le informazioni riguardanti prodotti non IBM sono ottenute dai fornitori di tali prodotti, dai loro annunci pubblicati o da altre fonti pubblicamente reperibili. 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 di IBM sono soggette a modifiche o a revoche senza notifica e rappresentano soltanto scopi ed obiettivi.

Tutti i prezzi IBM mostrati sono i prezzi al dettaglio suggeriti da IBM, sono attuali e soggetti a modifica senza preavviso. I prezzi al fornitore possono variare.

Queste informazioni hanno esclusivamente scopi di pianificazione. Le presenti informazioni sono soggette a modifiche prima che i prodotti descritti siano resi disponibili.

Queste informazioni contengono esempi di dati o prospetti utilizzati in attività aziendali giornaliere. Al solo scopo di raffigurarli come possibili, gli esempi comprendono i nomi di singoli, aziende, marchi e prodotti. Questi nomi sono fittizi e qualsiasi riferimento a nomi e indirizzi utilizzati realmente da aziende è puramente casuale.

LICENZA SOGGETTA ALLE LEGGI SUL DIRITTO D'AUTORE:

Queste informazioni contengono esempi di programmi applicativi in lingua originale, che illustrano le tecniche di programmazione su diverse piattaforme operative. È possibile copiare, modificare e distribuire questi programmi di esempio in qualsiasi formato senza pagare alcun corrispettivo a 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.

Ogni copia, parte di questi programmi di esempio o lavoro derivato, devono includere un avviso sul copyright, come ad esempio:

© (nome società) (anno). Le parti di questo codice provengono da IBM Corp. Sample Programs. © Copyright IBM Corp. _immettere l'anno o gli anni_. Tutti i diritti riservati.

Se si sta utilizzando la versione in formato elettronico di questo manuale, le fotografie e le illustrazioni a colori potrebbero non essere visualizzate.

Informazioni sulle interfacce di programmazione

Queste pubblicazioni sui riferimenti alla sicurezza illustrano le interfacce di programmazione che consentono al cliente di scrivere programmi per ottenere servizi di i5/OS.

Marchi registrati

I seguenti termini sono marchi dell'International Business Machines Corporation negli Stati Uniti e in altri paesi:

AIX
corrente
IBM
IBM (logo)
System i
z/OS

Intel, Intel Inside (logos), MMX e Pentium sono marchi di Intel Corporation negli Stati Uniti e/o in altri paese.

Microsoft, Windows, Windows NT e il logo Windows sono marchi registrati della Microsoft Corporation negli Stati Uniti e/o negli altri paesi.

Java e tutti i marchi e i logo basati su Java sono marchi o marchi registrati della Sun Microsystems, Inc. negli Stati Uniti e/o negli altri paesi.

Linux è un marchio registrato di Linus Torvalds negli Stati Uniti e/o negli altri paesi.

UNIX è un marchio registrato di The Open Group negli Stati Uniti e/o in altri paesi.

Altri nomi di aziende, prodotti o servizi riportati in questa pubblicazione sono marchi di altre società.

Windows

Termini e condizioni

Le autorizzazioni per l'utilizzo di queste pubblicazioni vengono concesse in base alle seguenti disposizioni.

Uso personale: è possibile riprodurre queste pubblicazioni per uso personale, non commerciale a condizione che vengano conservate tutte le indicazioni relative alla proprietà. Non è possibile distribuire, visualizzare o produrre lavori derivati di tali pubblicazioni o di qualsiasi loro parte senza chiaro consenso da parte di IBM.

Uso commerciale: è possibile riprodurre, distribuire e visualizzare queste Pubblicazioni unicamente all'interno del proprio gruppo aziendale a condizione che vengano conservate tutte le indicazioni relative alla proprietà. Non è possibile effettuare lavori derivati di queste pubblicazioni o riprodurre, distribuire o visualizzare queste pubblicazioni o qualsiasi loro parte al di fuori del proprio gruppo aziendale senza chiaro consenso da parte di IBM.

Fatto salvo quanto espressamente concesso in questa autorizzazione, non sono concesse altre autorizzazioni, licenze o diritti, espressi o impliciti, relativi alle pubblicazioni o a qualsiasi informazione, dato, software o altra proprietà intellettuale qui contenuta.

IBM si riserva il diritto di ritirare le autorizzazioni qui concesse qualora, a propria discrezione, l'utilizzo di queste pubblicazioni sia a danno dei propri interessi o, come determinato da IBM, qualora non siano rispettate in modo appropriato le suddette istruzioni.

Non è possibile scaricare, esportare o ri-esportare queste informazioni se non pienamente conformi con tutte le leggi e le norme applicabili, incluse le leggi e le norme di esportazione degli Stati Uniti.

IBM NON RILASCIA ALCUNA GARANZIA RELATIVAMENTE AL CONTENUTO DI QUESTE PUBBLICAZIONI. LE PUBBLICAZIONI SONO FORNITE "COSI' COME SONO", SENZA ALCUN TIPO DI GARANZIA, ESPRESSA O IMPLICITA, INCLUSE, A TITOLO ESEMPLIFICATIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ ED IDONEITÀ PER UNO SCOPO PARTICOLARE.

Indice analitico

Caratteri speciali

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Stampato in Italia

SC13-3195-10