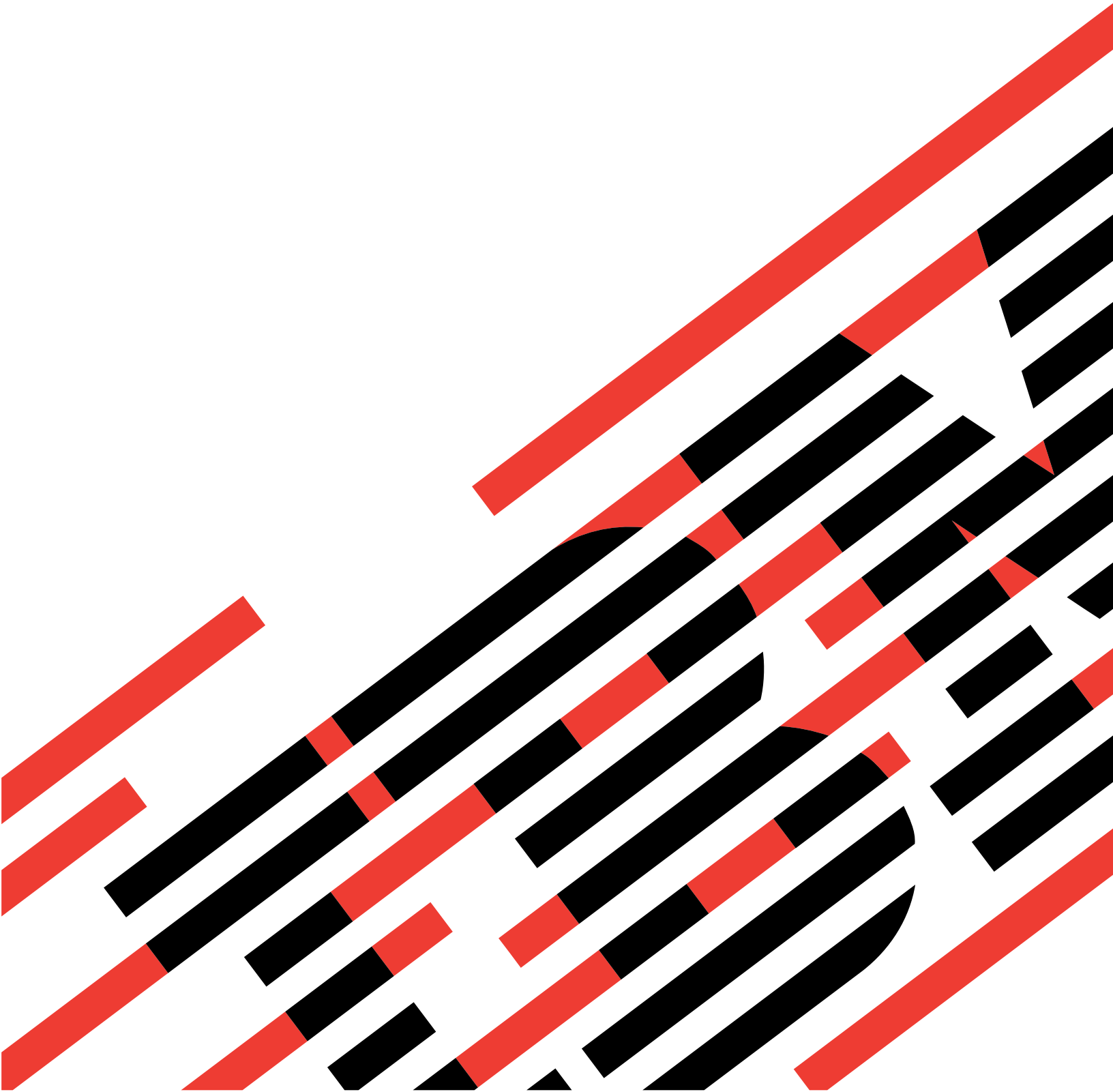
IBM

eserver

iSeries

Pianificazione e sicurezza di base del sistema



IBM

@server

iSeries

Pianificazione e sicurezza di base del sistema

Indice

Parte 1. Pianificazione e sicurezza di base del sistema

Pianificazione e sicurezza di base del sistema iSeries fornisce informazioni dettagliate sulla pianificazione e sulla configurazione dei dati inerenti alla sicurezza iSeries. Questo argomento pone l'accento sulle attività di pianificazione e fornisce i moduli che possono essere utilizzati per pianificare e registrare le decisioni relative alla sicurezza. Fornisce inoltre istruzioni dettagliate per la sicurezza di base del sistema. Considerando la natura di questo argomento, è possibile che si desideri stamparlo per visualizzare le informazioni in modo più approfondito.

La configurazione dei dati relativi alla sicurezza per l'iSeries prevede due tipi principali di attività: pianificazione e configurazione. Per verificare di aver impostato il livello di sicurezza necessario all'azienda, occorre visualizzare nuovamente gli argomenti sulla pianificazione:

- Informazioni preliminari sulla sicurezza di base del sistema fornisce una panoramica dei concetti sulla sicurezza generale e le risposte sulla sicurezza di base del sistema.
- Pianificare la sicurezza dell'utente fornisce le informazioni su come pianificare la sicurezza relativa agli utenti del sistema. Questo include la sicurezza fisica, la sicurezza dell'applicazione, la strategia generale per la sicurezza e i profili utente sul sistema.
- Pianificare la sicurezza delle risorse fornisce informazioni su come pianificare la sicurezza degli oggetti sul proprio sistema, inclusi le librerie e gli oggetti, le stampanti, l'emissione di stampa e le stazioni di lavoro.

Dopo aver completato le attività di pianificazione, è possibile rivedere questi argomenti e utilizzarli come supporto per l'impostazione dei dati relativi alla sicurezza del proprio sistema:

- Impostare la sicurezza dell'utente fornisce dettagli sull'impostazione dei dati relativi alla sicurezza dell'utente e del gruppo.
- Impostare la sicurezza delle risorse fornisce informazioni su come impostare la proprietà degli oggetti, l'autorizzazione pubblica e specifica agli oggetti e la sicurezza per le stampanti e le stazioni di lavoro.
- Verificare la sicurezza fornisce informazioni sulla verifica della sicurezza.
- Modificare le informazioni sulla sicurezza fornisce informazioni sull'aggiornamento e sulla modifica dei profili di gruppo e utente e della sicurezza delle risorse.
- Salvare le informazioni sulla sicurezza fornisce informazioni sulla copia di riserva delle informazioni sulla sicurezza.
- Monitorare la sicurezza fornisce liste di controllo per registrare i dati per la sicurezza e le informazioni sul controllo della sicurezza.

Oltre a questi argomenti, utilizzare i moduli di pianificazione per documentare le strategie di pianificazione e le decisioni relative alla sicurezza.

Capitolo 1. Novità

A partire dalla versione V4R5, Pianificazione e sicurezza di base del sistema costituisce una novità per l'Information Center. In precedenza, queste informazioni erano contenute nel manuale *Security-Basic* (SC41-5301-00). Sono state aggiornate per riflettere le informazioni correnti sull'impostazione della sicurezza per i sistemi V4R5.

Capitolo 2. Stampare questo argomento

E’ possibile visualizzare o scaricare una versione PDF di questo documento per la visualizzazione o la stampa. Per visualizzare i file PDF, è necessario avere installato Adobe® Acrobat® Reader. E’ possibile scaricare una copia dalla home page Adobe 

Per visualizzare o scaricare la versione PDF, selezionare Pianificazione e sicurezza di base del sistema (950 KB o 164 pagine).

Per salvare un PDF sulla stazione di lavoro per la visualizzazione o la stampa:

1. Aprire il PDF nel browser (fare clic sul precedente collegamento).
2. Nel menu del browser, fare clic su **File**.
3. Fare clic su **Salva con nome...**
4. Andare all’indirizzario nel quale si desidera salvare il PDF.
5. Fare clic su **Salva**.

Capitolo 3. Informazioni preliminari sulla sicurezza di base del sistema

La sicurezza riguarda tutti, dagli amministratori del sistema agli utenti. La sicurezza del sistema protegge i dati per l'azienda contenuti nell'iSeries da eventuali violazioni di accesso sia intenzionali che involontarie.

E' possibile personalizzare le condizioni di sicurezza del sistema in base alle condizioni ambientali ed alle proprie esigenze.

Si pensi alla sicurezza come ad una porta di ingresso al sistema. Le funzioni di sicurezza si utilizzano per **bloccare** o proteggere le informazioni dall'utilizzo non autorizzato.

Le funzioni di sicurezza si utilizzano per **ripristinare** la flessibilità del sistema, precedentemente bloccata, e personalizzarla per ogni utente.

Con un buon programma per la sicurezza è possibile offrire delle condizioni di sicurezza generale del sistema, ma non è possibile garantire la sicurezza delle apparecchiature o delle informazioni. Si consiglia di ripartire le responsabilità del sistema fra più dipendenti per essere sicuri che nessuno detenga il controllo esclusivo del sistema.

Pianificazione e sicurezza di base del sistema fornisce un approccio dettagliato alla pianificazione ed all'impostazione della sicurezza di base del sistema. Questo argomento sottolinea l'importanza della pianificazione della sicurezza del sistema e fornisce dei moduli di pianificazione utili per registrare le proprie decisioni relative alla sicurezza. Per suggerimenti in merito, nel presente documento viene proposto un esempio di azienda che sta pianificando la propria sicurezza.

Per garantire che la realizzazione della sicurezza del sistema abbia esito positivo, è essenziale una pianificazione valida e completa. Esaminare questi argomenti per documentarsi sulle fondamentali esigenze di sicurezza e sull'importanza della pianificazione della sicurezza:

- FAQ (Frequently asked questions) sulla sicurezza di base del sistema
- Una panoramica della sicurezza di base del sistema
- Un metodo di pianificazione della sicurezza di base del sistema

Si consiglia inoltre di predisporre un'adeguata pianificazione per il ripristino e le copie di riserva di tutte le informazioni presenti sul sistema. Inoltre, si consiglia di pianificare la sostituzione delle apparecchiature in caso di gravi problemi. Per ulteriori informazioni su una buona pianificazione della copia di riserva, consultare l'argomento Copia di riserva e ripristino nell'Information Center.

Informazioni dettagliate sulla pianificazione della sicurezza dell'utente

I seguenti argomenti forniscono delle tecniche per la pianificazione della sicurezza dell'utente:

- Pianificare la sicurezza delle applicazioni
- Pianificare la strategia di sicurezza
- Pianificare i gruppi di utenti
- Pianificare i singoli profili utente

Informazioni dettagliate sulla pianificazione della sicurezza delle risorse

I seguenti argomenti forniscono un approccio sistematico per pianificare la sicurezza delle risorse per gli utenti.

- Comprendere i tipi di autorizzazione
- Pianificare la sicurezza per le librerie dell'applicazione
- Determinare la proprietà di librerie e di oggetti

- Raggruppare gli oggetti
- Proteggere l'emissione di stampa
- Proteggere le stazioni di lavoro
- Pianificare l'installazione dell'applicazione

Moduli di pianificazione stampabili

Pianificazione e sicurezza di base del sistema fornisce dei moduli di pianificazione stampabili che consentono di registrare tutte le decisioni relative alla sicurezza. E' possibile stampare l'intero argomento in formato PDF o i singoli moduli di pianificazione utilizzando il pulsante di stampa del browser.

Istruzioni dettagliate per l'impostazione della sicurezza di base del sistema

Dopo aver completato la pianificazione della sicurezza, questo argomento fornisce delle istruzioni per rendere operativo il programma di sicurezza. I seguenti argomenti forniscono una guida per impostare la sicurezza del sistema.
- Impostare la sicurezza dell'utente
- Impostare la sicurezza delle risorse

FAQ (Frequently asked questions) sulla sicurezza di base del sistema

L'esame delle risposte alle FAQ sulla sicurezza può costituire un valido aiuto per una migliore comprensione dell'importanza della sicurezza per il sistema.

Perché è importante la sicurezza?

Le informazioni memorizzate nel sistema costituiscono una delle più importanti risorse dell'azienda. Quando si valutano i metodi di protezione delle informazioni, è necessario prendere in considerazione tre importanti obiettivi:
- **Riservatezza:** buone misure di sicurezza possono impedire che qualcuno consulti e venga a conoscenza di informazioni riservate.
- **Integrità:** per certi versi, un sistema di sicurezza ben progettato è in grado di assicurare l'accuratezza delle informazioni sul computer. Con il giusto tipo di sicurezza, è possibile impedire modifiche o cancellazioni non autorizzate di dati.
- **Disponibilità:** se qualcuno danneggia accidentalmente o intenzionalmente dei dati presenti nel sistema, non è possibile accedere a quelle risorse fino a che non vengono recuperate. Un buon sistema di sicurezza è in grado di impedire questo tipo di danni.

Quando si pensa alla sicurezza del sistema, generalmente si pensa di proteggerlo da persone esterne alla società, ad esempio i concorrenti commerciali. In realtà, la protezione dalla curiosità o dagli incidenti di sistema da parte di utenti autorizzati è spesso il maggior beneficio di un sistema di sicurezza ben progettato. In un sistema privo di efficienti funzioni per la sicurezza, un utente potrebbe accidentalmente cancellare un file importante. Un sistema funzionale per la sicurezza consente di evitare questo tipo di incidenti.

E' necessario porsi le seguenti domande quando si stabilisce il livello di sicurezza necessaria per il sistema:
- Quanto è importante il proprio computer (e i dati che vi sono memorizzati) per la propria azienda?
- Esiste una politica aziendale che richiede livelli di sicurezza specifici?
- I propri revisori richiedono un livello di sicurezza per le informazioni memorizzate nel computer?
- Si necessiterà di un certo grado di sicurezza nell'immediato futuro?

Perché personalizzare il proprio sistema?

L'iSeries comprende una vasta gamma di utenti. Un sistema di piccole dimensioni potrebbe avere da tre a cinque utenti che eseguono poche applicazioni. Un sistema di grandi dimensioni potrebbero avere migliaia di utenti su una vasta rete di comunicazione che eseguono molte applicazioni.

La progettazione iSeries fornisce una grande flessibilità per soddisfare le esigenze di una vasta gamma di utenti e di situazioni. Si ha la possibilità di apportare parecchie modifiche al modo in cui il sistema appare agli utenti nonché al suo funzionamento.

Alla consegna del sistema, probabilmente non si riterrà necessario personalizzarlo. L'IBM consegna il sistema con delle impostazioni iniziali, denominati **valori predefiniti**, per molte opzioni. Questi valori predefiniti sono le scelte che di solito funzionano meglio sulle nuove installazioni.

Nota: tutti i nuovi sistemi vengono consegnati con un livello di sicurezza predefinito di **40**. Questo livello di sicurezza garantisce che solo gli utenti definiti possono utilizzare il sistema. Evita inoltre i potenziali rischi di integrità e di sicurezza generati dai programmi in grado di eludere la sicurezza.

Tuttavia, se si effettua qualche personalizzazione, è possibile rendere il sistema uno strumento più semplice e più efficace per gli utenti. Ad esempio, è possibile assicurarsi che un utente richiami sempre il menu corretto quando si collega. E' possibile assicurarsi che i prospetti di ogni utente siano inviati alla stampante corretta. Gli utenti si affideranno maggiormente al sistema se verranno effettuate delle personalizzazioni iniziali per farlo apparire e percepire come il proprio sistema.

Chi dovrebbe essere responsabile?

Aziende diverse hanno diversi approcci alla sicurezza. A volte i programmatori sono responsabili di tutti gli aspetti della sicurezza. In altri casi, la persona che si occupa di gestire il sistema è responsabile anche della sicurezza. Se non si è certi del modo in cui attribuire la responsabilità nella propria società, qui di seguito è riportato un suggerimento:

- Il metodo di pianificazione della sicurezza delle risorse varia a seconda che l'azienda acquisti o sviluppi le applicazioni. Se si sviluppano le applicazioni per proprio conto, comunicare le esigenze di sicurezza delle risorse durante il processo di sviluppo. Se si acquistano le applicazioni, lavorare con il designer delle applicazioni. In entrambi i casi, chi progetta le applicazioni deve considerare la sicurezza come parte integrante del progetto.
- L'impostazione della sicurezza dovrebbe essere responsabilità di un responsabile della riservatezza. Il responsabile della riservatezza definisce gli utenti del sistema ed il loro accesso al sistema. Il responsabile della riservatezza ha altre responsabilità nel sistema, come ad esempio la copia di riserva ed il ripristino delle informazioni.
- Il responsabile della riservatezza si occupa inoltre di personalizzare il sistema, dal momento che molti elementi di sicurezza giocano un ruolo importante nella personalizzazione del sistema.

Indipendentemente dal metodo utilizzato per attribuire la responsabilità della sicurezza, **comunicare una normativa di sicurezza**. Un dirigente dell'azienda dovrebbe comunicare a tutti, preferibilmente in forma scritta, che le informazioni presenti nel computer sono una risorsa importante. Si consiglia di proteggere quelle informazioni, proprio come si farebbe con ogni altra risorsa dell'azienda. Consultare ″Esempio: normativa sulla sicurezza dell'Azienda di giocattoli JKL″ per un esempio di normativa di sicurezza.

Una volta stabilita l'esigenza di sicurezza del sistema, potrebbe essere necessario esaminare una panoramica delle considerazioni di sicurezza del sistema.

Una panoramica della sicurezza di base del sistema

Per effettuare una pianificazione efficace, è necessario comprendere la relazione esistente fra ciò che si desidera ottenere e gli strumenti forniti dal sistema. E' necessario conoscere il modo in cui le funzioni utente e di sistema interagiscono per il conseguimento degli obiettivi.

I seguenti argomenti introducono delle importanti nozioni sulla sicurezza e sulla personalizzazione e mostrano il loro funzionamento congiunto. Questi argomenti intendono fornire una panoramica utile prima dell'inizio della pianificazione. Tutti i concetti qui di seguito introdotti verranno esplicati in maniera più dettagliata via via che se ne presenterà la necessità durante il processo di pianificazione.

- Sicurezza del sistema incorporata
- Terminologia di base
- Considerazioni dell'utente circa la sicurezza
- Strumenti di sistema per la sicurezza e la personalizzazione

Sicurezza del sistema incorporata

Tutto ciò che concerne la sicurezza del sistema viene incorporato nel sistema. Non si tratta di un prodotto che si acquista a parte. Questo approccio integrato presenta diversi vantaggi:

- La sicurezza è coerente con il resto del sistema operativo. Essa utilizza gli stessi pannelli, comandi e terminologia.
- Gli utenti non possono ignorare la questione della sicurezza, poiché è parte integrante del software.
- La sicurezza progettata correttamente influenza in minima parte le prestazioni.
- La sicurezza segue sempre i nuovi sviluppi del software. Quando si rendono disponibili nuove funzioni, si rende disponibile la sicurezza relativa a tali funzioni.

L'iSeries viene consegnato con un livello di sicurezza di 40, che impedisce a utenti non autorizzati di collegarsi al sistema. Evita inoltre i potenziali rischi di integrità e di sicurezza da parte di programmi che possono eludere la sicurezza. Tuttavia, è possibile personalizzare alcune impostazioni di sicurezza o modificare i livelli di sicurezza. I livelli di sicurezza vengono descritti nell'argomento, ″Scegliere il livello di sicurezza.″

Una volta chiarito il concetto del modo in cui opera la sicurezza incorporata, è possibile familiarizzare con la comune terminologia dell'iSeries.

Terminologia di base

Questa serie di termini generici è molto importante per la comprensione della sicurezza iSeries:

Oggetto
Un oggetto è uno spazio denominato nel sistema che può essere manipolato. Gli esempi più comuni di oggetti sono i file ed i programmi. Altri tipi di oggetti includono comandi, code, librerie e cartelle. Gli oggetti presenti nel sistema vengono identificati dal nome dell'oggetto, dal tipo di oggetto e dalla libreria in cui risiede l'oggetto. E' possibile proteggere ogni oggetto presente nel sistema.

Libreria
Una libreria è un tipo speciale di oggetto utilizzato per raggruppare altri oggetti. Molti oggetti presenti nel sistema risiedono in una libreria.

Indirizzario
Un indirizzario è un'altra modalità di raggruppamento degli oggetti presenti nel sistema. Gli oggetti possono risiedere in un indirizzario. Un indirizzario può risiedere in un altro indirizzario, così da formare una struttura gerarchica.

Una volta acquisita la terminologia generica della sicurezza iSeries, è possibile esaminare il modo in cui un utente giudica la sicurezza.

Considerazioni dell'utente circa la sicurezza

Dal punto di vista dell'utente, la sicurezza influisce sul modo in cui gli utenti stessi utilizzano e portano a termine le attività nel sistema. Essa include inoltre il modo in cui gli utenti interagiscono con il sistema per portare a termine tali attività. E' importante considerare il modo in cui un utente giudica la sicurezza. Ad

esempio, l'impostazione della scadenza delle parole d'ordine ogni cinque giorni potrebbe risultare problematica ed interferire con la capacità dell'utente di portare a termine il proprio lavoro. D'altro canto, una normativa non rigorosa relativa alle parole d'ordine potrebbe causare dei problemi di sicurezza.

Per fornire la sicurezza più adatta al sistema, è necessario ripartire la sicurezza in parti specifiche che è possibile pianificare, gestire e monitorare. Dal punto di vista dell'utente, è possibile ripartire la sicurezza del sistema in diverse parti:

Accesso fisico al sistema

La sicurezza fisica protegge l'unità di sistema, tutte le unità di sistema ed i supporti magnetici di memorizzazione di riserva (ad esempio dischetti, nastri o CD) da perdite o danni involontari o intenzionali.

La maggior parte delle misure intraprese per proteggere la sicurezza fisica del sistema sono esterne al sistema stesso. Il sistema, tuttavia, viene consegnato con una chiave di blocco o una chiave elettronica che impedisce un utilizzo non autorizzato delle funzioni sull'unità di sistema.

L'argomento ″Pianificare la sicurezza fisica″ fornisce informazioni dettagliate che consentono di pianificare la sicurezza fisica del sistema.

Come si collegano gli utenti

La sicurezza del collegamento impedisce che una persona non identificata dal sistema possa collegarsi. Per collegarsi, è necessario immettere una combinazione valida di ID utente e parola d'ordine.

E' possibile utilizzare sia i valori di sistema che i singoli profili utente affinché la sicurezza del collegamento non venga violata. Ad esempio, è possibile richiedere che le parole d'ordine vengano modificate a cadenza regolare. E' inoltre possibile impedire l'utilizzo di parole d'ordine facilmente individuabili.

Operazioni consentite agli utenti

Un importante ruolo della sicurezza, e della personalizzazione del sistema, consiste nel definire le operazioni consentite agli utenti. Dal punto di vista della sicurezza, si tratta spesso di una funzione **limitante**, volta, ad esempio, ad evitare che si possano consultare determinate informazioni. Dal punto di vista della personalizzazione del sistema, si tratta di una funzione **qualificante**. Un sistema correttamente personalizzato consente di svolgere il proprio lavoro eliminando attività ed informazioni superflue.

Alcuni metodi utilizzati per definire le operazioni consentite agli utenti sono competenza del responsabile della riservatezza, altri sono competenza dei programmatori. Queste informazioni si concentrano principalmente sulle attività svolte solitamente da un responsabile della riservatezza. E' possibile trovare le descrizioni di tutti i valori di sistema nel Capitolo 3, ″Security System Values,″ del *Security-Reference* (SC41-5302).

Per il controllo delle operazioni consentite all'utente nel sistema, sono disponibili dei parametri nei singoli profili utente, nelle descrizioni lavoro e nelle classi. La seguente lista descrive brevemente le tecniche disponibili:

Limitare gli utenti a poche funzioni
: E' possibile limitare gli utenti ad uno specifico programma, menu o serie di menu e a pochi comandi di sistema in base al loro profilo utente. Generalmente, il responsabile della riservatezza crea e controlla i profili utente.

Limitare le funzioni di sistema
: Le funzioni di sistema consentono di salvare e ripristinare informazioni, gestire l'emissione di stampa e configurare i nuovi utenti del sistema. Ogni profilo utente specifica quali delle più comuni funzioni di sistema possono essere eseguite.

Sull'iSeries, le funzioni di sistema vengono eseguite utilizzando i comandi CL (control language) e le API (application programming interfaces). Poiché tutti i comandi e le API sono degli oggetti, è possibile utilizzare le autorizzazioni all'oggetto per controllare a chi sia consentito utilizzarli e portare a termine le funzioni di sistema.

Stabilire chi può utilizzare file e programmi

La sicurezza delle risorse consente di controllare l'utilizzo di ogni oggetto presente nel sistema. Per ogni oggetto, è possibile specificare a chi ne sia consentito l'utilizzo e le modalità di tale utilizzo. Ad esempio, è possibile specificare che un utente possa soltanto consultare le informazioni contenute in un file; che un altro utente possa modificare i dati contenuti nel file; che un terzo utente possa modificare il file o cancellare l'intero file.

Prevenire l'abuso delle risorse del sistema

La potenza di elaborazione del sistema può diventare tanto importante per l'azienda quanto i dati in esso memorizzati. Il responsabile della riservatezza garantisce che gli utenti non utilizzino impropriamente le risorse del sistema eseguendo i propri lavori con priorità alta, stampando per prima la propria documentazione o utilizzando troppa memoria del disco.

Modalità di comunicazione fra il sistema ed altri computer

Potrebbero essere necessarie ulteriori misure di sicurezza se il sistema comunica con altri computer o con stazioni di lavoro programmabili. Se non si dispone di adeguati controlli di sicurezza, è possibile che qualcuno da un altro computer della rete avvii un lavoro o abbia accesso a delle informazioni contenute nel proprio computer senza effettuare il processo di collegamento.

E' possibile utilizzare sia i valori di sistema che gli attributi di rete per controllare se nel sistema siano consentiti lavori remoti, accesso remoto dei dati o accesso da un PC remoto. Se è consentito l'accesso remoto, è possibile specificare il tipo di sicurezza da applicare. E' possibile trovare le descrizioni di tutti i valori di sistema nel Capitolo 3, ″Security System Values,″ del *Security-Reference* (SC41-5302).

Modalità di salvataggio delle informazioni relative alla sicurezza

E' necessario effettuare regolarmente delle copie di riserva delle informazioni contenute nel sistema. Oltre a salvare i dati contenuti nel sistema, è necessario salvare le informazioni relative alla sicurezza. Se si verifica un problema grave, è necessario essere in grado di ripristinare le informazioni sugli utenti del sistema, le informazioni relative all'autorizzazione e le informazioni stesse.

L'argomento ″Salvare le informazioni relative alla sicurezza″ spiega come salvare le informazioni di sicurezza. L'argomento Copia di riserva e ripristino nell'Information Center fornisce ulteriori informazioni circa le copie di riserva ed il ripristino dei dati relativi alla sicurezza.

Modalità di monitoraggio del piano di sicurezza

Il sistema fornisce diversi strumenti per monitorare l'efficacia della sicurezza:

- Quando si verificano delle violazioni della sicurezza vengono inviati dei messaggi all'operatore di sistema.
- E' possibile registrare su un giornale di controllo speciale le varie transazioni relative alla sicurezza.

L'argomento, ″Monitorare la sicurezza″ esamina per grandi linee l'utilizzo di tali strumenti. E' possibile trovare ulteriori dettagli circa il controllo della sicurezza nel Capitolo 9, ″Auditing Security on the System,″ del *Security-Reference* (SC41-5302).

Per meglio comprendere le modalità di personalizzazione del sistema, è necessario conoscere il parere dell'utente riguardo alla personalizzazione.

Considerazioni dell'utente circa la personalizzazione del sistema

E' possibile personalizzare il sistema per consentire agli utenti di svolgere il proprio lavoro giorno per giorno. Per personalizzare nel migliore dei modi il sistema per gli utenti, considerare le loro necessità al fine di far svolgere il lavoro nel migliore dei modi. E' possibile personalizzare il sistema in modo da mostrare i menu e le applicazioni in diversi modi:

Mostrare agli utenti ciò che vogliono consultare

La maggior parte delle persone organizza le proprie scrivanie ed i propri uffici in modo da poter accedere più facilmente agli oggetti necessari. E' quindi necessario considerare l'accesso degli utenti al sistema nello stesso modo. Dopo aver effettuato il collegamento al sistema, è necessario che l'utente visualizzi prima di tutto il menu o il pannello maggiormente utilizzato. Perché ciò avvenga, è possibile progettare con facilità i profili utente.

Eliminare il superfluo

La maggior parte dei sistemi contiene diverse applicazioni. La maggior parte degli utenti desidera visualizzare solo ciò che è necessario per i propri lavori. La limitazione degli utenti a poche funzioni di sistema facilita i loro lavori. Tramite i profili utente, le descrizioni lavoro e i menu appropriati, è possibile fornire ad ogni utente una visualizzazione specifica del sistema.

Inviare i dati nel posto giusto

Gli utenti non dovrebbero preoccuparsi di come far giungere la propria documentazione alla stampante corretta o del modo in cui eseguire i propri lavori batch. Ciò compete ai valori di sistema, ai profili utente ed alle descrizioni lavoro.

Assistenza

Non è importante che il sistema sia stato personalizzato bene, se poi gli utenti si pongono domande di tipo ″Dov'è finita la mia documentazione?″ o ″Il lavoro è ancora in esecuzione?″ I pannelli dell'**Operational Assistant** forniscono una semplice interfaccia per le funzioni di sistema, che consente agli utenti di trovare risposta a queste domande. Le diverse versioni dei pannelli del sistema, denominate **livelli di assistenza**, forniscono assistenza agli utenti con diversi livelli di competenza tecnica. Alla consegna del sistema, i pannelli dell'Operational Assistant sono automaticamente resi disponibili a tutti gli utenti. La progettazione delle applicazioni, tuttavia, potrebbe richiedere delle modifiche alle modalità di accesso degli utenti al menu dell'Operational Assistant.

L'iSeries fornisce degli strumenti di sistema che consentono di personalizzare la sicurezza del sistema in modo da proteggere le risorse e consentendo allo stesso tempo l'accesso alle stesse da parte degli utenti.

Strumenti di sistema per la sicurezza e la personalizzazione

Per effettuare una pianificazione efficace, è necessario comprendere la relazione esistente fra gli obiettivi di sicurezza e gli strumenti forniti dal sistema. E' possibile utilizzare questi strumenti di sistema per personalizzare la sicurezza del sistema.

Livello di sicurezza

L'IBM consegna tutti i nuovi iSeries con un livello di sicurezza pari a 40. Il livello di sicurezza 40 garantisce la sicurezza delle risorse, delle parole d'ordine e l'integrità del sistema. Se si desidera modificare il livello attivo della sicurezza del sistema, è possibile modificare il valore di sistema QSECURITY. Tuttavia, l'IBM consiglia vivamente di mantenere il livello di sicurezza impostato su 40. Per modificare il livello di sicurezza, un utente necessita della classe utente *SECOFR o delle autorizzazioni speciali *ALLOBJ e * SECADM.

Il sistema fornisce quattro livelli di sicurezza, come mostrato nella seguente tabella:

Tabella 1. Livelli di sicurezza disponibili nel sistema

Livello di sicurezza	Descrizione
Livello di sicurezza 20	Fornisce solo sicurezza delle parole d'ordine.
Livello di sicurezza 30	Fornisce sicurezza delle parole d'ordine e delle risorse.
Livello di sicurezza 40	Fornisce sicurezza delle parole d'ordine e delle risorse; sicurezza dell'integrità.
Livello di sicurezza 50	Fornisce sicurezza delle parole d'ordine e delle risorse; protezione dell'integrità avanzata.

L'argomento ″Scegliere il livello di sicurezza″ fornisce dettagli sulla determinazione del livello di sicurezza più adatto alle proprie esigenze.

Valori di sistema

E' possibile impostare i valori di sistema in modo da controllare il modo in cui alcune funzioni del sistema operativo operano nell'iSeries. E' necessario considerare i valori di sistema come parte integrante della politica aziendale. I valori di sistema si applicano a tutti coloro che utilizzano il sistema, a meno che qualcosa di più specifico, ad esempio un profilo utente, non sostituisca il valore di sistema.

I valori di sistema stabiliscono quale sia la stampante principale, in che modo il sistema visualizzi la data e la frequenza con cui è necessario modificare la parola d'ordine.

Attributi di rete

Gli attributi di rete definiscono alcune caratteristiche delle modalità di comunicazione del sistema con altri computer, inclusi i personal computer. Gli attributi di rete si applicano all'intero sistema.

Profili di gruppo

Un profilo di gruppo definisce un gruppo di utenti. E' necessario considerare i profili di gruppo come parte integrante della politica di reparto. E' possibile utilizzare i profili di gruppo come modello per la creazione dei singoli profili utente. E' inoltre possibile utilizzare i profili di gruppo per definire il modo in cui i membri del gruppo possono accedere agli oggetti presenti nel sistema. Per ulteriori informazioni sui profili di gruppo, consultare l'argomento ″Pianificare i gruppi di utenti.″

Profili utente

Il profilo utente è uno degli oggetti più potenti e versatili presenti nel sistema. Contiene la parola d'ordine dell'utente ed il menu che si visualizza all'utente dopo aver effettuato il collegamento. Il profilo utente definisce ciò che una persona può o non può fare nel sistema. Esso determina la visualizzazione univoca del sistema da parte dell'utente. L'argomento ″Pianificare la sicurezza dell'utente″ esamina i suggerimenti relativi alla pianificazione dei profili utente.

Descrizioni lavoro

Una descrizione lavoro funziona congiuntamente ai valori di sistema ed ai profili utente per determinare il modo in cui il sistema elabora i lavori di un utente. La descrizione lavoro configura una lista librerie iniziale dell'utente, per cui determina le librerie alle quali un utente accede automaticamente dopo il collegamento.

Sicurezza delle risorse

Il responsabile della riservatezza protegge le risorse (oggetti) presenti nel sistema, determinando chi è autorizzato ad utilizzarle e il modo in cui l'utente può accedere a tali oggetti. Il responsabile della riservatezza può impostare le autorizzazioni all'oggetto per i singoli oggetti o gruppi di oggetti (liste di autorizzazioni). I file, i programmi e le librerie sono i più comuni oggetti che richiedono protezione, sebbene la sicurezza del sistema consenta di impostare le autorizzazioni all'oggetto per qualunque oggetto presente nel sistema.

E' possibile gestire la sicurezza delle risorse in modo semplice ed efficace, se si pianifica un approccio diretto e generale. Uno schema di sicurezza delle risorse creato senza una precedente pianificazione può risultare complicato ed inefficace. L'argomento, ″Pianificare la sicurezza delle risorse″ descrive le modalità di pianificazione della sicurezza delle risorse.

Il sistema fornisce diversi strumenti di assistenza per la progettazione diretta di uno schema di sicurezza delle risorse:

- **Profili di gruppo:** è possibile raggruppare utenti simili in un singolo profilo di gruppo. Il gruppo di utenti, quindi, può condividere la stessa autorizzazione agli oggetti.
- **Liste di autorizzazioni:** è possibile raggruppare in una lista gli oggetti con simili esigenze di sicurezza. E' quindi possibile assegnare un'autorizzazione alla lista invece che ai singoli oggetti.
- **Proprietà dell'oggetto:** ogni oggetto presente nel sistema ha un proprietario. Gli oggetti possono appartenere ai profili di gruppo o ai singoli utenti. Una corretta assegnazione della proprietà dell'oggetto consente di (1) gestire le applicazioni e (2) delegare la responsabilità della sicurezza delle informazioni.
- **Gruppo principale:** è possibile specificare l'autorizzazione di gruppo principale per un oggetto. Il sistema memorizza l'autorizzazione di gruppo principale insieme all'oggetto. L'utilizzo dell'autorizzazione di gruppo principale può semplificare la gestione delle autorizzazioni e migliorare le prestazioni di controllo delle autorizzazioni.
- **Autorizzazione alla libreria:** è possibile inserire i file ed i programmi che richiedono protezione in una libreria e limitare l'accesso a tale libreria. Ciò risulta spesso più semplice che limitare l'accesso ad ogni singolo oggetto. Per proteggere gli oggetti più importanti, si potrebbe proteggere sia l'oggetto che la libreria.
- **Autorizzazione all'oggetto:** nel caso in cui l'accesso ad una libreria non sia abbastanza specifico, è possibile limitare l'autorizzazione ai singoli oggetti, ad esempio ai file.
- **Autorizzazione pubblica:** per ogni oggetto, è possibile definire il tipo di accesso disponibile per ogni utente del sistema che non abbia nessun'altra autorizzazione all'oggetto. L'autorizzazione pubblica è un efficace mezzo di protezione degli oggetti non riservati e garantisce buone prestazioni del sistema.
- **Autorizzazione all'indirizzario:** è possibile utilizzare l'autorizzazione all'indirizzario nello stesso modo in cui si utilizza l'autorizzazione alla libreria. E' possibile raggruppare gli oggetti in un indirizzario e proteggere l'indirizzario invece che i singoli oggetti.
- **Contenitore autorizzazioni:** quando si cancella un oggetto, si cancellano anche le informazioni relative all'autorizzazione per tale oggetto. I contenitori di autorizzazioni conservano le informazioni relative all'autorizzazione per i file definiti dal programma che vengono eliminati e creati di nuovo da un'applicazione. E' possibile utilizzare i contenitori di autorizzazioni come ausilio durante la migrazione dal System/36.

Strumenti di sicurezza

E' possibile utilizzare gli strumenti di sicurezza per gestire e monitorare l'ambiente della sicurezza nell'iSeries. E' inoltre possibile utilizzare gli strumenti del profilo utente per:

- Scoprire quali profili utente abbiano delle parole d'ordine predefinite.
- Pianificare che i profili utente non siano disponibili in certi momenti del giorno o della settimana.
- Pianificare che un profilo utente venga eliminato quando il dipendente lascia la società.
- Stabilire quali profili utente abbiano delle autorizzazioni speciali.
- Stabilire chi adotta l'autorizzazione agli oggetti presenti nel sistema.

E’ possibile utilizzare gli strumenti di sicurezza degli oggetti per tenere traccia delle autorizzazioni pubbliche e private associate ad oggetti riservati. E’ possibile stampare tali prospetti regolarmente (ad esempio, mensilmente) per riuscire a focalizzare l’impatto della sicurezza sulle questioni correnti. E’ possibile effettuare dei prospetti in modo da visualizzare solo le modifiche apportate dall’ultima volta in cui è stato effettuato il prospetto.

Altri strumenti forniscono la possibilità di monitorare:

- I programmi trigger
- I valori relativi alla sicurezza nelle voci di comunicazione, nelle descrizioni di sottosistema, nelle code di emissione, nelle code di lavori e nelle descrizioni lavoro.
- I programmi modificati o manomessi

Una volta compresa l’importanza della sicurezza del sistema, è possibile esaminare una descrizione del metodo di pianificazione che questo argomento utilizza come esempio.

Un metodo di pianificazione della sicurezza di base del sistema

Si consiglia di pianificare la sicurezza muovendosi dall’esterno all’interno e dal generale al particolare. Ad esempio, per pianificare i profili utente, è necessario prima di tutto considerare cosa vede l’utente (l’esterno). In seguito è necessario decidere in che modo realizzarlo (l’interno).

Si pianificano prima di tutto i valori di sistema ed i profili di gruppo (il generale) e poi si stabiliscono le eccezioni per i singoli utenti (il particolare).

Completare nell’ordine le attività di pianificazione presenti in ″Pianificare la sicurezza dell’utente″. Esse forniscono una progressione logica per la descrizione delle modalità di pianificazione dell’utilizzo del sistema e per stabilire le modalità di utilizzo del sistema ed i metodi per renderlo sicuro e personalizzarlo. All’interno di questi argomenti, utilizzare i fogli di lavoro di pianificazione per fornire una registrazione delle scelte di sicurezza e della loro implementazione. Verificare che questi fogli di pianificazione siano stati collocati in un posto sicuro. Le informazioni raccolte nei fogli di lavoro di pianificazione di ogni argomento consentiranno successivamente di impostare la sicurezza.

Nella pianificazione e nella progettazione della sicurezza del sistema, si procede dal basso verso l’alto. E’ necessario iniziare dalle forme di sicurezza di base per poi passare a forme di sicurezza più complesse. Iniziare dalla sicurezza fisica del sistema, per poi passare alla descrizione delle applicazioni dei valori di sistema. Infine, è necessario considerare la sicurezza degli utenti e degli oggetti presenti nel sistema.

In questi argomenti di pianificazione, è possibile trovare esempi in cui un’azienda tipo, l’Azienda di giocattoli JKL, utilizza questo approccio. Sebbene si tratti di un’azienda fittizia, l’azienda è un tipico esempio delle società del mondo reale. L’argomento ″Esempio: presentazione dell’Azienda di giocattoli JKL″ descrive quest’azienda di esempio.

Esempio: presentazione dell’Azienda di giocattoli JKL

Gli esempi facilitano la spiegazione e la comprensione dei vari argomenti. A tal fine, questi argomenti utilizzano come esempio l’Azienda di giocattoli JKL. L’Azienda di giocattoli JKL, una fabbrica di giocattoli di piccole dimensioni, ma in rapida crescita, desidera impostare la sicurezza su un sistema iSeries. Il presidente dell’azienda, John Smith, desidera che il nuovo sistema iSeries semplifichi l’onere della rapida crescita dell’Azienda di giocattoli JKL.

John ha assegnato a Sharon Jones, gestore account, la responsabilità di amministratore di sistema e responsabile della riservatezza. Il suo compito è quello di verificare che l’intera installazione, compresa la sicurezza, proceda senza problemi. Sharon è convinta dell’importanza della pianificazione. Attualmente l’azienda è di piccole dimensioni e la maggior parte dei dipendenti ha accesso alla maggior parte delle informazioni. Ma Sharon sa che tale situazione andrà modificandosi con l’espansione dell’azienda. Desidera che tutto si svolga secondo i piani fin dall’inizio.

Inizialmente, l'Azienda di giocattoli JKL ha in programma di eseguire queste applicazioni sul proprio sistema: Ordini cliente, Controllo inventario, Contratti e Tariffe e Crediti a breve termine. Leggendo gli argomenti relativi alla pianificazione, si avranno maggiori informazioni sulle modalità di gestione della sicurezza dell'Azienda di giocattoli JKL.

L'argomento ″Fasi del processo di pianificazione″ espone tutte le fasi da seguire durante la pianificazione della sicurezza del sistema.

Fasi del processo di pianificazione della sicurezza

La seguente tabella descrive ogni fase del processo di pianificazione ed il modo in cui le fasi sono correlate al resto del processo.

Tabella 2. Fasi del processo di pianificazione della sicurezza

Fase	Cosa fare in questa fase	Correlazione tra le fasi
Pianificare la sicurezza fisica	Descrivere in che modo si è pianificata la protezione dell'unità di sistema, dei dispositivi e dei supporti magnetici di riserva.	La maggior parte di queste informazioni sono indipendenti rispetto al resto del processo. Non immettere nel sistema le informazioni sulla pianificazione della sicurezza fisica; tuttavia, alcune di queste informazioni sono necessarie per pianificare i valori di sistema e la sicurezza delle risorse.
Pianificare l'applicazione	Descrivere le finalità, i menu principali e le librerie di tutte le applicazioni.	Fornisce la base per il resto del processo di pianificazione e per le altre scelte di sicurezza. Non immettere queste informazioni nel sistema.
Pianificare l'approccio globale	Decidere quale sarà l'approccio globale alla sicurezza. Scegliere i valori di sistema che supportano tale approccio.	Utilizzare le informazioni di pianificazione dell'applicazione per determinare l'approccio globale. I valori di sistema scelti influenzano le modalità di pianificazione ed i profili di gruppo.
Pianificare i gruppi di utenti	Decidere in che modo ripartire gli utenti nei gruppi. Decidere le caratteristiche di ogni gruppo e in che modo definirle nel sistema.	Utilizzare la descrizione dell'applicazione per determinare i gruppi nel sistema. I gruppi di utenti definiti influenzano le modalità di pianificazione dei singoli utenti nel sistema.
Pianificare i singoli profili utente	Assegnare ogni utente del sistema ad un gruppo. Definire ogni utente, includendo le caratteristiche che lo rendono diverso dal resto del gruppo. Ad esempio, gli utenti necessitano di un tipo di accesso ad un'applicazione o ad una libreria rispetto al resto del gruppo.	Utilizzare le informazioni sulla pianificazione dell'applicazione e sulla pianificazione dei gruppi di utenti per definire i singoli utenti.
Pianificare la sicurezza delle risorse	Decidere quali applicazioni rendere disponibili per tutti nel sistema. Se si ha l'esigenza di limitare alcune applicazioni, decidere quali utenti o gruppi saranno autorizzati ad utilizzarle.	Utilizzare le informazioni sulla pianificazione dell'applicazione e sulla pianificazione del profilo dei gruppi per pianificare la sicurezza delle risorse.

Tabella 2. Fasi del processo di pianificazione della sicurezza (Continua)

Fase	Cosa fare in questa fase	Correlazione tra le fasi
Pianificare l'installazione dell'applicazione	Decidere in che modo stabilire la proprietà e l'autorizzazione pubblica alle librerie dell'applicazione.	Utilizzare le informazioni sulla pianificazione della sicurezza delle risorse per pianificare l'installazione dell'applicazione.

Si consiglia di iniziare il processo di pianificazione della sicurezza pianificando la sicurezza dell'utente.

Capitolo 4. Pianificare la sicurezza dell'utente

La pianificazione della sicurezza dell'utente include la pianificazione di tutte le aree in cui la sicurezza influenza gli utenti collegati al sistema. E' essenziale la descrizione delle seguenti aree:

Sicurezza fisica
Per sicurezza fisica si intende la protezione dell'iSeries da furti e danni accidentali (o intenzionali). Inoltre include tutte le stazioni di lavoro, le stampanti ed i supporti magnetici di memorizzazione. ″Pianificare la sicurezza fisica″ contiene ulteriori informazioni sulla pianificazione della sicurezza fisica, sui rischi e sui suggerimenti dell'IBM.

Sicurezza dell'applicazione
La sicurezza dell'applicazione riguarda le applicazioni memorizzate nel sistema e le modalità di protezione delle stesse quando più utenti possono accedervi contemporaneamente. ″Pianificare la sicurezza delle applicazioni″ fornisce dettagli sulla descrizione delle applicazioni e sulle loro convenzioni di denominazione.

Strategia di sicurezza globale
La pianificazione della sicurezza include lo sviluppo di un programma di sicurezza che prenda in considerazione sia la situazione attuale che i programmi futuri dell'azienda. ″Pianificazione strategia di sicurezza globale″ fornisce ulteriori informazioni sulla determinazione delle normative di sicurezza, del livello di sicurezza, delle considerazioni sulla parola d'ordine e dei valori di sistema.

Sicurezza del gruppo di utenti
Un gruppo di utenti consiste in un insieme di utenti che ha necessità di utilizzare le stesse applicazioni nella stessa maniera. La pianificazione della sicurezza del gruppo di utenti comporta la determinazione dei gruppi di lavoro che pianificano l'utilizzo del sistema e delle esigenze dell'applicazione di quei gruppi. ″Pianificare i gruppi di utenti″ fornisce informazioni dettagliate sull'identificazione dei gruppi di utenti, la pianificazione dei profili di gruppo, la scelta dei valori di sistema e la determinazione dell'ambiente dell'utente.

Sicurezza del singolo utente
Dopo aver determinato i gruppi di utenti necessari, è possibile pianificare i singoli profili utente necessari. ″Pianificare i singoli profili utente″ fornisce ulteriori informazioni sulla denominazione degli utenti nel sistema, sulla determinazione delle responsabilità dei singoli utenti e sulla scelta dei valori di sistema.

Nei presenti argomenti di pianificazione si trovano collegamenti ai moduli di pianificazione che è possibile utilizzare per registrare le scelte di pianificazione.

Pianificare la sicurezza fisica

Quando si è pronti ad installare iSeries, è necessario creare un piano di sicurezza fisica in base alle seguenti domande:

- Dove verrà inserita l'unità di sistema?
- Dove verrà ubicata ciascuna stazione video?
- Dove verranno ubicate le stampanti?
- Di quali apparecchiature aggiuntive si necessita, ad esempio cablaggio, linee telefoniche, mobilia o aree di magazzino?
- Quali misure verranno prese per proteggere il sistema da emergenze come incendi o interruzioni di energia elettrica?

La sicurezza fisica deve far parte della pianificazione globale della sicurezza. Potrebbero essere necessarie delle misure specifiche di protezione a seconda del punto in cui vengono inseriti il sistema e le sue unità.

E’ possibile utilizzare il modulo Pianificazione sicurezza fisica per registrare le scelte circa la sicurezza fisica del sistema. Per essere sicuri di aver contemplato tutti gli aspetti della sicurezza fisica, esaminare questi argomenti:

- Sicurezza fisica per l’unità di sistema fornisce dettagli sulla protezione del sistema stesso.
- Sicurezza fisica per la documentazione del sistema e per i supporti magnetici di memorizzazione contiene informazioni sulla protezione dei documenti del sistema e dei supporti magnetici di memorizzazione.
- Sicurezza fisica per le stazioni di lavoro espone le modalità di protezione delle stazioni di lavoro.
- Sicurezza fisica per le stampanti e per l’emissione di stampa fornisce dettagli sulla protezione fisica delle stampanti e delle loro emissioni.
- Pianificare la normativa di sicurezza spiega in che modo preparare delle istruzioni per gli utenti ed una normativa di sicurezza.

Ogni unità di sistema ha un pannello di controllo per assistenza alla macchina e per l’esecuzione di specifiche operazioni di sistema, come ad esempio attivare e disattivare il sistema. Per evitare un utilizzo non autorizzato di queste operazioni di sistema, ogni unità di sistema è dotata di un interruttore con chiave di blocco o di una chiave elettronica. Essi forniscono un certo grado di protezione all’unità di sistema, ma l’interruttore con chiave di blocco o la chiave elettronica non possono sostituirsi ad un’adeguata sicurezza fisica.

Sicurezza fisica per l’unità di sistema

L’iSeries non richiede uno spazio per il computer con specifici controlli ambientali. Spesso l’unità di sistema è collocata in una zona dell’ufficio alla quale hanno accesso molte persone. I clienti apprezzano le dimensioni ridotte e la facilità di manutenzione dell’iSeries; tali caratteristiche, tuttavia, potrebbero anche costituire dei rischi per la sicurezza. Ad esempio, chiunque potrebbe facilmente sottrarre l’unità di sistema o eliminare i suoi componenti più importanti.

Si consiglia di assicurarsi che l’unità di sistema venga collocata in un luogo sicuro. La migliore ubicazione è in una stanza riservata e chiusa a chiave. Al limite, si consiglia di collocare l’unità di sistema in un luogo chiuso nelle ore non lavorative.

Rischi per l’unità di sistema

Oltre al furto dell’unità di sistema o dei suoi componenti, qui di seguito sono riportati alcuni altri rischi causati da un’inadeguata sicurezza fisica dell’unità di sistema:

Distruzione accidentale delle operazioni di sistema
Molti problemi di sicurezza derivano da utenti del sistema autorizzati. Supponiamo che una delle stazioni video del sistema si blocchi. L’operatore di sistema è ad un meeting fuori sede. L’utente della stazione video si dirige all’unità di sistema pensando che, ″Forse spingendo questo pulsante, la situazione si sistemerà.″ Quel pulsante potrebbe disattivare o ricaricare il sistema mentre sono in esecuzione dei lavori. Potrebbero essere necessarie diverse ore per recuperare parzialmente i file aggiornati. E’ possibile utilizzare l’interruttore con chiave di blocco dell’unità di sistema per evitare che ciò si verifichi.

Utilizzo della funzione dei DST (dedicated service tools) per eludere la sicurezza
La sicurezza non controlla le funzioni di manutenzione effettuate dal sistema, dal momento che il software del sistema potrebbe non funzionare correttamente quando è necessario eseguire queste funzioni. Una persona ben informata che conosca o indovini l’ID utente e la parola d’ordine degli strumenti di manutenzione potrebbe provocare seri danni al sistema. Per documentarsi meglio circa gli strumenti di manutenzione, consultare l’argomento Strumenti di manutenzione nell’Information Center.

Suggerimenti

- La soluzione ideale sarebbe quella di collocare l'unità di sistema in una stanza chiusa a chiave. Se ciò non è possibile, collocare l'unità in un luogo al quale non possano accedere persone esterne. Scegliere inoltre un'ubicazione in cui i dipendenti addetti possano monitorarla. Le seguenti caratteristiche di sicurezza fisica possono risultare utili per proteggere il sistema da manomissioni accidentali o intenzionali:
- Utilizzare la chiave elettronica o di blocco:
  - Impostare la modalità di funzionamento su Normal se si desidera avviare il sistema senza utilizzare la chiave.
  - Impostare la modalità di funzionamento su Auto se si ha intenzione di utilizzare la funzione automatica di avvio e disattivazione per avviare ed arrestare il sistema.
  - Rimuovere la chiave e collocarla in un posto sicuro.
- Modificare l'ID utente e la parola d'ordine dei DST (Service Tools) subito dopo aver installato il sistema e dopo che il personale addetto alla manutenzione lo abbia utilizzato. L'argomento Strumenti di manutenzione nell'Information Center spiega in maniera più dettagliata come effettuare tale operazione.

E' possibile consultare un esempio di piano dell'Azienda di giocattoli JKL per la sicurezza dell'unità, prima di pianificare la sicurezza fisica per la documentazione del sistema e per i supporti magnetici di memorizzazione.

Esempio: modulo Pianificazione sicurezza fisica dell'Azienda di giocattoli JKL—parte relativa all'unità di sistema

Segue un esempio della parte dell'unità di sistema del modulo Pianificazione sicurezza fisica utilizzato da Sharon Jones per il suo sistema:

Tabella 3. Modulo Pianificazione sicurezza fisica dell'Azienda di giocattoli JKL: esempio di unità di sistema

Modulo Pianificazione sicurezza fisica	
Preparato da: Sharon Jones	Data: 9/2/99
Unità di sistema:	
Descrivere le misure di sicurezza per proteggere l'unità di sistema (ad esempio, una stanza chiusa a chiave):	L'unità di sistema si trova nell'ufficio contabile. Durante il giorno, i dipendenti si trovano sempre nell'ufficio contabile e possono controllare l'unità di sistema. Essi sono anche responsabili sia delle registrazioni minime che di quelle importanti. Al di fuori delle ore lavorative regolari, l'area è bloccata.
Quale posizione della chiave di blocco viene utilizzata generalmente?	Normal
Dove si trova la chiave?	In una piccola cassaforte nell'ufficio di Sharon.
Altri commenti relativi all'unità di sistema:	L'unità di sistema sarà facilmente accessibile. Informare i dipendenti che si trovano nell'ufficio contabile di accertarsi che nessuno manometta l'area.

Dopo aver pianificato la sicurezza fisica dell'unità di sistema, è possibile pianificare la sicurezza fisica per la documentazione di sistema e per i supporti magnetici di memorizzazione.

Sicurezza fisica per la documentazione del sistema e per i supporti magnetici di memorizzazione

Un altro aspetto del piano di sicurezza fisica riguarda la memorizzazione di documentazione importante del sistema e di supporti magnetici di memorizzazione. La documentazione del sistema include informazioni che la IBM consegna insieme al sistema, alle informazioni sulla parola d'ordine, ai moduli per la pianificazione e a tutta la documentazione prodotta dal sistema.

A seconda del sistema, i supporti magnetici di riserva possono includere nastri, CD-ROM, dischetti o DVD. Si consiglia di conservare sia la documentazione del sistema che i supporti magnetici di riserva in azienda oltre che in un'altra postazione remota. In caso di problemi gravi, per ripristinare il sistema, sarà necessario utilizzare tali informazioni. Le seguenti informazioni suggeriscono delle modalità di memorizzazione della documentazione del sistema e dei supporti magnetici. Dopo aver scelto la modalità, registrare tali scelte nella sezione Documentazione e supporti magnetici di riserva del modulo Pianificazione sicurezza fisica.

Conservare la documentazione di sistema in modo sicuro

Le parole d'ordine degli strumenti di manutenzione e dei responsabili della riservatezza sono fondamentali per il funzionamento del sistema. Si consiglia di trascrivere queste parole d'ordine e di conservarle in un posto sicuro e riservato. Conservare inoltre una copia di queste parole d'ordine in un'ubicazione fuori sede così da poterle recuperare in caso di problemi gravi.

Conservare altra documentazione importante per il sistema, come le impostazioni di configurazione e le librerie delle principali applicazioni, in un luogo diverso dall'azienda, per poterla recuperare in caso di problemi gravi.

Conservare i supporti magnetici di memorizzazione in modo sicuro

Durante l'installazione del sistema, pianificare delle operazioni di salvataggio a cadenza regolare di tutte le informazioni presenti nel sistema su nastro o su altri supporti magnetici di memorizzazione. Queste copie di riserva consentono, se necessario, di ripristinare il sistema. Si consiglia inoltre di conservare tali copie di riserva in un posto sicuro fuori sede.

Rischi

- Danni ai supporti magnetici di riserva: se i supporti magnetici di riserva del sistema sono stati distrutti calamità o atti vandalici, potrebbe non essere possibile recuperare le informazioni che erano presenti nel sistema, eccezion fatta per la documentazione cartacea.
- Furto dei supporti magnetici di riserva o delle parole d'ordine: le informazioni aziendali riservate potrebbero essere state salvate su supporti magnetici di riserva. Una persona competente potrebbe riuscire a recuperare tali informazioni su un altro computer e stamparle o elaborarle.

Suggerimenti

- Conservare tutte le parole d'ordine ed i supporti magnetici di riserva in un armadietto chiuso a chiave e ignifugo.
- Portare le copie dei supporti magnetici di riserva in un luogo sicuro e fuori sede a cadenze regolari, ad esempio almeno ogni settimana.

E' possibile esaminare un esempio del programma dell'Azienda di giocattoli JKL per la memorizzazione della documentazione del sistema prima di pianificare la sicurezza fisica per le stazioni di lavoro.

Esempio: modulo Pianificazione sicurezza fisica dell'Azienda di giocattoli JKL —Parte relativa al supporto magnetico di riserva e alla documentazione

Sharon Jones dell'Azienda di giocattoli JKL ha completato la sezione relativa al supporto magnetico di riserva e alla documentazione del modulo Pianificazione sicurezza fisica come mostrato nella tabella seguente:

Tabella 4. Modulo Pianificazione sicurezza fisica dell'Azienda di giocattoli JKL: esempio di supporto magnetico di riserva e della documentazione

Modulo Pianificazione sicurezza fisica	
Preparato da: Sharon Jones	Data: 9/2/99
Supporto magnetico di riserva e documentazione:	

Tabella 4. Modulo Pianificazione sicurezza fisica dell'Azienda di giocattoli JKL: esempio di supporto magnetico di riserva e della documentazione (Continua)

Dove si trovano i nastri di riserva memorizzati nella propria azienda?	In un'ampia cassaforte ignifuga.
Dove si trovano i nastri di riserva conservati all'esterno della sede aziendale?	In una cassaforte ignifuga nell'ufficio contabile dell'azienda.
Dove vengono conservate le parole d'ordine del responsabile della riservatezza, del servizio e DST?	Con una combinazione sicura nell'ufficio di John Smith.
Dove si trova la documentazione importante di sistema, ad esempio il numero di serie e la configurazione?	In un'ampia cassaforte, fuori sede e nell'ufficio contabile.

Dopo aver pianificato la sicurezza della documentazione e della relativa archiviazione, è possibile pianificare la sicurezza fisica per le stazioni di lavoro.

Pianificare la sicurezza fisica per le stazioni di lavoro

Nella maggior parte dei casi, si desidera che tutti gli utenti riescano a collegarsi a qualunque stazione di lavoro disponibile e possano effettuare tutte le funzioni autorizzate. Tuttavia, se ci sono delle stazioni di lavoro pubbliche o private, sarà necessario adottare precauzioni particolari. Ad esempio, stazioni video che possono memorizzare delle sequenze tasti e i personal computer richiedono trattamenti particolari. Utilizzare quanto detto per completare la Parte 2 (Sicurezza fisica delle stazioni di lavoro e delle stampanti) del modulo Pianificazione sicurezza fisica.

Rischi associati alle stazioni di lavoro

Utilizzo di una stazione di lavoro in una postazione pubblica per scopi non autorizzati
Se delle persone esterne all'azienda potessero accedere alle postazioni con facilità, potrebbero potenzialmente consultare delle informazioni riservate. Se un utente del sistema lascia collegata una stazione di lavoro, qualcuno esterno all'azienda potrebbe riuscire ad entrare e ad accedere ad informazioni riservate.

Utilizzo di una stazione di lavoro in una postazione privata per scopi non autorizzati
Una stazione di lavoro ubicata in una postazione privata intralcerebbe il lavoro di un intruso costringendolo ad impiegare parecchie ore nel tentativo di eludere la sicurezza senza essere notato.

Utilizzo della funzione di riproduzione o di un programma di collegamento al PC su una stazione video per eludere le misure di sicurezza
Molte stazioni video hanno una funzione di registrazione e di riproduzione che consente agli utenti di memorizzare le sequenze tasti più utilizzate e di ripeterle premendo un solo tasto. Quando si utilizza un personal computer come stazione di lavoro nel sistema iSeries, è possibile creare un programma per automatizzare il processo di collegamento. Dal momento che gli utenti utilizzano spesso il processo di collegamento, potrebbero decidere di memorizzare i propri ID utente e le proprie parole d'ordine invece di immetterli tutte le volte che si collegano.

Suggerimenti

Tenere a mente questi suggerimenti durante l'impostazione della sicurezza fisica per le stazioni di lavoro:

- Se possibile, evitare di collocare le stazioni di lavoro in postazioni troppo pubbliche o troppo private.
- Far presente agli utenti del sistema l'importanza di scollegarsi prima di lasciare una stazione di lavoro. Si consiglia di includere le procedure di scollegamento nella normativa di sicurezza.
- Far presente che la registrazione di una parola d'ordine in una stazione video o in un programma del PC viola la sicurezza del sistema. Si consiglia di includere le procedure di registrazione della parola d'ordine nella normativa di sicurezza.

- Prendere provvedimenti utilizzando i valori di sistema del temporizzatore di inattività (QINACTITV e QINACTMSGQ), per evitare che l'utente lasci le stazioni di lavoro in ubicazioni pubbliche senza essersi scollegato dal sistema.
- Limitare le funzioni che gli utenti possono effettuare su stazioni di lavoro pubbliche autorizzando solo gli utenti con autorizzazione limitata ad accedere a tali stazioni di lavoro.
- Evitare che utenti autorizzati alla manutenzione ed alla sicurezza si colleghino a stazioni di lavoro private. Utilizzare il valore di sistema QLMTSECOFR per controllare il posto in cui un utente si collega con queste autorizzazioni.
- Evitare che gli utenti si colleghino contemporaneamente su più di una stazione di lavoro. E' possibile utilizzare il valore di sistema che limita le sessioni di unità (QLMTDEVSSN) per controllare il posto in cui gli utenti si collegano.

Per attuare questi suggerimenti, consultare gli argomenti ″Scegliere i valori di sistema che influenzano il collegamento″ e ″Pianificare la sicurezza delle risorse per le stazioni di lavoro″ per maggiori dettagli.

Per il modulo Pianificazione sicurezza fisica, è necessario identificare quali stazioni di lavoro possano costituire un rischio a causa della loro ubicazione fisica. E' possibile visionare l'esempio relativo a come Sharon Jones ha pianificato la sicurezza fisica delle stazioni di lavoro dell'Azienda di giocattoli JKL.

Dopo aver pianificato la sicurezza della stazione di lavoro, è possibile pianificare la sicurezza fisica per le stampanti e l'emissione di stampa.

Sicurezza fisica per le stampanti e per l'emissione di stampa

Una volta che si è avviata la stampa delle informazioni, la sicurezza del sistema non è in grado di controllare chi le stia vedendo. Per ridurre il rischio che qualcuno possa vedere delle informazioni importanti per l'azienda, si consiglia di proteggere le stampanti e l'emissione di stampa. Si consiglia inoltre di creare una normativa relativa alla stampa delle informazioni aziendali riservate.

Rischi associati alle stampanti e all'emissione di stampa

La propria azienda potrebbe correre i seguenti rischi. Questi sono i più comuni rischi di sicurezza associati alla stampante e all'emissione di stampa. Tuttavia, si consiglia di esaminare gli altri rischi che possono verificarsi nella situazione aziendale specifica.

- Una stampante ubicata in un luogo pubblico potrebbe far accedere persone non autorizzate ad informazioni riservate.
- L'emissione di stampa lasciata su una scrivania potrebbe rivelare delle informazioni.
- Il sistema potrebbe essere dotato soltanto di una o due stampanti. Potrebbe essere necessario stampare informazioni importanti o riservate, ad esempio assegni paga, che i dipendenti dell'azienda potrebbero vedere.

Suggerimenti

I seguenti suggerimenti possono risultare utili per la riduzione dei rischi di sicurezza associati alle stampanti ed alla loro emissione.

- Far presente agli utenti del sistema l'importanza della protezione dell'emissione di stampa riservata. Includere le scelte di sicurezza fisica relative alle stampanti nella normativa di sicurezza.
- Evitare di collocare le stampanti in luoghi pubblici.
- Pianificare la stampa di un'emissione molto riservata ed affidare ad una persona autorizzata l'incarico di rimanere accanto alla stampante durante l'operazione di stampa.

″Pianificare la sicurezza per le stampanti e per l'emissione di stampa″ propone dei suggerimenti utili alla gestione di un'emissione di stampa riservata.

E’ possibile consultare un esempio di piano dell’Azienda di giocattoli JKL per la sicurezza della stampante prima di iniziare a pianificare la normativa di sicurezza.

Esempio: modulo Pianificazione sicurezza fisica dell’Azienda di giocattoli JKL—parte relativa alla stazione di lavoro e alla stampante

Segue un esempio della Parte 2 del Piano di Sicurezza fisica che Sharon Jones ha utilizzato per l’Azienda di giocattoli JKL:

Tabella 5. Modulo Pianificazione sicurezza fisica dell’Azienda di giocattoli JKL: esempio relativo alla stazione di lavoro e alla stampante

Modulo Pianificazione sicurezza fisica			Parte 2 di 2
Sicurezza fisica delle stazioni di lavoro e delle stampanti			
Nome stazione di lavoro o stampante	Relativa ubicazione o descrizione	Rischi per la sicurezza	Misure di sicurezza da adottare
DSP06	Piattaforme di carico	Troppo pubblico	Scollegamento automatico. Limitare le funzioni che possono essere completate sulla stazione di lavoro.
DSP09	Servizio clienti	Troppo pubblico	Scollegamento automatico. Limitare le funzioni che possono essere completate sulla stazione di lavoro.
RMT12	Ufficio vendite distaccato	Troppo privato	Non consentire al responsabile della riservatezza di effettuare il collegamento su quella macchina.
PRT02	Contabilità, vicino all'unità di sistema	E' possibile visualizzare informazioni sensibili, ad esempio le liste delle tariffe	Assegnare il compito a qualcuno di monitorare l'emissione di stampa

Dopo aver completato il Modulo Pianificazione sicurezza fisica, continuare con l’argomento ″Pianificare la normativa di sicurezza″.

Pianificare la normativa di sicurezza

Potrebbe risultare utile fornire delle istruzioni di sicurezza a tutti i dipendenti per sottolineare le normative di sicurezza relative alla sicurezza fisica e del sistema. E’ possibile fornire le stesse istruzioni ai nuovi utenti che si aggiungono successivamente al sistema.

In queste istruzioni, è necessario includere alcune informazioni generali sulle modalità di protezione della sicurezza del sistema, come ad esempio scollegare le stazioni di lavoro e non condividere le parole d’ordine. E’ necessario che le istruzioni includano anche delle informazioni sulle specifiche scelte di sicurezza effettuate.

Nel leggere queste informazioni sulla pianificazione, prendere nota di tutto ciò che le istruzioni di sicurezza devono contenere. Si consiglia inoltre di prendere nota delle informazioni utili per la normativa di sicurezza.

Ad esempio, Sharon Jones dell’Azienda di giocattoli JKL ha preso nota delle seguenti istruzioni di sicurezza, durante la pianificazione della sicurezza fisica per il sistema:

```
Sottolineare l'importanza dell'operazione di scollegamento per la piattaforma di carico, il servizio
clienti e l'ufficio vendite distaccato. Il personale dell'ufficio contabile vigilerà
sull'unità di sistema.
```

Dopo aver completato il modulo Pianificazione sicurezza fisica, si è pronti a pianificare la sicurezza per le applicazioni.

Pianificare la sicurezza delle applicazioni

Per pianificare la sicurezza più adatta per le applicazioni, è necessario conoscere:

- Quali informazioni si ha intenzione di memorizzare nel sistema?
- Chi deve avere accesso a quelle informazioni?
- Che tipo di accesso è necessario? E' necessario modificare le informazioni o solo visionarle?

Man mano che si consultano gli argomenti di pianificazione dell'applicazione, si troverà la risposta alla prima domanda relativa a quali informazioni si ha intenzione di memorizzare nel sistema. Negli argomenti successivi, si decide chi necessita di quelle informazioni e il tipo di accesso necessario. Non immettere le informazioni per la pianificazione dell'applicazione nel sistema; tuttavia, saranno necessarie durante l'impostazione della sicurezza degli utenti e delle risorse.

Cos'è un'applicazione?

Nella prima fase di pianificazione della sicurezza delle applicazioni, è necessario descrivere le applicazioni che si ha intenzione di eseguire sul sistema. Un'applicazione consiste in un gruppo di funzioni tra loro correlate secondo logica. Ad esempio, nell'Azienda di giocattoli JKL, l'immissione degli ordini, l'invio degli ordini e la stampa delle fatture fanno tutti parte di un'applicazione denominata Elaborazione ordini.

Generalmente, sull'iSeries è possibile eseguire due diversi tipi di applicazioni:

- **Applicazioni aziendali**: applicazioni che si acquistano o sviluppano per effettuare le specifiche funzioni aziendali, come ad esempio l'elaborazione degli ordini o la gestione dell'inventario.
- **Applicazioni specifiche**: applicazioni che si utilizzano in tutta l'azienda per effettuare una serie di attività che non siano specifiche di un processo aziendale.

Quali moduli sono necessari?

Utilizzare i seguenti moduli per pianificare la sicurezza delle applicazioni:

- Modulo Descrizione dell'applicazione
- Modulo Descrizione della libreria
- Modulo Convenzioni di denominazione

Per stampare tali moduli, fare clic sul collegamento, selezionare il frame sulla destra, quindi fare clic sull'icona **Stampa** nel browser.

Leggere le seguenti informazioni per completare questi moduli di pianificazione.

- Descrivere le applicazioni
- Descrivere le convenzioni di denominazione
- Descrivere le informazioni sulla libreria
- Tracciare il diagramma dell'applicazione

Descrivere le applicazioni

A questo punto, è necessario raccogliere alcune informazioni generali su ciascuna delle applicazioni aziendali. Aggiungere le informazioni relative all'applicazione nei campi adeguati nel modulo Descrizione

dell'applicazione come descritto qui di seguito. Successivamente è possibile utilizzare queste informazioni per pianificare la sicurezza dei gruppi di utenti e delle applicazioni:

Nome e abbreviazione dell'applicazione
Assegnare all'applicazione un nome breve ed un'abbreviazione che è possibile utilizzare in forma stenografica nei moduli e per la denominazione degli oggetti utilizzati dall'applicazione.

Informazioni descrittive
Descrivere brevemente le funzioni dell'applicazione.

Menu principale e libreria
Determinare quale sia il menu principale per accedere all'applicazione. Indicare la libreria in cui si trova il menu. Generalmente il menu principale rimanda ad altri menu con funzioni dell'applicazione specifiche. Gli utenti preferiscono consultare il menu principale dell'applicazione principale subito dopo essersi collegati al sistema.

Programma iniziale e libreria
Talvolta le applicazioni eseguono un programma iniziale che configura le informazioni di background per l'utente o esegue una verifica di sicurezza. Se un'applicazione ha un programma iniziale o un programma di configurazione, elencarlo nel modulo.

Librerie dell'applicazione
In genere, ogni applicazione ha una libreria principale per i propri file. Includere tutte le librerie utilizzate dall'applicazione, comprese le librerie di programma e le librerie che appartengono ad altre applicazioni. Ad esempio, l'applicazione Ordini cliente dell'Azienda di giocattoli JKL utilizza la libreria dell'inventario per le descrizioni ed il saldo delle voci.

E' possibile utilizzare la relazione tra le librerie e le applicazioni per determinare chi ha necessità di accedere ad ogni libreria.

Reperimento delle informazioni sulle applicazioni

Se non si conoscono già le informazioni necessarie per le applicazioni, è necessario contattare il programmatore o il fornitore dell'applicazione.

Qui di seguito sono riportati i metodi per poter reperire da sé le informazioni, se non si ha accesso a queste informazioni su un'applicazione in esecuzione sul sistema.

- E' possibile che gli utenti dell'applicazione riferiscano il nome del menu principale e della libreria o è possibile osservarli mentre si collegano al sistema.
- Se gli utenti consultano l'applicazione subito dopo essersi collegati, cercare il campo **Programma iniziale** nei profili utente. Questo campo contiene il programma iniziale per l'applicazione. E' possibile utilizzare il comando DSPUSRPRF per visualizzare il programma iniziale.
- E' possibile elencare i nomi e le descrizioni di tutte le librerie presenti nel sistema. Utilizzare DSPOBJD *ALL *LIB. In questo modo vengono visualizzate tutte le librerie presenti nel sistema.
- E' possibile osservare i lavori attivi mentre gli utenti stanno eseguendo l'applicazione. Utilizzare il comando Gestione lavori attivi (WRKACTJOB) con un livello di assistenza intermedio per avere informazioni dettagliate sui lavori interattivi. Visualizzare i lavori e consultare le liste librerie ed i rispettivi blocchi degli oggetti per vedere quali librerie sono in uso.
- E' possibile visualizzare i lavori batch di un'applicazione utilizzando il comando Gestione lavori utente (WRKUSRJOB).

Per verificare che si siano raccolte tutte le informazioni necessarie per pianificare la sicurezza delle applicazioni, è necessario completare le seguenti attività prima di procedere:

- Completare un modulo Descrizione dell'applicazione per ognuna delle applicazioni aziendali. Riempire l'intero modulo, eccetto la sezione dei requisiti di sicurezza. Questa sezione verrà utilizzata per pianificare la sicurezza delle risorse per l'applicazione come descritto nell'argomento ″Pianificare la sicurezza delle risorse″.

- Preparare un modulo Descrizione dell'applicazione per ogni applicazione speciale, se applicabile. L'utilizzo del modulo consente di determinare in che modo fornire accesso all'applicazione.

Nota: la preparazione dei moduli Descrizione dell'applicazione per applicazioni speciali dell'IBM, ad esempio IBM Query per iSeries è facoltativa. L'accesso alle librerie utilizzate da queste applicazioni non richiede alcuna pianificazione speciale. Tuttavia potrebbe risultare utile raccogliere le informazioni e preparare i moduli.

E' possibile consultare un esempio di modulo Descrizione dell'applicazione dell'Azienda di giocattoli JKL prima di passare alla descrizione delle convenzioni di denominazione.

Esempio: modulo Descrizione dell'applicazione dell'Azienda di giocattoli JKL

Sharon Jones ha elencato tutte le applicazioni dell'azienda con le relative abbreviazioni nel suo modulo Descrizione dell'applicazione. Ha inoltre descritto brevemente il modo in cui gli utenti gestiscono queste applicazioni.

Ordini cliente (CO)
Immettere, tenere traccia e inviare gli ordini. Stampare le fatture.

Controllo inventario (IC)
Gestisce i livelli di inventario per i prodotti e i materiali finiti. Elabora tutta la transizione dell'inventario.

Contratti e tariffe (CP)
Gestisce contratti e tariffe speciali con i clienti.

Crediti a breve termine (AC)
Tiene traccia dei bilanci correnti. Stampa mensilmente le istruzioni.

La tabella riportata di seguito contiene la descrizione dell'applicazione Ordini cliente di Sharon Jones. Ha preparato i suoi moduli in maniera sistematica, cominciando con un'applicazione e descrivendo il resto.

Tabella 6. Modulo Descrizione dell'applicazione dell'Azienda di giocattoli JKL: esempio

Modulo Descrizione dell'applicazione	
Preparato da: `Sharon Jones`	Data: `9/3/99`
Nome applicazione: `Ordini cliente`	Abbreviazione: `CO`
Breve descrizione dell'applicazione:	`Immettere gli ordini del cliente, tenerne traccia prima di inviarli, inviare l'ordine, stampare le fatture e inviarle.`
Nome del menu principale: `COMAIN`	Libreria: `COPGMLIB`
Nome programma iniziale: `NA`	Libreria: `NA`
Elencare le librerie utilizzate dall'applicazione per i file e i programmi: • `CUSTLIB` • `ITEMLIB` • `CONTRACTS` • `COPGMLIB`	
Definire gli obiettivi della sicurezza per l'applicazione, ad esempio se alcune informazioni sono riservate:	

Oltre all'applicazione Ordini cliente, Sharon Jones ha preparato anche i moduli Descrizione dell'applicazione per queste applicazioni sul sistema dell'Azienda di giocattoli JKL:

- Controllo inventario
- Contratti e tariffe
- Crediti a breve termine

In seguito, è possibile descrivere le convenzioni di denominazione per gli oggetti sul proprio sistema.

Descrivere le convenzioni di denominazione

Quando si conosce il modo in cui il sistema denomina gli oggetti, è possibile pianificare e monitorare la sicurezza, risolvere i problemi e pianificare l'esecuzione della copia di riserva e del ripristino. La maggior parte delle applicazioni hanno delle regole in base alle quali assegnano dei nomi agli oggetti, ad esempio alle librerie, ai file ed ai programmi. Se le applicazioni provengono da origini diverse, ognuna di loro avrà probabilmente il proprio sistema di denominazione univoco.

Verificare che vengano registrate tutte le convenzioni di denominazione delle applicazioni e degli oggetti nel modulo Convenzioni di denominazione. Nel modulo Convenzioni di denominazione, elencare le regole utilizzate dalle applicazioni per la denominazione delle librerie e dei file. E' possibile utilizzare le righe vuote per altre convenzioni di denominazione, ad esempio programmi e menu. Se le applicazioni provengono da origini diverse, ognuna di loro avrà probabilmente delle convenzioni di denominazione univoche. Descrivere le convenzioni di denominazione per ogni applicazione. Potrebbe essere necessario preparare più di un modulo Convenzioni di denominazione.

E' possibile consultare un esempio del modo in cui Sharon ha utilizzato le convenzioni di denominazione degli oggetti presenti nel sistema dell'Azienda di giocattoli JKL prima di passare alla descrizione delle informazioni sulla libreria.

Esempio: modulo Convenzioni di denominazione dell'Azienda di giocattoli JKL

La tabella riportata di seguito mostra solo le convenzioni di denominazione per le librerie e per i file. Sarà necessario anche descrivere le convenzioni di denominazione per altri tipi di oggetti sul proprio sistema. Il modulo Convenzioni di denominazione contiene diversi oggetti comuni; tuttavia, potrebbe essere necessario prepararne altri.

Tabella 7. Modulo Convenzioni di denominazione dell'Azienda di giocattoli JKL: esempio

Modulo Convenzioni di denominazione	
Preparato da: Sharon Jones	Data: 9/3/99
Tipo di oggetto	**Convenzione di denominazione**
Librerie	Le librerie che contengono i file hanno nomi significativi, come CONTRACTS o ITEMLIB. Le librerie del programma utilizzano l'abbreviazione dell'applicazione seguite da PGMLIB, ad esempio ICPGMLIB.
File	I file principali hanno nomi significativi, ad esempio CUSTMAST per il file Cliente principale o ITEMMAST per il file Voce principale. Altri file dell'applicazione (utilizzati solo per conoscenze da parte dei programmatori) vengono definiti con l'abbreviazione dell'applicazione seguita da FILE e un numero, ad esempio ICFILE14.

Dopo aver completato il modulo Convenzioni di denominazione, è possibile cominciare con la descrizione delle informazioni sulla libreria.

Descrivere le informazioni sulla libreria

Dopo aver descritto le convenzioni di denominazione, è necessario descrivere le librerie presenti nel sistema. Le librerie identificano ed organizzano gli oggetti presenti nel sistema. La collocazione di file simili in un'unica libreria consente agli utenti di accedere facilmente alle applicazioni e ai file più importanti. E' inoltre possibile personalizzare le autorizzazioni degli utenti, cosicché essi possano accedere soltanto ad alcune librerie. Descrivere tutte le librerie presenti nel sistema per ogni applicazione. Potrebbe essere necessario preparare più di un Modulo Descrizione della libreria

Nota: inserire soltanto le informazioni descrittive relative alla libreria. Durante la pianificazione della sicurezza delle risorse della libreria verrà compilata la restante parte del modulo Descrizione della libreria. In seguito sarà necessario aggiungere informazioni sulle autorizzazioni alle librerie. Per

maggiori dettagli sul completamento della restante parte del modulo Descrizione della libreria, consultare ″Pianificare la sicurezza per le librerie dell'applicazione″.

Prima di procedere, verificare di aver completato le seguenti operazioni:

- Inserire le parti relative alla libreria ed al file del modulo Convenzioni di denominazione.
- Inserire le informazioni descrittive nel modulo Descrizione della libreria per ogni libreria dell'applicazione.

E' possibile consultare un esempio del modo in cui Sharon Jones dell'Azienda di giocattoli JKL abbia descritto le librerie, prima di tracciare un diagramma dell'applicazione.

Esempio: modulo Descrizione della libreria dell'Azienda di giocattoli JKL

Le due tabelle riportate di seguito descrivono due librerie che l'applicazione Ordini cliente utilizza nell'Azienda di giocattoli JKL. La prima tabella descrive una libreria che contiene i file e la seconda descrive una libreria che contiene i programmi.

Tabella 8. Modulo Descrizione della libreria dell'Azienda di giocattoli JKL: esempio Libreria che contiene i file

Modulo Descrizione della libreria	
Preparato da: Sharon Jones	Data: 9/3/99
Nome libreria: CUSTLIB	Nome descrittivo (testo): Libreria record cliente
Descrivere brevemente la funzione di questa libreria:	Conserva tutti i file del cliente, inclusi gli ordini e i crediti a breve termine.

Tabella 9. Modulo Descrizione della libreria dell'Azienda di giocattoli JKL: esempio Libreria che contiene i programmi

Modulo Descrizione della libreria	
Preparato da: Sharon Jones	Data: 9/3/99
Nome libreria: COPGMLIB	Nome descrittivo (testo): Libreria di programma Ordini cliente
Descrivere brevemente la funzione di questa libreria:	Conserva tutti i programmi per l'applicazione dell'ordine cliente.

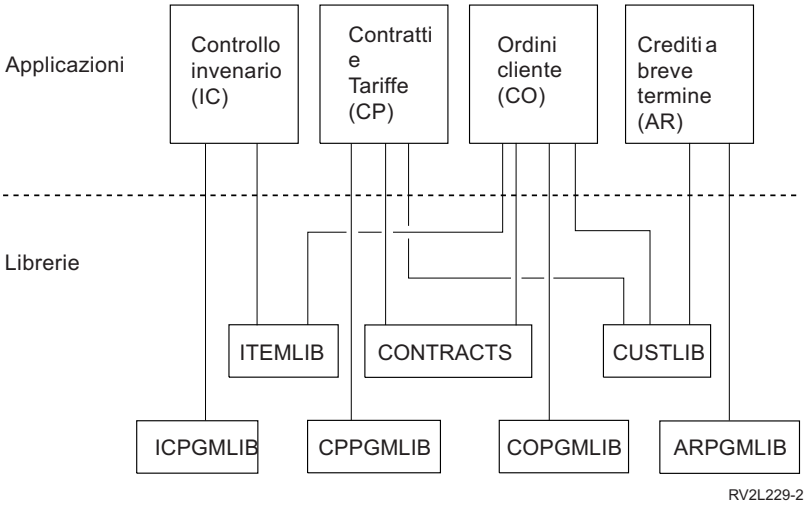
Dopo aver descritto le librerie, è necessario tracciare un diagramma dell'applicazione per il proprio sistema.

Tracciare il diagramma dell'applicazione

Durante la preparazione dei moduli Descrizione dell'applicazione e Descrizione della libreria, potrebbe risultare utile tracciare un diagramma che mostri la relazione tra le applicazioni e le librerie. Il diagramma consentirà di pianificare la sicurezza sia dei gruppi di utenti che delle risorse.

La figura sottostante mostra il diagramma delle applicazioni e delle librerie dell'Azienda di giocattoli JKL disegnato da Sharon Jones:

Diagramma delle applicazioni e delle librerie dell'Azienda di giocattoli JKL



La raccolta di alcune informazioni relative alle applicazioni ed alle librerie risulterà ora utile per le molte scelte di sicurezza che è necessario prendere. Sarà questa un'occasione per documentarsi meglio sul sistema e sulle applicazioni.

Per verificare che si siano raccolte le necessarie informazioni sulle applicazioni, è necessario:
- Completare il modulo Descrizione dell'applicazione per ogni applicazione aziendale presente nel sistema.
- Facoltativamente, preparare un modulo Descrizione dell'applicazione per ogni applicazione speciale presente nel sistema.
- Riempire le sezioni relative alla libreria ed al file del modulo Convenzioni di denominazione.
- Preparare un modulo Descrizione della libreria per ogni libreria dell'applicazione.
- Tracciare un diagramma della relazione fra le applicazioni e le librerie.

Dopo aver completato questi moduli, è possibile iniziare a pianificare la strategia di sicurezza globale.

Pianificare la strategia di sicurezza globale

Dopo aver pianificato la sicurezza delle applicazioni, si è pronti a pianificare la strategia di sicurezza globale. Prima di tutto, è necessario scegliere l'approccio globale per la sicurezza del sistema. Nel farlo, considerare le attuali esigenze dell'azienda rispetto a quelle future.

Servirsi di queste informazioni come guida durante il processo di pianificazione al fine di determinare la normativa e gli obiettivi di sicurezza. E' inoltre possibile utilizzare tali informazioni per scegliere i valori di base del sistema che influenzano tutti gli utenti del sistema.

Quali moduli sono necessari?

Per completare la pianificazione delle applicazioni, utilizzare il modulo Selezione valori di sistema.

Quando si esaminano questi argomenti per scegliere i valori di sistema, è necessario utilizzare il modulo Piano di sicurezza fisica ed i moduli Descrizione dell'applicazione completati in precedenza.

Esaminare tali argomenti per pianificare la strategia di sicurezza:
- Scrivere la normativa di sicurezza
- Scegliere il livello di sicurezza
- Scegliere i valori di sistema che influenzano il collegamento

- Scegliere i valori di sistema che influenzano le parole d'ordine
- Utilizzare i valori di sistema per personalizzare il sistema

Scrivere la normativa di sicurezza

Prima di iniziare la pianificazione, preparare una relazione sulla politica aziendale riguardo la sicurezza del sistema. Questa relazione costituisce un accordo fra gli utenti e i dirigenti dell'azienda. Consentono di prendere decisioni e di determinare ciò che è importante. E' necessario che la normativa di sicurezza specifichi l'approccio globale e le informazioni che richiedono protezione.

E' necessario che ogni sistema abbia delle caratteristiche di sicurezza. E' possibile adottare uno di questi approcci per la sicurezza:

- **Rigoroso**: alcuni denominano questo schema di sicurezza ″fondamentale″. In un ambiente di sicurezza rigoroso, agli utenti è consentito l'accesso solo alle informazioni ed alle funzioni necessarie per l'esecuzione del loro lavoro. Tutte le altre vengono escluse. Molti revisori consigliano l'approccio rigoroso.
- **Medio**: un approccio di sicurezza medio consente agli utenti l'accesso agli oggetti in base alle autorizzazioni loro assegnate.
- **Non rigoroso**: In un ambiente di sicurezza non rigoroso, si consente agli utenti autorizzati l'accesso alla maggior parte degli oggetti presenti nel sistema. Si limita l'accesso in caso di specifiche risorse critiche o confidenziali, un singolo reparto o un'azienda di piccole dimensioni utilizza generalmente l'approccio non rigoroso nei propri sistemi.

L'approccio globale consente di effettuare delle scelte circa le esigenze di sicurezza specifiche. L'approccio di sicurezza per il sistema dovrebbe fare in modo che la filosofia relativa all'accesso alle informazioni venga applicata a tutta l'azienda. Se non si è convinti circa il tipo di approccio da utilizzare, provare il seguente:

- Utilizzare il modulo Descrizione dell'applicazione già completato per determinare chi può o non può avere accesso a tali applicazioni.
- Esaminare le tecnologie che si utilizzano nell'azienda. Ad esempio, se si ha intenzione di collegare il sistema o la rete ad Internet, sarà necessario un ambiente di sicurezza maggiormente restrittivo per proteggere il sistema da altri utenti di Internet.
- Consultarsi con gli altri membri dell'organizzazione, ad esempio con gli addetti alla sicurezza, per meglio determinare le proprie esigenze di sicurezza.

Si ricordi che è sempre possibile modificare la normativa. La maggior parte delle aziende richiedono una sicurezza più rigorosa man mano che si espandono. Queste informazioni consentono di configurare uno schema di sicurezza al quale si possa successivamente aggiungere ulteriore sicurezza, senza dover apportare molte modifiche o verificare di nuovo tutte le applicazioni.

Cosa proteggere

Oltre a specificare l'approccio globale alla sicurezza nella normativa di sicurezza, è necessario identificare le informazioni più importanti per l'azienda. Il sistema di sicurezza deve essere progettato in modo da proteggere queste informazioni. E' possibile utilizzare diversi requisiti per individuare le risorse più importanti:

- **Riservatezza**: informazioni generalmente non disponibili ai dipendenti dell'azienda. Il libro paga costituisce un esempio di informazioni riservate.
- **Competitività**: informazioni utili per battere la concorrenza, ad esempio specifiche e formule dei prodotti.
- **Operazioni**: informazioni relative al proprio computer essenziali per le quotidiane operazioni dell'azienda, ad esempio documentazione relativa alla clientela e valutazione dell'inventario.

Sharon Jones, responsabile della riservatezza, e John Smith, presidente dell'azienda, hanno collaborato alla preparazione di una relazione sulla normativa di sicurezza. John Smith ha utilizzato questi appunti per la stesura della normativa di sicurezza dell'Azienda di giocattoli JKL. E' possibile esaminare la normativa di sicurezza inviata dall'Azienda di giocattoli JKL a tutti i propri dipendenti, una volta completate la pianificazione e l'impostazione della sicurezza. Ricordarsi di prendere appunti su ciò che si desidera aggiungere alla normativa di sicurezza durante la lettura di questi argomenti relativi alla pianificazione.

Tabella 10. Normativa di sicurezza dell'Azienda di giocattoli JKL: esempio

Approccio globale

Non rigoroso: la maggior parte delle persone deve accedere alla maggior parte delle informazioni.

Informazioni importanti

- Contratti e tariffe speciali
- Libro paga
- La documentazione relativa alla clientela e all'inventario è disponibile solo per i dipendenti dell'azienda.

Regole generali

- Ogni sistema deve disporre di un profilo utente. L'utente non può condividere profili o parole d'ordine.
- L'utente deve modificare la propria parola d'ordine ogni 60 giorni.

Dopo aver preso appunti sulla normativa di sicurezza, è possibile scegliere il livello di sicurezza.

Scegliere il livello di sicurezza

Il valore di sistema QSECURITY consente di controllare il livello di sicurezza desiderato nel sistema. Per comprendere il funzionamento dei livelli di sicurezza, si pensi al sistema come ad un edificio, in cui si tenti di entrare.

Livello 20: sicurezza parola d'ordine

Se si seleziona il livello 20, si dispone di un certo grado di protezione. Il vigilante alla porta dell'edificio chiede l'ID e la parola d'ordine segreta. Solo chi possiede entrambe le informazioni viene ammesso all'edificio. Una volta entrati, tuttavia, è possibile muoversi liberamente.

Se qualcuno riesce a sentire la parola d'ordine segreta e la utilizza per accedere all'edificio, si resta senza protezione.

Livello 30: parola d'ordine e sicurezza delle risorse

Il livello 30 ha le stesse caratteristiche del livello 20, ma consente anche di controllare chi accede ad alcune parti dell'edificio e che cosa fa una volta entrato. E' possibile fornire accesso ad alcune parti dell'edificio, mentre lo si limita ad altre mettendo dei sorveglianti alle porte.

E' possibile consentire a chi ha accesso ai settori riservati di muoversi liberamente o è possibile esigere che si richiedano informazioni agli impiegati autorizzati alle informazioni (programmi). Un intruso che entri utilizzando la parola d'ordine di qualcun altro potrebbe superare la sorveglianza all'interno per raggiungere i settori protetti.

Livello 40: protezione di integrità

Il livello 40 fornisce la stessa protezione del livello 30, inoltre il sistema verifica l'accesso dell'utente. La vigilanza alle porte all'interno dell'edificio controlla le parole d'ordine e le registrazioni di tutti gli utenti che entrano.

Livello 50: protezione di integrità avanzata

Al livello 50, la vigilanza applica una serie di regole ancora più rigorose per evitare che chi dispone di adeguate conoscenze riesca ad eludere la sorveglianza, convalidando l'identità di chiunque abbia effettuato la registrazione.

Suggerimenti

iSeries viene consegnato con un livello di sicurezza 40. Il livello di sicurezza 40 costituisce la migliore opzione per la maggior parte delle installazioni, sia nel caso di una normativa di sicurezza rigorosa, media o non rigorosa. Se si sceglie un approccio non rigoroso, è possibile configurare l'accesso pubblico alla maggior parte delle risorse presenti nel sistema. Utilizzando il livello di sicurezza 40 fin dall'inizio, si dispone della flessibilità necessaria per rendere il sistema più sicuro nel futuro senza dover apportare molte modifiche.

Se i programmi dell'applicazione vengono acquistati, controllare presso il fornitore dell'applicazione che i programmi siano stati verificati con il livello 40. Alcune applicazioni utilizzano delle operazioni che generano errori al livello di sicurezza 40. Se le applicazioni non sono state verificate al livello 40 o 50, partire dal livello 30. Utilizzare la funzione di giornale di controllo per verificare che le applicazioni registrino degli errori di autorizzazione. Se ciò non si verifica, è possibile passare al livello 40 o 50.

Il livello di sicurezza 50 evita che si verifichino eventi che normalmente non ricorrono nella maggior parte dei sistemi. Il sistema effettua ulteriori verifiche ogni qualvolta vengono eseguiti programmi sul sistema. Tali ulteriori verifiche potrebbero sortire un effetto negativo sulle prestazioni.

Dopo aver immesso la scelta del livello di sicurezza nel modulo Selezione valori di sistema, è possibile scegliere i valori di sistema che influenzano il collegamento.

Scegliere i valori di sistema che influenzano il collegamento

Dopo aver scelto il livello di sicurezza, è possibile personalizzare ciò che viene visualizzato agli utenti ed il modo in cui essi interagiscono con il sistema utilizzando i valori di sistema. Potrebbe essere necessario pianificare questi valori di sistema ed utilizzare il modulo Selezione valori di sistema per registrare le scelte.

La seguente tabella descrive i valori di sistema utilizzati in questo argomento.

Tabella 11. Valori di sistema iSeries e loro descrizioni

Valore di sistema	Descrizione
QMAXSIGN	Limita il numero di tentativi di collegamento consecutivi.
QMAXSGNACN	Specifica l'operazione intrapresa dal sistema se si raggiunge il numero massimo di tentativi di collegamento consecutivi.
QLMTDEVSSN	Determina la possibilità di un utente di collegarsi a più di una stazione di lavoro con lo stesso profilo utente.
QINACTITV	Determina quando il sistema intraprende un'operazione sui lavori inattivi.
QINACTMSGQ	Determina l'operazione intrapresa dal sistema quando un lavoro è rimasto inattivo per il periodo di tempo specificato dal valore di sistema QINACTITV.
QDSCJOBITV	Controlla se e quando il sistema termina un lavoro temporaneamente scollegato.
QLMTSECOFR	Restringe il campo d'azione del responsabile della riservatezza, che detiene l'autorizzazione su tutti gli oggetti presenti nel sistema per le specifiche unità.

Limitare il numero di tentativi di collegamento (QMAXSIGN e QMAXSGNACN)

Due valori di sistema determinano il numero di volte in cui è possibile tentare di collegarsi al sistema e l'operazione che il sistema intraprende una volta raggiunto il limite.

Il valore di sistema QMAXSIGN (numero massimo di tentativi di collegamento) limita il numero di tentativi di collegamento errati consecutivi consentiti dal sistema prima di intraprendere delle operazioni. Un tentativo di collegamento errato indica che si sta tentando di utilizzare un particolare profilo utente con una parola d'ordine non valida o con un'autorizzazione non appropriata per una stazione di lavoro.

Il valore di sistema QMAXSGNACN (numero massimo di operazioni di collegamento) specifica le operazioni eseguite dal sistema se si tenta di collegarsi troppe volte in una riga. I valori possibili sono:

1 Impedire ogni ulteriore tentativo di collegamento all'unità. Questa operazione viene definita come disabilitazione dell'unità. Nessuno può collegarsi all'unità fino a che una persona autorizzata non modifichi l'unità utilizzando il comando WRKCFGSTS. Generalmente questa opzione non costituisce una protezione sufficiente, specialmente quando i tentativi di collegamento al sistema vengono effettuati da un personal computer o da un sistema remoto.

Un operatore di sistema o chiunque disponga dell'autorizzazione *USE all'unità può rendere nuovamente disponibile l'unità.

2 Impedire ogni ulteriore tentativo di collegamento al profilo utente. Questa operazione viene definita come disabilitazione del profilo utente. Nessuno può collegarsi con tale profilo fino a che una persona autorizzata non lo abiliti utilizzando il comando Modifica profilo utente (CHGUSRPRF).

Per abilitare un profilo utente (modificare lo stato), è necessario essere un responsabile della riservatezza con l'autorizzazione ad utilizzare tale profilo.

3 Disabilitare sia il profilo utente che l'unità.

Rischi e suggerimenti

Alcuni pirati informatici si dilettano a risalire alle parole d'ordine e a violare i sistemi. Limitando il numero di tentativi di collegamento consentiti, si limitano le loro possibilità di risalire alle parole d'ordine.

Il valore di sistema QMAXSIGN (numero massimo di collegamenti non validi) determina il numero di tentativi di collegamento consentiti. Impostare tale valore su un numero abbastanza alto in modo da evitare di arrecare fastidi agli utenti. Impostare tale valore su un numero abbastanza basso in modo da scoraggiare distrazioni nell'immissione dei caratteri e da evitare di dare ad un potenziale intruso troppe possibilità di indovinare. Si consiglia di impostare il valore del numero massimo di tentativi di collegamento su un valore compreso tra 3 e 5.

Il numero massimo di operazioni di collegamento consigliato (QMAXSGNACN) è 3, sebbene la disabilitazione dell'unità e del profilo utente potrebbe creare degli inconvenienti agli utenti del sistema. Una stazione di lavoro ubicata in un luogo privato potrebbe dare ad un intruso la possibilità di tentare molte differenti combinazioni di profilo utente e di parola d'ordine. Se il sistema non dispone di stazioni di lavoro che costituiscono un rischio a causa della loro ubicazione, la disabilitazione del solo profilo utente costituisce probabilmente una protezione sufficiente.

Controllare il modulo Sicurezza fisica già completato. Se si hanno delle stazioni di lavoro in ubicazioni remote o si hanno degli utenti remoti (utenti che accedono al sistema attraverso linee telefoniche o collegamenti VPN), è possibile limitare il collegamento in maniera più rigorosa. Verificare di aver aggiunto le scelte per QMAXSIGN e QMAXSGNACN alla Parte 2 del modulo Selezione valori di sistema.

Può risultare utile esaminare un esempio che illustra le modalità di funzionamento congiunto di questi valori di sistema al fine di limitare i tentativi di collegamento prima di scegliere dei valori di sistema che limitino gli utenti ad una sola stazione di lavoro alla volta.

Esempio: limitare i tentativi di collegamento: Sharon Jones ha limitato i tentativi di collegamento a 3 (QMAXSIGN è 3) ed ha scelto di disabilitare sia il profilo che l'unità se si supera il limite (QMAXSGNACN è 3). Qui di seguito è riportato un esempio di ciò che potrebbe accadere se si raggiungessero questi valori:

1. Roger immette due volte la propria parola d'ordine in maniera errata.

2. Dopo il secondo tentativo riceve un messaggio che lo avvisa che un altro tentativo di collegamento errato disabiliterà il profilo utente.
3. Egli commette un altro errore.
4. Il sistema disabilita il suo profilo e la stazione di lavoro non ha più un pannello di collegamento. Se Roger tenta di collegarsi ad un'altra stazione di lavoro, riceve un messaggio di errore.
5. A questo punto deve chiedere a Sharon di abilitare il suo profilo per riprovare. Sharon o l'operatore di sistema devono rendere disponibile anche la stazione di lavoro di Roger. Se Roger non ricorda la sua parola d'ordine, Sharon può assegnarli una parola d'ordine temporanea che egli dovrà modificare quando si collegherà nuovamente.

Qui di seguito è possibile esaminare il valore di sistema che limita gli utenti ad una stazione di lavoro alla volta.

Limitare gli utenti ad una stazione di lavoro alla volta

Il valore di sistema QLMTDEVSSN (Limite sessioni unità) stabilisce se uno stesso utente può collegarsi a più di una stazione di lavoro contemporaneamente. I valori possibili sono:

0 Il sistema consente ad un numero illimitato di utenti di collegarsi contemporaneamente con lo stesso profilo utente.

1 E' possibile utilizzare un profilo utente solo su un'unità alla volta. L'utente potrebbe disporre di più sessioni sulla stessa unità.

Rischi e suggerimenti

Consentire agli utenti di collegarsi ad una sola stazione di lavoro alla volta favorisce buone abitudini di sicurezza. Cattive abitudini di sicurezza costituiscono un rischio per la sicurezza:

- Se si limitano gli utenti ad un'unità, si scoraggia la condivisione di ID utente e di parole d'ordine. Se si condividono gli ID utente, vengono compromessi il controllo e l'affidabilità. Non sarà più possibile individuare chi ha veramente eseguito determinate funzioni sul sistema.
- E' indispensabile che gli utenti ricordino di scollegarsi da una stazione di lavoro prima di spostarsi su un'altra. Le stazioni di lavoro lasciate collegate, ma non utilizzate, costituiscono un rischio per la sicurezza.

L'impostazione consigliata per il valore di sistema QLMTDEVSSN è 1 e limita gli utenti ad una singola unità. Assegnare ad ogni utente del sistema un ID utente ed una parola d'ordine univoci con le autorizzazioni appropriate, quindi limitarli all'utilizzo di una sola stazione di lavoro alla volta. Verificare di aver aggiunto la scelta per QLMTDEVSSN alla Parte 2 del modulo Selezione valori di sistema.

E' quindi possibile iniziare a pianificare i valori di sistema per i lavori inattivi.

Pianificare i valori di sistema per i lavori inattivi

Tre valori di sistema funzionano congiuntamente per determinare quale operazione viene intrapresa dal sistema quando un utente dimentica di scollegare la stazione di lavoro.

Intervallo supero tempo lavoro inattivo (QINACTITV)

Il valore di sistema QINACTITV determina se il sistema intraprende un'operazione nel caso in cui ci si sia collegati ad una stazione video, ma essa sia rimasta inattiva per un determinato periodo di tempo.

Nota: **Inattivo** indica che l'utente non ha premuto il tasto Invio o un tasto funzionale durante l'intervallo specificato.

Coda messaggi lavoro inattivo (QINACTMSGQ)

L'impostazione del valore di sistema QINACTMSGQ determina il comportamento del sistema nel caso in cui scada il limite di tempo specificato nel valore di sistema QINACTITV. Se si seleziona ENDJOB, il sistema termina ogni lavoro che sia rimasto inattivo più a lungo dell'intervallo di supero tempo scelto per QINACTITV. Se si seleziona DSCJOB, il sistema scollega un lavoro

inattivo. Se si specifica il nome di una coda messaggi, il sistema invia un messaggio di avvertenza a quella coda quando un lavoro è rimasto inattivo troppo a lungo.

Quando il sistema **scollega** un lavoro in una stazione di lavoro, sospende temporaneamente il lavoro. La stazione di lavoro ritorna al pannello di collegamento. Il lavoro scollegato riprende quando lo stesso utente si collega nuovamente alla stessa stazione di lavoro.

Intervallo supero tempo lavoro scollegato (QDSCJOBITV)
Il valore di sistema QDSCJOBITV controlla se e quando il sistema termina un lavoro che è stato temporaneamente scollegato. I lavori possono essere scollegati automaticamente dal sistema, come risultato dei valori di sistema QINACTITV e QINACTMSGQ. Gli utenti possono inoltre richiedere che i loro lavori siano temporaneamente scollegati utilizzando un'opzione del menu dell'Operational Assistant o il comando DSCJOB (Scollegamento lavoro).

Rischi e suggerimenti

Se Sharon dimentica di scollegarsi dalla stazione di lavoro prima di uscire, John può andare alla stazione di lavoro ed eseguire qualunque funzione ella fosse autorizzata ad effettuare sul sistema.

Si consiglia di regolare le stazioni video inattive soprattutto modo per due motivi:

- Si dispone di un ambiente di sicurezza rigoroso con informazioni riservate memorizzate nel sistema.
- Si dispone di stazioni di lavoro ubicate in luoghi a cui persone esterne all'azienda possono avere facile accesso.

Normali incombenze lavorative spesso interrompono gli utenti nelle loro stazioni di lavoro. Sfruttare il funzionamento congiunto di questi tre valori di sistema per consentire le normali interruzioni e continuare comunque a proteggere la sicurezza del sistema.

Per eliminare questi rischi, l'IBM consiglia di utilizzare contemporaneamente i valori di sistema QINACTITV, QINACTMSGQ, e QDSCJOBITV per consentire le normali interruzioni di lavoro e continuare a proteggere la sicurezza del sistema.

Intervallo supero tempo lavoro inattivo (QINACTITV): rendere l'intervallo abbastanza breve in modo da evitare che le stazioni di lavoro non vengano lasciate senza sorveglianza, ma non così breve da creare inconvenienti agli utenti. L'impostazione consigliata è 30 minuti. Quando un lavoro è rimasto inattivo per 30 minuti, il sistema intraprende un'operazione specificata nella coda messaggi lavoro inattivo.

Coda messaggi lavoro inattivo (QINACTMSGQ): scegliere Scollegamento lavoro. Il sistema scollega tutti i lavori rimasti inattivi nel lasso di tempo specificato nell'intervallo supero tempo lavoro inattivo. Il sistema sospende il lavoro e scollega la stazione video. Quando lo stesso utente si collega nuovamente, il lavoro riprende dal punto in cui era stato interrotto.

Quest'operazione risulta più comoda per gli utenti, dal momento che il sistema sospende i lavori invece di terminarli. Lo scollegamento di un lavoro inattivo fornisce al sistema la stessa protezione offerta dalla chiusura del lavoro.

Nota: il sistema non può scollegare alcuni lavori. Nel caso in cui il sistema non possa scollegare un lavoro inattivo, esso termina il lavoro. Tale operazione potrebbe causare la perdita delle informazioni. Utilizzare l'impostazione di QINACTMSGQ per inviare i messaggi alla coda messaggi dell'operatore di sistema.

Intervallo supero tempo lavoro scollegato (QDSCJOBITV): incoraggiare gli utenti del sistema a scollegarsi temporaneamente dal sistema quando devono assentarsi dalle stazioni di lavoro per brevi periodi, terminare il loro lavoro e scollegarsi quando devono assentarsi per periodi più lunghi.

Utilizzare QDSCJOBITV per terminare i lavori scollegati prima che il sistema avvii l'attività notturna, ad esempio la ripulitura automatica. Impostarlo su un valore abbastanza lungo per consentire all'utente di tornare alla stazione di lavoro entro le ore lavorative, ma abbastanza breve da poter terminare i lavori prima dell'avvio dell'attività notturna. Scegliere 300 minuti (cinque ore) in modo da dare all'attività notturna il tempo necessario per completarsi senza interferire con il lavoro dell'utente.

Nota: per evitare che due utenti tentino di modificare le stesse informazioni contemporaneamente, il sistema **blocca** un record prima di aggiornarlo. Ogni blocco nelle risorse resta attivo quando il sistema scollega un lavoro dell'utente. A seconda della progettazione dell'applicazione e del numero di utenti presenti nel sistema, i blocchi potrebbero causare dei problemi nelle prestazioni del sistema. Verificare con il programmatore o con il fornitore dell'applicazione se il blocco può influenzare le prestazioni.

E' possibile esaminare un esempio del funzionamento congiunto di questi valori di sistema per la gestione dei lavori inattivi nel sistema.

Dopo aver registrato le scelte per i lavori inattivi nel modulo Selezione valori di sistema, è possibile decidere in che modo limitare i luoghi da cui il responsabile della riservatezza può collegarsi.

Esempio: gestire i lavori inattivi con i valori di sistema QINACTITV, QINACTMSGQ e QDSCJOBITV: Si supponga di aver impostato l'intervallo di supero tempo lavoro inattivo (QINACTITV) su 30 minuti. Il sistema scollega i lavori inattivi (QINACTMSGQ è DSCJOB). L'intervallo supero tempo lavoro scollegato (QDSCJOBITV) è 300 minuti (5 ore). Ad esempio, se Sharon dimentica di scollegare il sistema alle 9:30, il sistema scollega il suo lavoro alle 10:00 e termina il lavoro alle 15:00.

Aggiungere le scelte per i valori di sistema QINACTITV, QINACTMSGQ e QDSCJOBITV sulla Parte 2 del modulo Selezione valori di sistema.

Dopo aver registrato le decisioni per i lavori inattivi nel modulo Selezione valori di sistema, è possibile decidere come limitare i luoghi da cui il responsabile della riservatezza può collegarsi.

Limitare i luoghi da cui il responsabile della riservatezza può collegarsi

E' possibile limitare il numero di utenti autorizzati a modificare gli oggetti della sicurezza e del controllo ad alcune stazioni di lavoro. Tale operazione impedisce agli utenti di collegarsi di nascosto alle stazioni di lavoro da ubicazioni remote. Il valore di sistema QLMTSECOFR (limitazione responsabile riservatezza) consente di realizzare ciò. Se si imposta QLMTSECOFR su 1, gli utenti con l'autorizzazione speciale per tutti gli oggetti (*ALLOBJ) o al servizio (*SERVICE) possono collegarsi solo alla console o ad altre stazioni di lavoro designate.

QLMTSECOFR limita il responsabile della riservatezza, gli utenti con l'autorizzazione a tutti gli oggetti presenti nel sistema ed il personale addetto alla manutenzione della console. E' possibile utilizzare il comando GRTOBJAUT (Concessione autoriz. oggetto) per dare a questi utenti l'accesso alle altre unità.

Nota: per il funzionamento del valore di sistema QLMTSECOFR, il livello di sicurezza del sistema deve essere 30 o superiore.

Rischi e suggerimenti

Si consiglia di impostare il valore di sistema QLMTSECOFR su 1. Nell'eventualità che qualcuno riesca a sentire o a scoprire la parola d'ordine di chi dispone del profilo del responsabile della riservatezza, è necessario che riesca ad accedere ad un'unità che consenta di collegarsi.

Dopo aver scelto QLMTSECOFR nella Parte 2 del modulo Selezione valori di sistema, è possibile scegliere i valori di sistema che influenzano le parole d'ordine.

Scegliere i valori di sistema che influenzano le parole d'ordine

Si consiglia di consentire agli utenti di scegliere le proprie parole d'ordine invece di farle assegnare dal responsabile della riservatezza. Quando gli utenti creano le proprie parole d'ordine, generalmente non hanno necessità di trascriverle. Le parole d'ordine trascritte di solito vengono conservate in posti ovvi costituendo così un rischio per la sicurezza.

Suggerimento per la creazione delle parole d'ordine

Per gli utenti potrebbe non essere semplice pensare a parole d'ordine valide. Suggerire tale tecnica: utilizzare una frase facile da ricordare per riuscire a creare una parola d'ordine che risulti difficile da indovinare. Ad esempio, dopo una vacanza si potrebbe utilizzare la frase ″Il 4 luglio la pesca è stata scarsa″ per creare la parola d'ordine `4LPSS`.

Diversi valori di sistema regolano le parole d'ordine. E' possibile controllare la frequenza con cui gli utenti devono modificare le parole d'ordine. E' inoltre possibile stabilire molte regole per evitare l'utilizzo di parole d'ordine che siano facili da indovinare. Molti di questi valori di sistema sono importanti per le società di grandi dimensioni. Solo pochi di questi valori sono importanti per tutte le società.

Utilizzando un'opzione nel menu ASSIST o il comando Modifica parola d'ordine (CHGPWD), gli utenti possono assegnare parole d'ordine proprie. Quando gli utenti modificano le proprie parole d'ordine, il sistema verifica la nuova parola d'ordine in base ai valori di sistema della parola d'ordine. Se un utente modifica una parola d'ordine utilizzando il comando CHGUSRPRF, il sistema non verifica la nuova parola d'ordine in base ai valori del sistema di sicurezza.

Nota: se sono stati impostati i valori di sistema della parola d'ordine, il sistema non consente che la nuova parola d'ordine sia la stessa del nome del profilo utente, a meno che non si utilizzi il comando CHGUSRPRF per impostare la parola d'ordine.

La seguente tabella mostra i valori di sistema che influenzano le parole d'ordine con le relative definizioni:

Tabella 12. Valori di sistema iSeries relativi alla parola d'ordine

Valore di sistema	Descrizione
QPWDEXPITV	Richiede agli utenti di modificare le proprie parole d'ordine dopo un periodo specificato.
QPWDMAXLEN	Consente di specificare il numero massimo di caratteri delle parole d'ordine.
QPWDMINLEN	Consente di specificare il numero minimo di caratteri delle parole d'ordine.
QPWDRQDDIF	Impedisce agli utenti di utilizzare alternativamente due diverse parole d'ordine.

Questi argomenti forniscono maggiori dettagli sui valori di sistema relativi alle parole d'ordine:

- Determinare la durata della parola d'ordine
- Determinare la lunghezza delle parole d'ordine
- Limitare la duplicazione delle parole d'ordine

Immettere `WRKSYSVAL *SEC` nella riga comandi CL e visualizzare le informazioni in linea per i valori di sistema che iniziano con i caratteri QPWD.

Determinare la durata della parola d'ordine

Il valore di sistema QPWDEXPITV determina la frequenza con cui gli utenti devono modificare le parole d'ordine.

Il sistema avvisa gli utenti quando la data di scadenza della parola d'ordine si avvicina. Se una parola d'ordine scade, il sistema richiede agli utenti di modificare le parole d'ordine al successivo collegamento.

Suggerimenti

Gli utenti dovrebbero modificare periodicamente le proprie parole d'ordine. Ciò scoraggia la condivisione delle parole d'ordine con altri utenti del sistema. Inoltre, se un utente non autorizzato individua la parola d'ordine di qualcuno, quella parola d'ordine funzionerà solo per un breve lasso di tempo. Impostare l'intervallo della parola d'ordine su un valore abbastanza lungo da evitare fastidi agli utenti, ma sufficientemente breve da fornire una buona sicurezza. Per evitare tali problemi, impostare l'intervallo su un valore compreso fra i 45 ed i 60 giorni.

Dopo aver immesso la scelta per il valore di sistema QPWDEXPITV nella Parte 2 del modulo Selezione valori di sistema, è possibile determinare la lunghezza delle parole d'ordine.

Determinare la lunghezza delle parole d'ordine

Ad alcuni utenti non piace scrivere con la tastiera. Se potessero, sceglierebbero una parola d'ordine di una lettera o le proprie iniziali. Purtroppo è molto più facile per un intruso indovinare delle parole d'ordine brevi. Il valore di sistema QPWDMINLEN consente di impostare una lunghezza minima per tutte le parole d'ordine del sistema.

Se il sistema comunica con altri sistemi, gli utenti potrebbero scambiare le parole d'ordine fra i due computer. Alcuni metodi di comunicazione limitano la parola d'ordine ad un massimo di 8 caratteri. Il valore di sistema QPWDMAXLEN consente di specificare una lunghezza massima per le parola d'ordine.

Suggerimenti

Impostare la lunghezza minima della parola d'ordine su 6. Questo valore elimina l'utilizzo di iniziali ed incoraggia gli utenti ad essere un po' più creativi nella scelta delle parole d'ordine. Impostare la lunghezza massima della parola d'ordine su 8 se il sistema comunica con altri sistemi.

Dopo aver immesso le scelte per i valori di sistema QPWDMINLEN e QPWDMAXLEN nella Parte 2 del modulo Selezione valori di sistema, è possibile decidere di quanto limitare la duplicazione delle parole d'ordine.

Limitare la duplicazione delle parole d'ordine

Il comando Modifica parola d'ordine (CHGPWD) richiede che la nuova parola d'ordine sia diversa dalla vecchia. Gli utenti, tuttavia, possono alternare la scelta tra due diverse parole d'ordine, a meno che non si utilizzi il valore di sistema QPWDRQDDIF per evitarlo. La seguente tabella mostra le scelte per il valore di sistema QPWDRQDDIF:

Tabella 13. Valori per il valore di sistema QPDRQDDIF

Valore	Numero di parole d'ordine 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

Suggerimenti

Utilizzare l'intervallo di scadenza della parola d'ordine ed i valori della parola d'ordine duplicata per richiedere che quelle parole d'ordine siano le stesse per un anno. Ad esempio, se le parole d'ordine scadono entro 60 giorni, selezionare 7 per il valore di sistema QPWDRQDDIF.

Dopo aver immesso la scelta per il valore di sistema QPWDRQDDIF nella Parte 2 del modulo Selezione valori di sistema, è possibile decidere come utilizzare i valori di sistema per personalizzare il sistema.

Utilizzare i valori di sistema per personalizzare il sistema

iSeries utilizza i valori di sistema e gli attributi di rete per controllare molte altre funzioni oltre alla sicurezza. I programmatori del sistema e dell'applicazione utilizzano la maggior parte di questi valori di sistema ed attributi. E' necessario che il responsabile della riservatezza imposti dei valori di sistema e degli attributi di rete per personalizzare il sistema.

Assegnare un nome al sistema

Per assegnare un nome al sistema si utilizza l'attributo di rete SYSNAME. Il nome del sistema viene visualizzato nell'angolo superiore destro del pannello di collegamento e nella documentazione del sistema. Viene inoltre utilizzato quando il sistema comunica con un altro sistema o con dei personal computer che utilizzano iSeries Access per Windows.

Quando il sistema comunica con altri sistemi o personal computer, il nome di sistema identifica e distingue il sistema dagli altri presenti nella rete. I computer si scambiano i nomi di sistema ogni qualvolta comunicano. Dopo aver assegnato un nome al sistema, si consiglia di non modificarlo, in quanto la sua eventuale modifica influenzerebbe gli altri sistemi della rete.

Suggerimenti

Scegliere un nome univoco e significativo per il sistema. Anche se al momento non si è in comunicazione con altri computer, lo si potrebbe essere in futuro. Se il sistema fa parte di una rete, probabilmente il gestore della rete suggerirà il nome del sistema da utilizzare.

Ad esempio, Sharon Jones dell'Azienda di giocattoli JKL ha deciso di denominare il sistema JKLTOY.

Visualizzare l'ora e la data sul sistema

E' possibile impostare la sequenza in cui vengono visualizzati l'anno, il mese ed il giorno quando il sistema stampa o visualizza la data. E' inoltre possibile specificare quale carattere deve essere utilizzato dal sistema fra l'anno (Y), il mese (M) ed il giorno (D).

Il valore di sistema QDATFMT determina il formato della data. Il seguente grafico mostra il modo in cui il sistema stampa la data, 16 giugno 2000, per ogni possibilità di scelta:

Tabella 14. QDATFMT (formati data sistema)

Scelta	Descrizione	Risultato
YMD	anno, mese, giorno	00/06/16
MDY	mese, giorno, anno	06/16/00
DMY	giorno, mese, anno	16/06/00
JUL	data giuliana	00/168

Nota: questi esempi utilizzano la barra (/) come separatore della data.

Il valore di sistema QDATSEP determina quale carattere utilizzare fra anno, mese e giorno. La seguente tabella mostra le scelte. Si utilizza un numero per specificare la scelta:

Tabella 15. QDATSEP (separatore data sistema)

Carattere separatore	Valore QDATSEP	Risultato
/ (barra)	1	16/06/00
- (trattino)	2	16-06-00
. (punto)	3	16.06.00
, (virgola)	4	16,06,00
(spazio)	5	16 06 00

Nota: i precedenti esempi utilizzano il formato DMY.

Il valore di sistema QTIMSEP determina il carattere utilizzato dal sistema per separare le ore, i minuti ed i secondi quando viene visualizzata l'ora. Si utilizza un numero per specificare la scelta. La seguente tabella mostra il modo in cui le ore 10:30 del mattino verrebbe formattato utilizzando ciascun valore:

Tabella 16. QTIMSEP (separatore ora sistema)

Carattere separatore	QTIMSEP	Risultato
: (due punti)	1	10:30:00
. (punto)	2	10.30.00
, (virgola)	3	10,30,00
(spazio)	4	10 30 00

Scegliere la denominazione delle unità di sistema

Il sistema configura automaticamente tutte le nuove stazioni video e le nuove stampanti collegate. Il sistema assegna un nome ad ogni nuova unità. Il valore di sistema QDEVNAMING determina il modo in cui vengono assegnati i nomi. Il seguente grafico mostra in che modo il sistema denomina la terza stazione video e la seconda stampante collegate al sistema:

Tabella 17. Denominazione unità di sistema

Scelta	Formato denominazione	Nome stazione video	Nome stampante
1	iSeries	DSP03	PRT02
2	S/36	W3	P2
3	Indirizzo dell'unità	DSP010003	PRT010002

Nota: nell'esempio precedente, la stazione video e la stampante sono collegate al primo cavo.

Suggerimenti

Utilizzare le convenzioni di denominazione di iSeries, a meno che non sia in esecuzione un software che richiede la denominazione S/36. I nomi iSeries per le stazioni video e le stampanti sono più comodi dei nomi che utilizzano l'indirizzo dell'unità. I nomi delle stazioni video e delle stampanti vengono visualizzati sui diversi pannelli dell'Operational Assistant. I nomi delle stampanti vengono inoltre utilizzati per gestire l'emissione di stampa.

Dopo che il sistema ha configurato una nuova unità, utilizzare il comando Modifica descrizione unità (video) CHGDEVDSP o il comando Modifica descrizione unità (stampante) CHGDEVPRT per immettere una descrizione dell'unità significativa. Includere nella descrizione l'indirizzo fisico dell'unità e la sua ubicazione, ad esempio *ufficio di John Smith, linea 1 indirizzo 6*.

Scegliere la stampante di sistema

Utilizzare il valore di sistema QPRTDEV per assegnare la stampante di sistema. Questo valore di sistema, il profilo utente e la descrizione lavoro determinano quale stampante viene utilizzata dal lavoro. Il lavoro utilizza la stampante di sistema a meno che il profilo utente o la descrizione lavoro non ne specifichino una diversa.

Suggerimenti

Generalmente, la stampante di sistema dovrebbe essere la stampante più veloce del sistema. Utilizzare la stampante di sistema per documenti lunghi e per l'emissione del sistema.

Nota: i nomi delle stampanti non verranno resi noti fino a che non sarà stato installato e configurato il sistema. A questo punto, prendere nota dell'ubicazione della stampante di sistema. Inserire il nome della stampante in un secondo momento.

Consentire la visualizzazione dell'emissione di stampa completata

Il sistema fornisce agli utenti la possibilità di trovare la propria emissione di stampa. Il pannello Gestione emissione di stampa mostra tutte le emissioni che sono attualmente in stampa o in attesa di stampa. E' inoltre possibile consentire agli utenti di consultare una lista di emissioni di stampa completate. Questo pannello mostra quando e su quale stampante è stata stampata l'emissione. Ciò può risultare utile per individuare i documenti persi.

La funzione di account del lavoro ed il valore di sistema QACGLVL consentono di visualizzare le emissioni di stampa completate. L'opzione *PRINT per il valore di sistema QACGLVL consente di salvare le informazioni sull'emissione di stampa completata.

Suggerimenti

La memorizzazione delle informazioni sull'emissione di stampa completata occupa spazio sul sistema. A meno che non si ritenga che gli utenti stamperanno molti documenti, probabilmente non sarà necessario fornire questa funzione. Immettere NO nel modulo Selezione valori di sistema. Questo valore imposta il livello di account del lavoro su *NONE.

- Assicurarsi di aver scritto una relazione sulla normativa di sicurezza per la propria azienda simile all'esempio dell'Azienda di giocattoli JKL preparato da Sharon Jones e John Smith.
- Verificare di aver immesso le scelte per i valori di sistema nel modulo Selezione valori di sistema.
- Prendere nota di ciò che si desidera includere la memo relativa alla sicurezza.

Dopo aver immesso tutte le opzioni di sistema nel modulo Selezione valori di sistema ed aver redatto una normativa di sicurezza, è possibile pianificare i gruppi di utenti.

Esempio: normativa di sicurezza dell'Azienda di giocattoli JKL

La memo riportata di seguito mostra la normativa di sicurezza che John Smith, presidente dell'Azienda di giocattoli JKL, invia ai suoi impiegati. Egli ha utilizzato le note create insieme a Sharon per sviluppare questa memo di sicurezza.

Tabella 18. Esempio: memo di sicurezza dell'Azienda di giocattoli JKL

Da: John Smith, Presidente

Tabella 18. Esempio: memo di sicurezza dell'Azienda di giocattoli JKL (Continua)

Azienda di giocattoli JKL

A: Tutti gli impiegati dell'Azienda di giocattoli JKL

Oggetto: Sicurezza del nuovo sistema

Avete tutti partecipato ad un incontro informativo sul nuovo sistema. Quelli che utilizzeranno il sistema hanno iniziato il corso e cominceranno l'elaborazione degli ordini dei clienti la prossima settimana. Vi anticipo che questo sistema diventerà presto fondamentale per il successo dei nostri affari.

Desidero rivedere le decisioni e le normative sulla sicurezza ed enfatizzare la loro importanza. Queste normative sono state progettate per proteggere le informazioni fondamentali per la nostra azienda.

- Sharon Jones è il responsabile della riservatezza del nuovo sistema. Ken Harrison sarà il suo assistente. In caso di dubbi o di problemi relativi alla sicurezza, contattarli.
- Le decisioni su chi può effettuare le funzioni sul sistema si basano sulle normative attuali relative alle informazioni. Ad esempio:
  - Le informazioni sui contratti e sulle tariffe speciali vengono considerate riservate. Non devono mai essere rivelate a persone esterne all'azienda.
  - Solo l'ufficio contabile può impostare e modificare i limiti di credito per i nostri clienti.
- Chiunque abbia la necessità di utilizzare il sistema riceverà un ID utente e una parola d'ordine. Verrà richiesta la modifica della parola d'ordine la prima volta in cui si effettua il collegamento al sistema e ogni 60 giorni dopo quella data. Scegliere una parola d'ordine che possa essere ricordata, ma che non sia ovvia. Il modulo che si riceve insieme all'ID utente contiene alcuni suggerimenti per la creazione delle parole d'ordine.
- *Non condividete la parola d'ordine con nessuno*. Il nostro obiettivo è stato quello di consentire a tutti i dipendenti di effettuare qualsiasi operazione sul sistema necessaria per il proprio lavoro. Se si necessita dell'accesso alle informazioni, contattare Sharon o Ken. Se viene dimenticata la parola d'ordine, Sharon o Ken possono impostarne immediatamente una nuova. Non esiste alcun motivo per cui un utente effettui il collegamento con un ID utente e una parola d'ordine non propri.
- Probabilmente avete imparato ad utilizzare la funzione di registrazione e riproduzione nella vostra stazione di lavoro per salvare le immissioni. *Non* utilizzare questo metodo per memorizzare la vostra parola d'ordine.
- Non lasciate la vostra stazione di lavoro collegata quando siete lontani dalla vostra scrivania. Durante il corso avete imparato a scollegare temporaneamente la vostra stazione di lavoro. Utilizzare questa funzione se avete la necessità di lasciare la postazione per un breve periodo di tempo. Se vi dovete allontanare per un lungo periodo, terminare il lavoro e utilizzare la funzione di scollegamento regolare.

  Scollegarsi quando si lascia la stazione di lavoro è particolarmente importante nelle ubicazioni che sono accessibili al pubblico generico, ad esempio la piattaforma di carico, l'area di servizio clienti e gli uffici vendite distaccati.
- Sebbene l'unità di sistema sia solida, evitare di modificarla. I pannelli di controllo sull'unità verranno disattivati, ma è preferibile che non vengano toccati. I membri dell'ufficio contabile sono responsabili della sicurezza dell'unità di sistema.

Ricordare che il nuovo sistema è stato progettato per rendere più semplici tutti i lavori e per migliorare le prestazioni aziendali. Le nostre normative di sicurezza devono essere d'aiuto e non di ostacolo. In caso di domande o problemi, non esitate a contattare Sharon, Ken o il sottoscritto.

Dopo aver creato una bozza della normativa di sicurezza, è possibile cominciare con Pianificare i gruppi di utenti.

Pianificare i gruppi di utenti

La prima fase del processo di pianificazione, la scelta della strategia di sicurezza, è simile all'impostazione della politica dell'azienda. Si è ora pronti a pianificare i gruppi di utenti, la qual cosa è simile alla scelta della politica di reparto.

Che cos'è un gruppo di utenti?

Un gruppo di utenti consiste esattamente in ciò che il nome indica: un gruppo di persone che ha necessità di utilizzare le stesse applicazioni nello stesso modo. Generalmente, un gruppo di utenti è formato da persone che lavorano nello stesso reparto e che hanno simili responsabilità di lavoro. Si definisce un gruppo di utenti creando un profilo di gruppo.

Che cosa fa un profilo di gruppo?

Un profilo di gruppo persegue due scopi nel sistema:

- **Strumento di sicurezza**: un profilo di gruppo fornisce un semplice modo di stabilire chi può utilizzare alcuni oggetti presenti nel sistema (autorizzazioni all'oggetto). E' possibile definire le autorizzazioni all'oggetto per un intero gruppo invece che per ogni singolo membro del gruppo.
- **Strumento di personalizzazione**: è possibile utilizzare un profilo di gruppo 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. E' possibile definirle nel profilo di gruppo e copiarle nei singoli profili utente.

Utilizzando i profili di gruppo risulta più facile mantenere uno schema semplice e coerente sia per la sicurezza che per la personalizzazione.

Quali moduli sono necessari?

Per pianificare i gruppi di utenti, sono necessari i seguenti moduli:

- Modulo Identificazione gruppo di utenti
- Modulo Descrizione del gruppo di utenti

Nota: potrebbe essere necessario un modulo Descrizione del gruppo di utenti per ogni gruppo di utenti presenti nel sistema.

Esaminare questi argomenti per completare tali moduli:

- Identificare i gruppi di utenti.
- Pianificare i profili di gruppo.
- Scegliere i valori che influenzano il collegamento.
- Scegliere i valori che limitano ciò che un utente può fare.
- Scegliere i valori che configurano l'ambiente dell'utente.

Identificare i gruppi di utenti

Quando si pianificano i gruppi di utenti, è necessario prima di tutto identificare i gruppi di utenti presenti nel sistema. Ciò consente di pianificare gli accessi alle risorse necessarie per questi gruppi. Cercare di utilizzare un metodo semplice per identificare i gruppi di utenti. Prendere in considerazione i reparti o i gruppi di lavoro che intendono utilizzare il sistema. Fare riferimento al diagramma dell'applicazione precedentemente disegnato per le proprie applicazioni. Verificare l'esistenza di una relazione naturale tra i gruppi di lavoro e le applicazioni:

- E' possibile identificare l'applicazione principale per ogni gruppo di lavoro?
- Si conoscono le applicazioni necessarie ad ogni gruppo? Quali applicazioni non sono necessarie?
- A quale gruppo dovrebbero appartenere le informazioni contenute in ogni libreria dell'applicazione?

Se è possibile rispondere con un ″sì″ a tali domande, si può quindi iniziare a pianificare i gruppi di utenti. Tuttavia, se si è risposto ″a volte″ o ″forse″, potrebbe risultare utile utilizzare un approccio sistematico per identificare i gruppi di utenti.

E' possibile esaminare un esempio di utilizzo di tale approccio per identificare i gruppi di utenti.

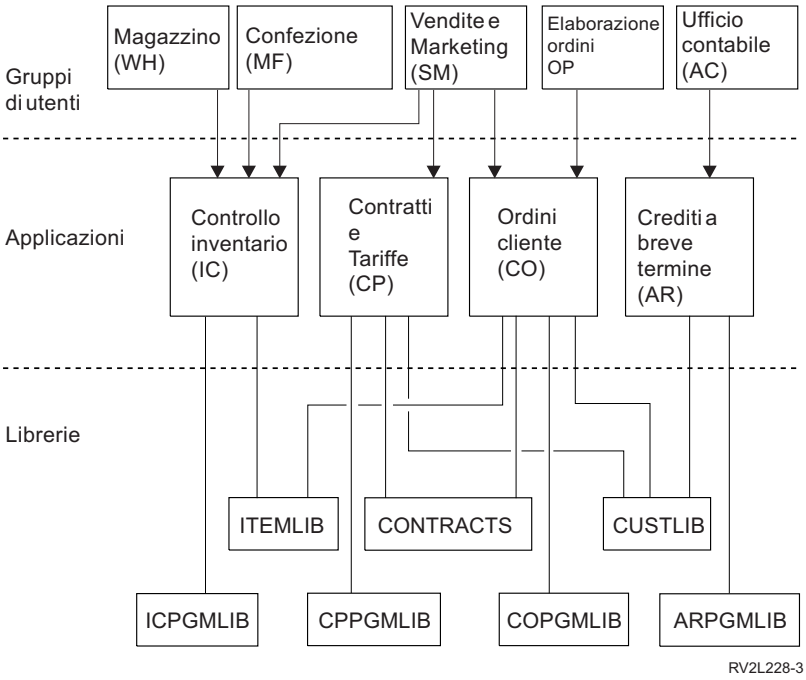
Nota: rendere gli utenti membri di un unico profilo di gruppo consente di semplificare la gestione della sicurezza. In alcune situazioni, tuttavia, può risultare vantaggioso che gli utenti appartengano a più di un profilo di gruppo.

Quando gli utenti appartengono a più di un profilo di gruppo risulta più facile effettuare la gestione piuttosto che conferire molte autorizzazioni riservate ai singoli profili utente.

Esempio: identificare i gruppi di utenti

Se la relazione tra i gruppi di lavoro e le applicazioni appare complicata e vaga, l'utilizzo di una tecnica di matrice come il modulo Identificazione gruppo di utenti consentirebbe di rendere tutto più chiaro. Quando si tracciano su una matrice le esigenze degli utenti del sistema e delle loro applicazioni, ne deriveranno modelli simili. Oltre a riempire il modulo Identificazione gruppo di utenti, Sharon Jones ha utilizzato il proprio diagramma dell'applicazione per identificare quali gruppi di utenti hanno necessità di accedere alle applicazioni.

La seguente illustrazione mostra il diagramma dell'applicazione dell'Azienda di giocattoli JKL.



Se l'approccio alla sicurezza è non rigoroso, utilizzare una X per indicare che un utente necessita di un'applicazione. Se l'approccio alla sicurezza è rigoroso, è necessario considerare in che modo si utilizzano le applicazioni. Invece di inserire una X nella matrice, utilizzare una V (visualizzazione) se si ha solo necessità di consultare le informazioni contenute in un'applicazione. Utilizzare una C (modifica) se si ha necessità di apportare modifiche alle informazioni. Utilizzare una O (proprietario) se si risponde in prima persona delle informazioni.

Ad esempio, nell'Azienda di giocattoli JKL, diversi gruppi necessitano dell'applicazione Contratti e Tariffe:

- Il reparto Vendite e Marketing stabilisce le tariffe e la creazione dei contratti della clientela. Ad essi *appartengono* le informazioni relative alle tariffe ed ai contratti.
- Il reparto Ordini cliente modifica indirettamente le informazioni sui contratti. Quando si elaborano gli ordini, le quantità sui contratti subiscono delle modifiche. Essi hanno necessità di *modificare* le informazioni sulle tariffe e sui contratti.

- Chi elabora gli ordini ha necessità di consultare le informazioni relative alle limitazioni del credito per pianificare il proprio lavoro, ma non gli è consentito di apportarvi modifiche. E' necessario *consultare* il file dei limiti di credito.

Tabella 19. Modulo Identificazione gruppo di utenti dell'Azienda di giocattoli JKL: esempio

Modulo Identificazione gruppo di utenti					
Preparato da: Sharon Jones		Data: 9/2/99			
		Accesso necessario per le applicazioni			
Nome utente	Reparto	APP: CO	APP: IC	APP: PC	APP: AR
Ken H.	Elaborazione ordini (OP)	O	C	C	C
Karen R.	Elaborazione ordini (OP)	O	C	C	C
Kris T.	Ufficio contabile (AC)	V		V	O
Sandy J.	Ufficio contabile (AC)	V	C	V	O
Peter D.	Ufficio contabile (AC)	C		V	O
Ray W.	Magazzino (WH)	V	O	V	
Rose Q.	Magazzino (WH)	V	O	V	
Roger T.	Vendite e Marketing (SM)	C	C	O	C
Sharon J.	Dirigenti (MG)	C	C	C	C

Nota:

- Se l'ambiente della sicurezza è *non rigoroso*, utilizzare una X per contrassegnare le applicazioni di cui necessitano gli utenti.
- Se l'ambiente della sicurezza è *medio*, utilizzare una A per contrassegnare quali utenti avranno l'autorizzazione per quali applicazioni.
- Se l'ambiente della sicurezza è *rigoroso*, potrebbe essere necessario utilizzare C (modifica), V (visualizzazione) e O per specificare *come* si utilizzano le applicazioni.

Sharon Jones ha preso nota delle proprie scelte nell'approntare la matrice:

- L'elaborazione ordini e l'ufficio contabile si forniscono una reciproca copia di riserva. Oggi, richiedono applicazioni simili. Sarebbe necessario, tuttavia, che rimanessero due gruppi separati dal momento che, nel futuro, diventeranno più specializzati man mano che aumenterà il numero dei dipendenti.
- Sebbene non sia consentito all'elaborazione ordini di modificare direttamente l'inventario o i contratti, i saldi dei contratti e degli articoli vengono automaticamente modificati quando si creano e si compilano gli ordini. In seguito diventerà una questione relativa alla sicurezza?
- Il personale Vendite e Marketing è interessato a tutti i settori dell'azienda e a tutte le applicazioni. Stabilisce le tariffe e le descrizioni degli articoli. Si occupa dei nuovi clienti, sebbene l'ufficio contabile stabilisca le limitazioni del credito. E' responsabile dell'impostazione di tutti i termini e delle tariffe dei contratti.

Decidere quali saranno i gruppi di utenti. Compilare il modulo Identificazione gruppo di utenti, se risulta necessario ai fini della scelta.

Dopo aver aggiunto gli utenti al modulo Identificazione gruppo di utenti, è possibile pianificare un profilo di gruppo.

Pianificare un profilo di gruppo

Dopo aver identificato i gruppi di utenti, si è pronti per pianificare un profilo per ogni gruppo. Molte delle scelte effettuate influiscono sia sulla sicurezza che sulla personalizzazione. Ad esempio, quando si

specifica un menu iniziale, è possibile limitare un utente solo a quel menu. Ma è inoltre necessario verificare che l'utente veda visualizzato il menu corretto dopo essersi collegato.

Preparare un modulo Descrizione del gruppo di utenti per un gruppo di utenti in forma di esempio. Dopo aver completato il primo modulo, tornare indietro e completare i moduli per gli altri gruppi necessari.

La sicurezza e la personalizzazione nell'iSeries vengono progettate per essere molto flessibili. Il metodo di pianificazione contenuto in questo argomento fornisce una buona modalità di progettazione dei profili di gruppo e delle descrizioni lavoro, sebbene il programmatore ed il fornitore dell'applicazione potrebbero consigliare un metodo diverso.

Denominare i profili di gruppo

Dal momento che il profilo di gruppo si comporta come un tipo speciale di profilo utente, potrebbe essere necessario identificare facilmente i profili di gruppo su liste e pannelli. E' necessario assegnare loro dei nomi speciali. Per essere visualizzati insieme sulle liste, i profili di gruppo dovrebbero iniziare con gli stessi caratteri, ad esempio `GRP` (per il gruppo) o `DPT` (per il reparto). Utilizzare queste istruzioni durante la denominazione dei gruppi di utenti:

- I nomi dei gruppi di utenti possono essere lunghi fino a 10 caratteri.
- Il nome può includere lettere, numeri e caratteri speciali: cancelletto (#), dollaro ($), carattere di sottolineatura (_) e segno at (@).
- Il nome non può cominciare con un numero.

Nota: per ogni profilo di gruppo, il sistema assegna un numero di identificazione del gruppo (*gid*). Di solito, è possibile che il sistema crei un *gid*. Se si utilizza il sistema in una rete, potrebbe essere necessario assegnare dei gid specifici ai profili di gruppo. Verificare con l'amministratore di rete se sia necessario assegnare dei gid.

E' necessario aggiungere il proprio sistema di denominazione per i profili di gruppo nel relativo campo del modulo Convenzioni di denominazione. Ad esempio, Sharon Jones ha scelto DPT come convenzione di denominazione per i profili di gruppo. Ella ha riempito la relativa sezione del modulo Convenzioni di denominazione.

Tabella 20. Modulo Convenzioni di denominazione dell'Azienda di giocattoli JKL: esempio di profilo di gruppo

Tipo di oggetto	Convenzione di denominazione
Profili di gruppo	Utilizzare i caratteri DPT seguiti dall'abbreviazione del reparto. La descrizione del testo del profilo di gruppo dovrebbe essere il nome del reparto.

Determinare le applicazioni e le librerie necessarie al gruppo di utenti

Se non lo si è già fatto, aggiungere i gruppi di utenti e le librerie al diagramma dell'applicazione precedentemente disegnato. Questa immagine visiva consente di decidere le esigenze della risorsa e dell'applicazione di ogni gruppo.

Nella Parte 1 del modulo Descrizione del gruppo di utenti indicare l'applicazione principale del gruppo, che è l'applicazione maggiormente utilizzata. Elencare le altre applicazioni necessarie per il gruppo.

Fare riferimento al modulo Descrizione dell'applicazione e al diagramma dell'applicazione per vedere le librerie necessarie per ogni gruppo. Consultarsi con il programmatore o con il fornitore dell'applicazione per trovare il miglior metodo che consenta di accedere a queste librerie. La maggior parte delle applicazioni utilizza una di queste tecniche:

- L'applicazione include le librerie contenute nella lista iniziale delle librerie dell'utente.

- L’applicazione esegue un programma di configurazione che colloca le librerie nella lista librerie dell’utente.
- Le librerie non devono necessariamente trovarsi nella lista librerie. I programmi dell’applicazione specificano sempre la libreria.

Il sistema utilizza una lista librerie per trovare i file ed i programmi necessari durante l’esecuzione delle applicazioni. La **lista librerie** è una lista di librerie in cui il sistema cerca gli oggetti necessari all’utente. Consta di due parti:

1. **Parte sistema**: specificata nel valore di sistema QSYSLIBL, la parte sistema viene utilizzata per le librerie OS/400. Non è necessario modificare il valore predefinito per questo valore di sistema.
2. **Parte utente**: il valore di sistema QUSRLIBL fornisce la parte utente della lista librerie. La descrizione lavoro dell’utente specifica la lista iniziale delle librerie o i comandi dopo che l’utente si è collegato. Se si dispone di una lista librerie iniziale, essa sostituisce il valore di sistema QUSRLIBL. Si consiglia di includere le librerie dell’applicazione nella parte utente della lista librerie.

Utilizzare la descrizione lavoro

Quando un utente si collega al sistema, la descrizione lavoro dell’utente definisce molte caratteristiche del lavoro, inclusi il modo in cui si stampa il lavoro, come vengono eseguiti i lavori batch e la lista iniziale delle librerie. Il sistema dispone di una descrizione lavoro, denominata QDFTJOBD, che può essere utilizzata durante la creazione dei profili di gruppo. Tuttavia, QDFTJOBD specifica il valore di sistema QUSRLIBL come lista iniziale delle librerie. Se si desidera che diversi gruppi di utenti abbiano accesso a diverse librerie quando si collegano, è necessario creare descrizioni lavoro univoche per ogni gruppo.

Elencare ogni libreria necessaria al gruppo nel modulo Descrizione del gruppo di utenti. Se la libreria dovesse essere inclusa nella lista iniziale delle librerie della descrizione lavoro del gruppo, indicare ogni nome libreria nel modulo.

E’ possibile esaminare un esempio del modo in cui Sharon Jones ha descritto i propri gruppi di utenti dell’Azienda di giocattoli JKL, prima di iniziare a scegliere i valori che influenzano il collegamento.

Esempio: modulo Descrizione del gruppo di utenti dell’Azienda di giocattoli JKL

La prima tabella mostra la Parte 1 del modulo Descrizione del gruppo di utenti che Sharon Jones ha preparato per il reparto Vendite e Marketing. Tenere presente che lei non include le librerie CONTRACTS e CPPGMLIB nella lista iniziale delle librerie del gruppo. L’applicazione le aggiunge automaticamente alla lista librerie invece di inserirle alla lista iniziale delle librerie DPTSM. Quando un utente esce dall’applicazione, il sistema elimina tali librerie dalla lista librerie. Ciò fornisce una sicurezza aggiuntiva per tali librerie, poiché è possibile accedervi solo tramite i programmi dell’applicazione.

Tabella 21. Modulo Descrizione del gruppo di utenti dell’Azienda di giocattoli JKL: esempio di Informazioni descrittive

Modulo Descrizione del gruppo di utenti	Parte 1 di 2
Preparato da: `Sharon Jones`	Data: `9/5/99`
Nome gruppo di profili: `DPTSM` Descrizione del profilo: `Reparto Vendite e Marketing`	
Applicazione principale per il gruppo: `Contratti e tariffe` Elencare altre applicazioni necessarie per il gruppo: `Inventario (per immettere le descrizioni e le tariffe della voce), Ordini cliente`	

Tabella 21. Modulo Descrizione del gruppo di utenti dell'Azienda di giocattoli JKL: esempio di Informazioni descrittive (Continua)

Elencare ogni libreria necessaria per il gruppo. Contrassegnare (✓) ogni libreria che dovrebbe trovarsi nella lista librerie iniziale del gruppo: • ✓CUSTLIB • ✓ITEMLIB • ✓COPGMLIB • ✓ICPGMLIB • CPPGMLIB • CONTRACTS

Inoltre, Sharon ha avviato il modulo Descrizione del gruppo di utenti per il reparto Magazzino.

Tabella 22. Modulo Descrizione del gruppo di utenti: Informazioni descrittive

Modulo Descrizione del gruppo di utenti	Parte 1 di 2
Preparato da: Sharon Jones	Data: 9/5/99
Nome profilo di gruppo: DPTWH Descrizione del gruppo: Reparto Magazzino	
Applicazione principale per il gruppo: Controllo inventario Elencare le altre applicazioni necessarie per il gruppo: nessuna	
Elencare ogni libreria necessaria per il gruppo. Inserire un segno di spunta (✓) davanti ad ogni libreria nella lista librerie iniziale per il gruppo: • ✓ITEMLIB • ✓ICPGMLIB	

Dopo aver completato la Parte 1 del modulo Descrizione del gruppo di utenti, è possibile iniziare scegliendo valori che influenzano il collegamento.

Scegliere i valori che influenzano il collegamento

Dopo aver pianificato i profili di gruppo nel sistema, è necessario scegliere i valori di sistema che influenzano il collegamento. Inserire le scelte nella Parte 2 del modulo Descrizione del gruppo di utenti. Tenere presente che si scelgono dei valori che verranno copiati per creare dei singoli profili per i membri del gruppo. Iniziare inserendo il nome del profilo di gruppo selezionato ed una breve descrizione (Testo) per il gruppo.

Se si personalizza correttamente il sistema, gli utenti dovranno immettere sul pannello di collegamento solo i propri ID utente e le proprie parole d'ordine. I loro profili utente forniscono gli altri valori di collegamento.

Parola d'ordine

Impostare la parola d'ordine per un profilo di gruppo su *NONE. Ciò impedisce che qualcuno si colleghi utilizzando il profilo di gruppo. Successivamente, durante la copia del profilo di gruppo per creare i singoli profili utente, si imposterà una parola d'ordine per ogni utente.

Programma iniziale e procedura iniziale

Un programma iniziale dell'utente, denominato anche **programma di collegamento**, è in esecuzione prima che il sistema visualizzi il primo menu. Inserire il nome del programma e la relativa libreria nel

profilo di gruppo, anche se la libreria fa parte della lista iniziale delle librerie. Specificandoli entrambi, è possibile verificare che il sistema esegua il programma corretto e non è necessario occuparsi delle modifiche alla lista librerie.

Un programma o una procedura iniziali vengono utilizzati per una di queste ragioni:

- Alcune applicazioni utilizzano un programma iniziale per configurare l'ambiente dell'applicazione.
- Si desidera che un utente esegua solo un programma senza visualizzare mai un menu. Ad esempio, nell'Azienda di giocattoli JKL, chi utilizza la stazione di lavoro sulla piattaforma di caricamento può eseguire solo il programma per la ricezione dell'inventario. Ciò consente di evitare rischi per la sicurezza su una stazione di lavoro collocata in una postazione accessibile.

L'impostazione del campo **Possibilità limitate** di un utente su *YES o *PARTIAL evita che l'utente modifichi il programma iniziale nel pannello di collegamento.

Verificare con il programmatore che le applicazioni richiedano un programma o una procedura iniziale.

Menu iniziale e Libreria Menu iniziale

Il menu iniziale, denominato anche **primo menu**, è il primo menu che l'utente vede visualizzato dopo il collegamento. Il programma iniziale viene eseguito prima della visualizzazione del primo menu. Se il programma iniziale mostra qualche pannello, l'utente vede visualizzati tali pannelli prima che il sistema mostri il menu iniziale.

Di solito, il menu iniziale di un gruppo deve essere il menu principale dell'applicazione principale del gruppo. Specificare il nome del menu e la sua libreria.

Se si imposta il campo **Possibilità limitate** di un utente su *YES, l'utente non può modificare il menu iniziale nel pannello di collegamento. Se si imposta il campo *Possibilità limitate* di un utente su *PARTIAL, l'utente può modificare il menu iniziale nel pannello di collegamento.

Libreria corrente

La libreria corrente è anche denominata **libreria predefinita**. Quando si specifica la libreria corrente per un utente si verifica quanto segue:

- Se un utente crea degli oggetti, ad esempio programmi d'interrogazione, il sistema colloca tali oggetti nella libreria corrente, a meno che l'utente non specifichi una libreria diversa.
- Il sistema aggiunge automaticamente la libreria corrente alla parte utente della lista librerie. E' possibile, ma non necessario, includerla nella lista iniziale delle librerie nella descrizione lavoro.
- La libreria corrente diventa la prima libreria contenuta nella parte utente della lista librerie. Il sistema cerca nella libreria corrente i file ed i programmi prima di cercare nelle librerie contenute nella lista librerie dell'utente.
- Se non si assegna una libreria corrente per un utente, il sistema assegna la libreria QGPL (scopi generali).

Suggerimenti

La libreria corrente è particolarmente importante se si ha intenzione di utilizzare il programma su licenza IBM Query per iSeries o un altro programma simile. Utilizzare uno di questi approcci:

- Creare una libreria condivisibile da ogni membro del gruppo. Inserire tutti i programmi ed i file di interrogazione del gruppo in tale libreria. Assegnarle lo stesso nome del profilo di gruppo e farne la libreria corrente del gruppo.
- Assegnare una libreria personale ad ogni utente che abbia intenzione di utilizzare Query. Assegnare alla libreria lo stesso nome del profilo utente. Specificare tale libreria come libreria corrente nei singoli profili dei membri del gruppo, non nel profilo di gruppo.

Nella Parte 2 del modulo Descrizione utente, compilare le scelte per i campi che influenzano il collegamento.

Dopo aver scelto i valori che influenzano il collegamento, è possibile scegliere i valori che limitano le operazioni consentite all'utente.

Scegliere i valori che limitano le operazioni consentite all'utente

Dopo aver immesso le scelte per i valori che influenzano il collegamento nella Parte 2 del modulo Descrizione del gruppo di utenti, è necessario occuparsi della limitazione delle operazioni consentite all'utente nel sistema. Può risultare utile limitare le operazioni consentite agli utenti per diverse ragioni:

- Impedire che qualcuno utilizzi i comandi CL. Durante il loro utilizzo, infatti, potrebbe esserci il rischio di provocare inavvertitamente dei danni.
- Limitare gli utenti a specifiche applicazioni e funzioni.
- Fornire un ambiente semplice in cui gli utenti non siano confusi da possibilità di scelta superflue.

Molti fattori determinano il numero di operazioni consentite all'utente:

- Progettazione dell'applicazione
- Valori di sistema
- Sicurezza delle risorse
- Profili di gruppo
- Profili utente
- Descrizioni lavoro

Due campi del profilo di gruppo o utente, **Possibilità limitate** e **Classe utente**, determinano in che misura un utente può sostituire le scelte già effettuate.

Possibilità limitate

Il campo **Possibilità limitate** viene denominato **Limitare utilizzo riga comandi**. E' possibile limitare la modifica da parte degli utenti dei valori contenuti nel pannello di collegamento, l'immissione di comandi e la modifica del programma di gestione del tasto attenzione. E' possibile scegliere limitazioni rigorose (*YES), limitazioni medie (*PARTIAL) o nessuna limitazione (*NO). La seguente tabella mostra le operazioni consentite da ciascuno di questi valori:

Tabella 23. Funzioni consentite per i valori di Possibilità limitate

Valore Possibilità limitate	Modificare programma iniziale	Modificare menu iniziale	Modificare libreria corrente	Modificare programma di attenzione	Immettere comandi
*YES	No	No	No	No	Pochi valori[1]
*PARTIAL	No	Sì	No	No	Sì
*NO	Sì	Sì	Sì	Sì	Sì

1 Sono consentiti questi comandi: SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPJOBLOG, e STRPCO. L'utente non può utilizzare F9 per visualizzare una riga comandi da qualunque menu o pannello dell'Operational Assistant.

Classe utente

La classe utente, denominata anche **tipo di utente**, determina quali opzioni vengono visualizzate all'utente nell'Operational Assistant e nei menu di sistema. Determina inoltre quali funzioni di sistema possono essere utilizzate dall'utente, a meno che non si elenchino le autorizzazioni nel campo **Autorizzazione speciale**.

Suggerimenti per le possibilità limitate e la classe utente

La maggior parte degli utenti non necessita o non desidera accedere ai comandi CL o alle funzioni di sistema. I pannelli dell'Operational Assistant forniscono agli utenti sufficienti informazioni e su come controllare il proprio lavoro. Tali suggerimenti consentono agli utenti di accedere solo alle risorse di sistema necessarie per completare le loro attività:

- In ogni profilo di gruppo, impostare il campo **Possibilità limitate** su *YES. Impostare il campo *Classe utente* su *USER.
- Sovrascrivere queste specifiche per i singoli utenti che richiedono le funzioni di sistema.
- Verificare che i menu forniscano un mezzo per spostarsi tra le applicazioni, se gli utenti lo richiedono.

Dopo aver immesso le scelte per la classe utente e le possibilità limitate nella Parte 2 del modulo Descrizione del gruppo di utenti, è possibile scegliere i valori che configurano l'ambiente dell'utente.

Scegliere i valori che configurano l'ambiente dell'utente

Dopo aver immesso le scelte per limitare le operazioni consentite agli utenti sul sistema nella Parte 2 del modulo Descrizione del gruppo di utenti, è possibile scegliere i valori per determinare l'ambiente operativo dell'utente. Molti campi del profilo utente determinano l'ambiente operativo dell'utente: quale stampante utilizzare, dove inviare messaggi, con che priorità eseguire i lavori. Per molti di questi campi, si consiglia l'impostazione predefinita. Nei seguenti paragrafi vengono descritti alcuni campi.

- **Descrizione lavoro e libreria descrizione lavoro**: questi campi del profilo indicano al sistema quale descrizione lavoro utilizzare quando l'utente si collega. La descrizione lavoro contiene la lista iniziale delle librerie. E' necessario che ogni gruppo di utenti disponga di una descrizione lavoro con lo stesso nome del profilo di gruppo. Le descrizioni lavoro vengono generalmente inserite nella libreria QGPL.
- **Unità di stampa e coda di emissione**: ogni emissione di stampa creata dall'utente viene inviata all'unità di stampa elencata nel profilo, a meno che lo specifico lavoro di stampa non la invii ad un'altra stampante. I membri di un gruppo di utenti vengono generalmente collocati insieme e condividono la stessa stampante. E' possibile specificare tale stampante nel profilo di gruppo e copiarla in ogni singolo profilo utente. L'unità di stampa dell'utente è inoltre denominata **stampante predefinita**.

  Una coda di emissione contiene l'emissione di stampa prima che venga stampata. Generalmente, ogni unità di stampa ha la propria coda di emissione con lo stesso nome. E' possibile specificare *DEV per la coda di emissione per segnalare al sistema di utilizzare la coda di emissione dell'unità di stampa.

  Riempire i campi del nome della descrizione lavoro e relativa libreria e della stampante predefinita e coda di emissione nel modulo Descrizione del gruppo di utenti.
- **Impostazione dell'interfaccia dell'Operational Assistant**: alla consegna del sistema, il menu dell'Operational Assistant per tutti gli utenti è il programma di gestione del tasto attenzione. Quando gli utenti premono il tasto Attenzione, si visualizza il menu dell'Operational Assistant (ASSIST). Se i programmi dell'applicazione utilizzano già un diverso programma di gestione del tasto attenzione, è necessario fornire un diverso metodo agli utenti per giungere al menu dell'Operational Assistant:
  - Aggiungere il menu dell'Operational Assistant sotto forma di opzione dai menu dell'applicazione principale, utilizzando `GO ASSIST` o `CALL QEZAST`.
  - Immettere `GO ASSIST` dalla riga comandi.

Se il campo **Possibilità limitate** è impostato su *YES nel profilo utente, l'utente non può utilizzare il comando GO per visualizzare un menu. E' necessario fornire agli utenti dell'Operational Assistant un metodo per accedere al menu ASSIST.

E' possibile esaminare un esempio dei valori scelti da Sharon Jones per il modulo Descrizione del gruppo di utenti dell'Azienda di giocattoli JKL.

Per completare queste fasi di pianificazione, è necessario:

- Completare un modulo Descrizione del gruppo di utenti per ogni gruppo di utenti dell'azienda.

- Descrivere come vengono denominati i gruppi di utenti nel modulo Convenzioni di denominazione.
- Aggiungere i gruppi di utenti al diagramma delle applicazioni e delle librerie.

Dopo aver completato queste attività, è possibile iniziare a pianificare i singoli profili utente.

Esempio: modulo Descrizione del gruppo di utenti dell'Azienda di giocattoli JKL—parte 2

Sharon Jones ha annotato degli appunti sui reparti di Vendita e Marketing e Magazzino quando ha preparato il modulo Descrizione del gruppo di utenti per il personale addetto alle Vendite e al Marketing.

- `Il personale del reparto Vendite e Marketing utilizzeranno spesso IBM Query per iSeries. E' necessario che ogni utente abbia una libreria privata. Il magazzino può avere una libreria di gruppo.`
- `Chi lavora nel magazzino come addetto alla ricezione della merce necessiterà del programma iniziale piuttosto che di un menu iniziale`

Sharon ha preparato la Parte 2 del modulo Descrizione del gruppo di utenti per due reparti.

Tabella 24. Modulo Descrizione del gruppo di utenti dell'Azienda di giocattoli JKL: esempio reparto Vendite e Marketing

Nome campo	Valore consigliato	Scelta
Nome profilo di gruppo (Utente)		DSTSM
Parola d'ordine	*NONE	*NONE
Classe utente (Tipo utente)	*USER	*USER
Libreria corrente (Libreria predefinita)	*uguale al nome profilo di gruppo*	(lasciare uno spazio nel gruppo; completare i singoli profili)
Programma iniziale da richiamare (Programma di collegamento)		
Libreria programma iniziale		
Menu iniziale (Primo menu)		CPMAIN
Libreria menu iniziale		CPMAINLIB
Possibilità limitate (Limitare utilizzo della riga comandi)	*YES	*PARTIAL
Testo (Descrizione utente)		Vendite e marketing
Descrizione lavoro	*uguale al nome profilo di gruppo*	DPTSM
Libreria descrizione lavoro		QGPL
Nome profilo di gruppo (Gruppo di utenti)	*NONE[1]	*NONE
Unità di stampa (Stampante predefinita)		PRT03
Coda di emissione	*DEV	*DEV

Tabella 25. Modulo Descrizione del gruppo di utenti dell'Azienda di giocattoli JKL: esempio reparto Magazzino

Nome campo	Valore consigliato	Scelta
Nome profilo di gruppo (Utente)		DPTWH
Parola d'ordine	*NONE	*NONE
Classe utente (Tipo utente)	*USER	*USER
Ambiente speciale		
Libreria corrente (Libreria predefinita)	*uguale al nome profilo di gruppo*	DPTWH

Tabella 25. Modulo Descrizione del gruppo di utenti dell'Azienda di giocattoli JKL: esempio reparto Magazzino (Continua)

Nome campo	Valore consigliato	Scelta
Programma iniziale da richiamare (Programma di collegamento)		
Libreria programma iniziale		
Menu iniziale (Primo menu)		ICMAIN
Libreria menu iniziale		ICPGMLIB
Possibilità limitate (Limitare utilizzo della riga comandi)	*YES	*YES
Testo (Descrizione utente)		Reparto magazzino
Descrizione lavoro	*uguale al nome profilo di gruppo*	DPTWH
Libreria descrizione lavoro		QGPL
Nome profilo di gruppo (Gruppo di utenti)	*NONE[1]	*NONE
Unità di stampa (Stampante predefinita)		PRT04
Coda di emissione	*DEV	*DEV
1 Il nome profilo di gruppo deve essere *NONE per un profilo di gruppo. Un profilo di gruppo non può essere un membro di un altro gruppo.		

Ora è possibile cominciare la pianificazione dei singoli profili utente.

Pianificare i singoli profili utente

Dopo aver deciso la strategia di sicurezza globale ed aver pianificato i gruppi di utenti, si è ora pronti a pianificare i singoli profili utente.

Quali moduli sono necessari?

Utilizzare questi moduli per pianificare i singoli profili utente:

- Modulo Singolo profilo utente
- Modulo Responsabilità del sistema

Sarà necessario inoltre utilizzare le informazioni contenute nei seguenti moduli già completati:

- Modulo Definizione del gruppo di utenti
- Modulo Convenzioni di denominazione
- Diagramma dell'applicazione

Denominare i profili utente

Il nome del profilo utente indica il modo in cui si viene identificati nel sistema. Immettere il nome del profilo utente nel campo **ID utente** del pannello di collegamento. Ogni lavoro eseguito ed ogni emissione di stampa creata vengono associati al proprio nome profilo 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 di comunicazione limitano l'ID utente a 8 caratteri.

- Un nome del profilo utente può includere lettere, numeri e caratteri speciali: cancelletto (#), dollaro ($), carattere di sottolineatura (_) e segno at (@). Non può iniziare con un numero o un carattere di sottolineatura (_).
- Il sistema non distingue fra lettere maiuscole e minuscole contenute nel nome del profilo utente. Se si immettono caratteri alfabetici minuscoli, il sistema li converte in caratteri maiuscoli.
- I pannelli e le liste utilizzati per gestire i profili utente visualizzano tali profili in ordine alfabetico in base al nome del profilo utente.
- Tutti i profili forniti dalla IBM iniziano con la lettera Q. Per mantenere i profili separati dai profili forniti dalla IBM, evitare di assegnare nomi che iniziano con il carattere Q.

Suggerimenti

Una tecnica per l'assegnazione dei nomi dei profili utente consiste nell'utilizzare i primi 7 caratteri del cognome seguiti dal primo carattere del nome. Qui di seguito vengono riportate le convezioni di denominazione utilizzate da Sharon per i profili utente nell'Azienda di giocattoli JKL:

Tabella 26. Modulo Convenzioni di denominazione dell'Azienda di giocattoli JKL: esempio di profilo utente

Nome utente	Nome profilo utente
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Jones, Sharon	JONESS

Tale metodo consente di ricordare facilmente i nomi dei profili utente. Inoltre, le liste ed i pannelli vengono sistemati in ordine alfabetico per cognome.

Ad esempio, Sharon Jones dell'Azienda di giocattoli JKL ha intenzione di utilizzare questa tecnica di denominazione. Ha compilato la relativa sezione del modulo Convenzioni di denominazione.

Tabella 27. Modulo Convenzioni di denominazione dell'Azienda di giocattoli JKL: esempio di profilo utente

Tipo di oggetto	Convenzione di denominazione
Profili utente	Utilizzare i primi 7 caratteri del cognome dell'utente, seguiti dal primo carattere del nome dell'utente. Le descrizioni del profilo utente saranno cognome, nome.

Descrivere il modo in cui si ha intenzione di denominare i profili utente nel modulo Convenzioni di denominazione, quindi determinare chi sarà responsabile delle funzioni di sistema e scegliere i valori per ogni utente.

Determinare i responsabili delle funzioni di sistema

Durante la pianificazione dei singoli profili utente, è necessario prima di tutto determinare le responsabilità dei singoli soggetti nel sistema. Per mantenere efficiente il funzionamento del sistema, è necessario del personale che esegua regolarmente varie funzioni di gestione e di manutenzione. Il personale addetto a queste attività necessita dell'autorizzazione ad eseguire i comandi e ad effettuare le funzioni di sistema.

Scegliere i valori che limitano le attività consentite ad un utente tratta il modo in cui i campi **Classe utente** e **Possibilità limitate** controllano le funzioni di sistema alle quali un utente può accedere. Di solito, alla maggior parte degli utenti non dovrebbe essere consentito eseguire le funzioni di sistema (impostare la classe utente su *USER e le possibilità limitate su *PARTIAL o *YES). Tuttavia, alcuni utenti necessitano di ulteriore autorizzazione per mantenere efficiente il funzionamento del sistema.

La seguente tabella elenca alcune importanti attività di gestione del sistema. Essa indica inoltre la classe utente e le autorizzazioni speciali che è possibile assegnare a chi detiene tali responsabilità. Questa lista

consente di determinare quali utenti del sistema necessitino di autorizzazioni speciali. Tuttavia, non si propone di essere uno strumento di pianificazione completo per il funzionamento e la manutenzione del sistema. Questa tabella riporta la classe utente e le autorizzazioni speciali che funzionano con la maggior parte dei sistemi. Potrebbe essere necessario assegnare autorizzazioni diverse a seconda del sistema

Quando si assegna una classe utente diversa da *USER nel profilo, l'utente riceve automaticamente una determinata serie di autorizzazioni speciali per eseguire le funzioni di sistema. E' possibile assegnare ad un utente autorizzazioni speciali diverse da quelle specificate nel campo classe utente, sebbene potrebbe non essere necessario.

Tabella 28. Responsabilità del sistema, classe utente e autorizzazione speciale

Funzione di sistema[1]	**Descrizione**	**Classe utente richiesta [2]**	**Autorizzazione speciale richiesta [3]**
Operazioni di sistema	Gestire l'emissione di stampa, rispondere ai messaggi del sistema, monitorare le operazioni di routine, eseguire l'IPL (initial program load).	*SYSOPR	*JOBCTL
Manutenzione del sistema	Eseguire le funzioni di manutenzione del sistema, ad esempio stabilire una pianificazione di ripulitura automatica ed il monitoraggio dell'utilizzo del disco.	*SYSOPR	*JOBCTL
Copia di riserva di sistema	Salvare regolarmente le librerie dell'applicazione, le librerie di sistema e le informazioni sulla sicurezza. Consultare l'argomento Copia di riserva e ripristino dell'Information Center per ulteriori dettagli su queste funzioni.	*SYSOPR	*SAVSYS
Gestione del profilo	Aggiungere nuovi profili utente, mantenere i profili esistenti.	*SECADM	*SECADM
Gestione della sicurezza delle risorse	Mantenere le autorizzazioni agli oggetti presenti nel sistema.	*SECOFR	*ALLOBJ
Manutenzione del programma	Applicare periodiche modifiche al programma (PTF) nelle librerie fornite dalla IBM. Apportare modifiche alle librerie dell'applicazione.	*SECOFR	*ALLOBJ
Controllo della sicurezza	Impostare la funzione di controllo della sicurezza. Determinare quali eventi, utenti ed oggetti è necessario controllare.		*AUDIT [4]
Configurazione del sistema	Aggiungere, modificare e eliminare unità dal sistema.		*IOSYSCFG[5]

Tabella 28. Responsabilità del sistema, classe utente e autorizzazione speciale (Continua)

Funzione di sistema[1]	Descrizione	Classe utente richiesta [2]	Autorizzazione speciale richiesta [3]

1 Impostare il campo Possibilità limitate su *NO per gli utenti con queste responsabilità.

2 Questa è la classe utente minima richiesta. La classe utente fornisce l'autorizzazione per utilizzare i comandi e le opzioni di menu necessari per eseguire la funzione. A seconda della sicurezza delle risorse, potrebbe essere necessaria un'ulteriore autorizzazione all'oggetto.

3 Questa particolare autorizzazione speciale è necessaria per le responsabilità del lavoro. La classe utente potrebbe assegnare ulteriori autorizzazioni speciali.

4 L'autorizzazione speciale *AUDIT non dispone di una classe utente corrispondente. La classe utente *SECOFR include l'autorizzazione speciale *AUDIT. Tuttavia, il revisore probabilmente non necessita di altre funzionalità della classe utente *SECOFR. E' necessario specificare l'autorizzazione speciale *AUDIT per ogni singolo utente che ha necessità di effettuare controlli nel sistema.

5 L'autorizzazione speciale *IOSYSCFG non dispone di una classe utente corrispondente. La classe utente *SECOFR include l'autorizzazione speciale *IOSYSCFG. E' necessario specificare l'autorizzazione speciale *IOSYSCFG solo per i singoli utenti che hanno necessità di configurare il sistema. Essi potranno creare linee, programmi di controllo ed unità o configurare TCP/IP. Tuttavia, l'utente che configura il sistema potrebbe non avere necessità di altre funzionalità della classe utente *SECOFR.

Suggerimenti

Utilizzare la precedente tabella per pianificare chi debba eseguire le funzioni di sistema. Come minimo, è necessario affidare a due persone la gestione della sicurezza del sistema e ad altre due la gestione delle operazioni e della copia di riserva.

Utilizzare il modulo Responsabilità del sistema come strumento di gestione e di controllo del sistema. Tenere traccia di chiunque abbia l'autorizzazione speciale al sistema e del motivo per cui necessiti di tale autorizzazione speciale.

E' possibile esaminare un esempio del modo in cui Sharon Jones abbia determinato le responsabilità degli utenti prima di scegliere i valori per ogni utente.

Esempio: modulo Responsabilità del sistema dell'Azienda di giocattoli JKL

Segue un esempio del modulo Responsabilità del sistema completato da Sharon Jones:

Tabella 29. Modulo Responsabilità del sistema dell'Azienda di giocattoli JKL: esempio

Chi è il responsabile principale della riservatezza? Sharon Jones Chi è il sostituto del responsabile della riservatezza? Ken Harrison			
Nome profilo	Nome utente	Classe	Commenti
JONESS	Sharon Jones	*SECOFR	Sharon è il responsabile principale della riservatezza e l'amministratore del sistema
HARRISOK	Ken Harrison	*SECOFR	Ken è il sostituto di Sharon come amministratore generale del sistema.
JOHNSONS	Sandy Johnson	*SYSOPR	Sandy ha la responsabilità primaria per le operazioni di sistema e la copia di riserva.
ROGERSK	Karen Rogers	*SYSOPR	Karen aiuterà Sandy con le operazioni e la copia di riserva di sistema.
WILLISR	Rose Willis	*SYSOPR	Rose farà funzionare il sistema durante il secondo spostamento.

Dopo aver completato il modulo Responsabilità del sistema, è possibile cominciare a selezionare i valori di sistema per ogni utente.

Scegliere i valori per ogni utente

Dopo aver determinato le responsabilità degli utenti del sistema, è possibile iniziare a scegliere i valori per ogni utente. Grazie alla pianificazione dei profili di gruppo sotto forma di modelli per i singoli profili utente, si è già eseguito gran parte del lavoro. Utilizzare il modulo Singolo profilo utente per assegnare ogni utente al gruppo corretto e per definire in che modo l'utente si distingue dagli altri membri del gruppo. E' necessario completare un modulo Singolo profilo utente per un gruppo di utenti come esempio, quindi tornare indietro e preparare i moduli Singolo profilo utente per ogni ulteriore gruppo di utenti.

Inserire il nome del profilo di gruppo e le altre informazioni descrittive nella parte superiore del modulo Singolo profilo utente.

Esempio: informazioni descrittive del modulo Singolo profilo utente dell'Azienda di giocattoli JKL

Qui di seguito è riportato il modo in cui Sharon Jones ha riempito la parte superiore del modulo Singolo profilo utente.

Tabella 30. Modulo Singolo profilo utente dell'Azienda di giocattoli JKL: esempio di informazioni descrittive

Modulo Singolo profilo utente	
Preparato da: Sharon Jones	Data: 9/5/99
Nomi del profilo di gruppo: DPTOP	
Proprietario degli oggetti creati:	Autorizzazione di gruppo agli oggetti creati:
Tipo di autorizzazione di gruppo:	

Determinare i valori per i membri del gruppo

Nel modulo Singolo profilo utente trascrivere il nome del profilo e la descrizione (nome utente) di ogni membro del gruppo. I seguenti paragrafi descrivono il modo in cui determinare gli altri valori per ogni membro del gruppo.

Tenere presente che il profilo di gruppo costituisce un modello per i singoli profili utente. Nel modulo Singolo profilo utente è necessario specificare solo ciò che differisce dal gruppo.

- **Assegnazione delle parole d'ordine**: il modo più facile per assegnare le parole d'ordine iniziali agli utenti consiste nell'utilizzare la stessa parola d'ordine del nome del profilo. E' quindi possibile richiedere di modificare la parola d'ordine la prima volta che l'utente si collega impostando la scadenza della parola d'ordine. Nell'argomento Impostare la scadenza della parola d'ordine viene spiegato come eseguire automaticamente tale operazione durante la copia del profilo di gruppo. Se si ha intenzione di farlo, non è necessario elencare le parole d'ordine nel modulo Singolo profilo utente.
- **Classe utente e Possibilità limitate**: esaminare il modulo Responsabilità del sistema per capire quali membri di ogni gruppo necessitano di un valore diverso per i campi **Classe utente** e **Possibilità limitate**. Immettere le informazioni appropriate nel modulo Singolo profilo utente per chiunque necessiti di valori diversi da quelli del profilo di gruppo.
- **Specifica degli altri valori**: verificare se un utente particolare necessita di valori diversi da quelli specificati nel modulo Descrizione del gruppo di utenti per il gruppo. Nel modulo Descrizione del gruppo di utenti, i campi **Classe utente** e **Possibilità limitate** vengono elencati nella parte superiore, poiché i loro valori spesso potrebbero differire per qualche membro del gruppo. Elencare ogni altro campo diverso per i membri del gruppo con il quale si sta lavorando.

Per completare questa fase di pianificazione, verificare di aver:

- Completato il modulo Selezione valori di sistema.

- Descritto il modo in cui pianificare la denominazione dei profili utente nel modulo Convenzioni di denominazione.
- Preparato un modulo Singolo profilo utente per ogni gruppo di utenti dell'azienda.

E' possibile esaminare un esempio delle informazioni utilizzate da Sharon per i singoli utenti prima di pianificare la sicurezza delle risorse

Esempio: modulo Singolo profilo utente dell'Azienda di giocattoli JKL

Nell'Azienda di giocattoli JKL, chi lavora nella piattaforma di carico può eseguire un solo programma. Sharon ha limitato questi utenti a poche funzioni perché lavorano in un'area in cui il pubblico può accedere facilmente alle stazioni di lavoro. Questi membri del reparto Magazzino hanno un programma iniziale e nessuno menu iniziale. Il reparto Elaborazione ordini ha due stampanti locali e una in un ufficio vendite distaccato. Tuttavia, Sharon ha assegnato ad alcuni utenti una stampante differente da quella del gruppo.

Di seguito viene riportato un modulo Singolo profilo utente che Sharon Jones ha completato per il reparto Magazzino e Elaborazione ordini nell'Azienda di giocattoli JKL. Tenere presente che lei ha inserito i dati nei campi solo quando erano diversi dai valori impostati nel profilo di gruppo.

Tabella 31. Modulo Singolo profilo utente dell'Azienda di giocattoli JKL: esempio di reparto Magazzino

Nomi profilo di gruppo: DPTWH					
Creare una voce per ogni membro del gruppo:					
Profilo utente	**Testo (descrizione)**	**Classe utente**	**Possibilità limitate**	**Programma iniziale/Libreria**	**Menu iniziale/Libreria**
WILLISR	Willis, Rose	*SYSOPR	*NO		
WAGNERR	Wagner, Ray			ICRCPT/ICPGMLIB	nessuno
AMESJ	Ames, Janice			ICRCPT/ICPGMLIB	nessuno
FOSSJ	Foss, Julie				
WOODBURC	Woodburt, Carol				

Tabella 32. Modulo Singolo profilo utente: esempio reparto Elaborazione ordini

Nomi del profilo di gruppo: DPTOP				
Creare una voce per ogni membro del gruppo:				
Profilo utente	**Testo (descrizione)**	**Classe utente**	**Possibilità limitate**	**Unità di stampa**
HARRISOK	Harrison, Ken	*SECOFR	*NO	PRT05
RICHARDK	Richards, Karen			
UNGERJ	Unger, Jeff			PRT04
BELLB	Bell, Brad			PRT04

In seguito è possibile cominciare con la pianificazione della sicurezza delle risorse.

Capitolo 5. Pianificare la sicurezza delle risorse

Una volta completato il processo di pianificazione degli utenti presenti nel sistema, è possibile pianificare la sicurezza delle risorse che protegge gli oggetti nel sistema. Nella sezione ″Impostare la sicurezza delle risorse,″ si impara in che modo impostare la sicurezza delle risorse nel sistema.

I valori di sistema ed i profili degli utenti controllano chi ha accesso al sistema ed impediscono a utenti non autorizzati di collegarsi. La sicurezza delle risorse controlla le operazioni che gli utenti autorizzati del sistema possono eseguire una volta collegati. La sicurezza delle risorse supporta i principali obiettivi di sicurezza sul sistema per proteggere:

- la riservatezza delle informazioni
- la precisione delle informazioni per impedire modifiche non autorizzate
- la disponibilità delle informazioni per impedire danni accidentali o intenzionali

E' possibile pianificare la sicurezza delle risorse in diversi modi, a seconda che l'azienda sviluppi le applicazioni o le acquisti. Nel caso di applicazioni sviluppate, si consiglia di comunicare al programmatore i requisiti di sicurezza delle informazioni durante il processo di progettazione dell'applicazione. Nel caso di applicazioni acquistate, è necessario determinare le esigenze di sicurezza e farle corrispondere alla modalità con cui il fornitore ha progettato le applicazioni. Le tecniche qui descritte risulteranno utili in entrambi i casi.

Questo argomento fornisce un approccio di base per la pianificazione della sicurezza delle risorse. Esso introduce le principali tecniche e mostra le modalità con cui è possibile utilizzarle. I metodi qui descritti non funzioneranno necessariamente per ogni società e per ogni applicazione. Per la pianificazione della sicurezza delle risorse, consultare il programmatore o il fornitore dell'applicazione.

Esaminare questi argomenti per suggerimenti sulla pianificazione della sicurezza delle risorse:

- Determinare gli obiettivi per la sicurezza delle risorse
- Conoscere i tipi di autorizzazione
- Pianificare la sicurezza per le librerie dell'applicazione
- Determinare la proprietà delle librerie e degli oggetti
- Raggruppare gli oggetti
- Proteggere l'emissione di stampa
- Proteggere le stazioni di lavoro
- Riepilogo dei suggerimenti sulla sicurezza delle risorse
- Pianificare l'installazione dell'applicazione

Quali moduli sono necessari?

Effettuare delle copie dei seguenti moduli e compilarli secondo quanto indicato nel presente argomento. Effettuare l'intero processo per un'applicazione, quindi ripeterlo per ogni ulteriore applicazione.

Tabella 33. Moduli di pianificazione necessari per pianificare la sicurezza delle risorse

Nome modulo	Numero di copie necessarie
Modulo Lista di autorizzazioni	Varie
Modulo Sicurezza dell'emissione di stampa e della stazione di lavoro	Uno

Aggiungere informazioni ai seguenti moduli, con cui si è lavorato in precedenza:

Tabella 34. Moduli di pianificazione da modificare

Nome modulo	Pronto in
Modulo Descrizione della libreria	Descrivere le informazioni sulla libreria
Modulo Descrizione del gruppo di utenti	Pianificare profili di gruppo

Fare riferimento a questi moduli precedentemente preparati:

Tabella 35. Moduli di pianificazione necessari per completare la sicurezza delle risorse

Nome modulo	Pronto in:
Modulo Descrizione della libreria	Disegnare il diagramma dell'applicazione e Identificare i gruppi di utenti
Modulo Descrizione dell'applicazione	Descrivere le informazioni sulle applicazioni
Modulo Singolo profilo utente	Scegliere i valori per ogni utente
Modulo Identificazione gruppo di utenti	Identificare i gruppi di utenti
Modulo Responsabilità del sistema	Determinare i responsabili delle funzioni di sistema
Modulo Pianificazione sicurezza fisica	Pianificare la sicurezza fisica

Determinare gli obiettivi per la sicurezza delle risorse

Per iniziare a pianificare la sicurezza delle risorse, è necessario prima di tutto conoscere gli obiettivi. iSeries fornisce un'implementazione flessibile della sicurezza delle risorse. Offre la possibilità di proteggere le risorse più importanti esattamente nella maniera desiderata. La sicurezza delle risorse, tuttavia, comporta anche un ulteriore sovraccarico per le applicazioni. Ad esempio, ogni qualvolta un'applicazione richieda un oggetto, il sistema deve verificare l'autorizzazione dell'utente per tale oggetto. E' necessario valutare l'esigenza di riservatezza rispetto al costo delle prestazioni. Se si sceglie la sicurezza delle risorse, considerare il valore della sicurezza rispetto ai costi.

Per evitare che la sicurezza delle risorse comprometta le prestazioni delle applicazioni, seguire queste istruzioni.

- Avvalersi di uno schema semplice per la sicurezza delle risorse.
- Proteggere soltanto gli oggetti che è necessario preservare.
- Utilizzare la sicurezza delle risorse ad integrazione, e non in sostituzione, degli altri strumenti per la protezione delle informazioni, ad esempio:
  - Limitando gli utenti a menu ed applicazioni specifici.
  - Impedendo agli utenti di immettere determinati comandi (possibilità limitate nei profili utente).

Iniziare la pianificazione della sicurezza delle risorse definendo gli obiettivi. E' possibile definire gli obiettivi di sicurezza nel modulo Descrizione dell'applicazione oppure nel modulo Descrizione della libreria.

Il modulo utilizzato dipende dal modo in cui le informazioni sono organizzate nelle librerie.

Se lo si desidera, è possibile visionare un esempio di obiettivi di sicurezza dell'Azienda di giocattoli JKL prima di esaminare i tipi di autorizzazioni che è possibile utilizzare per la sicurezza delle risorse.

Esempio: obiettivi di sicurezza dell'Azienda di giocattoli JKL

Sharon Jones nell'Azienda di giocattoli JKL ha utilizzato il modulo Descrizione della libreria per descrivere i requisiti della sicurezza per la libreria Record cliente (CUSTLIB):

Tabella 36. Modulo Descrizione della libreria dell'Azienda di giocattoli JKL: esempio di obiettivi di sicurezza

Modulo Descrizione della libreria	Parte 1 di 2
Definire gli obiettivi della sicurezza per la libreria, ad esempio se le informazioni sono riservate:	Oggi, chiunque lavori nell'azienda può avere accesso alle informazioni sui clienti e agli ordini dei clienti. Per proteggere l'accuratezza delle informazioni, è necessario controllare chi può modificare tali informazioni.

Sharon ha utilizzato il modulo Descrizione dell'applicazione per l'applicazione Contratti e Tariffe per descrivere gli obiettivi sulla sicurezza per l'intera applicazione.

Tabella 37. Modulo Descrizione dell'applicazione dell'Azienda di giocattoli JKL: esempio degli obiettivi della sicurezza

Modulo Descrizione dell'applicazione	Parte 1 di 2
Definire gli obiettivi della sicurezza per la libreria, ad esempio se le informazioni sono riservate:	Le informazioni relative ai contratti e alle tariffe speciali sono riservate. Solo pochi utenti sono autorizzati a visualizzarle o modificarle: • Il personale addetto alle Vendite e al Marketing e tutti i dirigenti devono poter creare, modificare ed analizzare i contratti. Devono poter utilizzare i file e i programmi. • Il personale addetto all'Elaborazione ordini modifica i contratti e visualizza le tariffe indirettamente nel momento in cui vengono immessi o inviati gli ordini. Essi non possono avere accesso ai contratti e ai prezzi se non nel momento in cui immettono o modificano un ordine.

Scrivere gli obiettivi della sicurezza per un'applicazione nel modulo Descrizione dell'applicazione o nel modulo Descrizione della libreria. E' possibile inoltre visualizzare nuovamente i tipi di autorizzazioni che possono essere utilizzati per pianificare la sicurezza delle risorse.

Conoscere i tipi di autorizzazione

Dopo aver determinato gli obiettivi per la sicurezza delle risorse ed aver registrato le scelte nel modulo Descrizione della libreria, è possibile iniziare a pianificare i tipi di autorizzazione. La sicurezza delle risorse definisce il modo in cui gli utenti hanno accesso agli oggetti presenti nel sistema.

Autorizzazione indica il modo in cui si è autorizzati ad utilizzare un oggetto. Ad esempio, è possibile che si sia autorizzati a visionare delle informazioni o a modificare le informazioni presenti nel sistema. Il sistema fornisce diversi tipi di autorizzazione. L'IBM raggruppa questi tipi di autorizzazione in categorie, denominate **autorizzazioni definite dal sistema**, che sono in grado di soddisfare le esigenze della maggior parte degli utenti. La seguente tabella elenca le categorie e spiega in che modo si applicano alla protezione dei file e dei programmi.

Nota: durante la pianificazione delle autorizzazioni, fare riferimento alle seguenti tabelle.

Tabella 38. Autorizzazioni definite dal sistema

Nome autorizzazione	Operazioni consentite per i file	Operazioni non consentite per i file	Operazioni consentite per i programmi	Operazioni non consentite per i programmi
*USE	Visualizzare le informazioni nel file.	Modificare o cancellare tutte le informazioni nel file. Cancellare il file.	Eseguire il programma.	Modificare o cancellare il programma.

Tabella 38. Autorizzazioni definite dal sistema (Continua)

Nome autorizzazione	Operazioni consentite per i file	Operazioni non consentite per i file	Operazioni consentite per i programmi	Operazioni non consentite per i programmi
*CHANGE	Visualizzare, modificare e cancellare i record nel file.	Cancellare o eliminare il contenuto dell'intero file.	Modificare la descrizione del programma.	Modificare o cancellare il programma.
*ALL	Creare e cancellare il file. Aggiungere, modificare e cancellare i record nel file. Autorizzare altri utenti ad utilizzare il file.	Nessuna	Creare, modificare e cancellare il programma. Autorizzare altri utenti ad utilizzare il programma.	Modificare il proprietario del programma, se il programma adotta l'autorizzazione.
*EXCLUDE[1]	Nessuna	Ogni accesso al file.	Nessuna	Ogni accesso al programma.
1 *EXCLUDE sostituisce ogni autorizzazione concessa al pubblico o tramite un profilo di gruppo.				

Comprendere le modalità di funzionamento congiunto dell'autorizzazione all'oggetto e dell'autorizzazione alla libreria

Per progettare una sicurezza delle risorse di base, provare a pianificare la sicurezza per tutte le librerie. Per effettuare ciò, è necessario comprendere in che modo le autorizzazioni definite dal sistema si applicano alle librerie, come mostrato nella seguente tabella:

Tabella 39. Autorizzazioni definite dal sistema per le librerie

Nome autorizzazione	Operazioni consentite	Operazioni non consentite
*USE	• Per gli oggetti presenti nella libreria, ogni operazione consentita dall'autorizzazione all'oggetto specifico. • Per la libreria, esaminare le informazioni descrittive.	• Aggiungere nuovi oggetti alla libreria. • Modificare la descrizione della libreria. • Cancellare la libreria.
*CHANGE	• Per gli oggetti presenti nella libreria, ogni operazione consentita dall'autorizzazione all'oggetto specifico. • Aggiungere nuovi oggetti alla libreria. • Modificare la descrizione della libreria.	• Cancellare la libreria.
*ALL	• Tutto ciò che è consentito modificare. • Cancellare la libreria. • Autorizzare altri utenti ad utilizzare la libreria.	• Nessuna

E' inoltre necessario comprendere le modalità di funzionamento congiunto dell'autorizzazione alla libreria e all'oggetto. La seguente tabella fornisce degli esempi di autorizzazione necessarie sia per l'oggetto che per la libreria:

Tabella 40. Modalità di funzionamento congiunto dell'autorizzazione alla libreria e dell'autorizzazione all'oggetto

Tipo oggetto	Operazioni	Autorizzazione all'oggetto necessaria	Autorizzazione alla libreria necessaria
File	Modificare i dati	*CHANGE	*USE
File	Cancellare il file	*ALL	*USE
File	Creare il file	*ALL	*CHANGE
Programma	Eseguire il programma	*USE	*USE
Programma	Modificare (ricompilare) il programma	*ALL	*CHANGE
Programma	Cancellare il programma	*ALL	*USE

L'autorizzazione all'indirizzario è simile all'autorizzazione alla libreria. Per accedere all'oggetto è necessaria l'autorizzazione a tutti gli indirizzari presenti nel nome percorso di un oggetto.

Si è ora pronti per pianificare la sicurezza delle librerie dell'applicazione.

Pianificare la sicurezza per le librerie dell'applicazione

Dopo aver determinato gli obiettivi della sicurezza delle risorse, è possibile iniziare a pianificare la sicurezza delle librerie dell'applicazione. Scegliere una delle librerie dell'applicazione con cui lavorare quando si segue il processo qui descritto. Se il sistema memorizza i file ed i programmi in librerie separate, scegliere una libreria che contenga i file. Al termine dell'argomento, ripetere queste operazioni per le restanti librerie dell'applicazione.

Esaminare le informazioni raccolte relative alle applicazioni ed alle librerie:

- Modulo Descrizione dell'applicazione
- Modulo Descrizione della libreria
- Modulo Descrizione del gruppo di utenti per tutti i gruppi che necessitano della libreria
- Diagramma di applicazioni, librerie e gruppi di utenti

Considerare quali gruppi richiedono le informazioni contenute in una libreria, il motivo della richiesta e il loro futuro utilizzo.

Determinare il contenuto della libreria

Le librerie dell'applicazione contengono importanti file dell'applicazione. Esse possono inoltre contenere altri oggetti, la maggior parte dei quali sono strumenti di programmazione per il corretto funzionamento dell'applicazione, ad esempio:

- File di lavoro
- Aree dati e code messaggi
- Programmi
- File di messaggio
- Comandi
- Code di emissione

La maggior parte degli oggetti, diversi dai file e dalle code di emissione, non costituiscono un rischio per la sicurezza. Essi contengono generalmente piccole quantità di dati dell'applicazione, spesso in un formato non facilmente intelligibile al di fuori dei programmi. E' possibile elencare i nomi e le descrizioni di tutti gli oggetti presenti in una libreria utilizzando il comando Visualizzazione libreria. Ad esempio, per elencare il contenuto della libreria CONTRACTS: `DSPLIB LIB(CONTRACTS) OUTPUT(*PRINT)`

In seguito è necessario decidere quale autorizzazione pubblica si desidera disporre per le librerie dell'applicazione e le librerie di programma.

Scegliere l'autorizzazione pubblica per le librerie dell'applicazione

In relazione alla sicurezza delle risorse, **pubblico** indica chiunque sia autorizzato a collegarsi al sistema. **L'autorizzazione pubblica** consente ad un utente di accedere ad un oggetto nel caso in cui non disponga di un altro accesso più specifico. Oltre a scegliere l'autorizzazione pubblica per oggetti già presenti nella libreria, è possibile specificare l'autorizzazione pubblica per ogni nuovo oggetto successivamente aggiunto alla libreria. Per effettuare ciò, si utilizza il parametro **CRTAUT (Creazione autorizzazione)**. Generalmente, l'autorizzazione pubblica agli oggetti della libreria e l'autorizzazione creazione libreria per i nuovi oggetti dovrebbe essere la stessa.

Il valore di sistema QCRTAUT (Creazione autorizzazione) determina l'autorizzazione pubblica per i nuovi oggetti su tutto il sistema. L'IBM fornisce il valore di sistema QCRTAUT con *CHANGE. Evitare di modificare QCRTAUT, poiché molte funzioni di sistema lo utilizzano. Se si specifica *SYSVAL per CRTAUT (Creazione autorizzazione) di una libreria dell'applicazione, esso utilizzerà il valore di sistema QCRTAUT (*CHANGE).

Utilizzare il più possibile l'autorizzazione pubblica, per questioni di semplicità e per ottenere buone prestazioni. Porsi le seguenti domande al fine di determinare l'autorizzazione pubblica per una libreria:

- E' consigliabile che tutti i dipendenti dell'azienda abbiano accesso alla maggior parte delle informazioni contenute in questa libreria?
- Quale tipo di accesso alla maggior parte delle informazioni contenute in questa libreria dovrebbero avere le persone?

Soffermarsi sulle scelte relative alla maggior parte delle persone ed alla maggior parte delle informazioni. Successivamente si imparerà in che modo gestire le eccezioni. Spesso la pianificazione della sicurezza delle risorse è un processo circolare. E' possibile che sia necessario modificare l'autorizzazione pubblica dopo aver esaminato i requisiti degli specifici oggetti. Tentare diverse combinazioni dell'autorizzazione pubblica e privata sia agli oggetti che per le librerie prima di sceglierne una che soddisfi le proprie esigenze di sicurezza e di prestazioni.

Verificare l'autorizzazione adeguata

L'autorizzazione *CHANGE agli oggetti e l'autorizzazione *USE ad una libreria risultano adatte per la maggior parte delle funzioni dell'applicazione. E' tuttavia necessario porre alcune domande al programmatore o al fornitore dell'applicazione per determinare se alcune funzioni dell'applicazione necessitano di un'ulteriore autorizzazione:

- Durante l'elaborazione vengono cancellati alcuni file o altri oggetti contenuti nella libreria? Vengono eliminati dei file? Vengono aggiunti dei membri ai file? La cancellazione di un oggetto, l'eliminazione di un file o l'aggiunta di un membro del file richiede l'autorizzazione *ALL all'oggetto.
- Durante l'elaborazione vengono creati dei file o altri oggetti nella libreria? La creazione di un oggetto richiede l'autorizzazione *CHANGE alla libreria.

E' possibile esaminare un esempio delle scelte fatte da Sharon per le autorizzazioni agli oggetti prima di stabilire l'autorizzazione pubblica alle librerie programmi.

Esempio: modulo Descrizione della libreria dell'Azienda di giocattoli JKL

Sharon Jones ha rivisto gli obiettivi della sicurezza per la libreria Record cliente, oltre alle informazioni sulle applicazioni e sui reparti che utilizzano le informazioni sul cliente. Ha annotato le seguenti conclusioni:

- Ogni reparto, ad eccezione dei reparti Magazzino e Confezione, necessita di modificare le informazioni sul cliente.

- Tutti gli utenti nei reparti Magazzino e Confezione hanno profili utente con Possibilità limitate (Sì) e sono limitati a determinati menu e programmi. I menu gli consentono di visualizzare le informazioni sul cliente, ma non di modificarle.
- L'autorizzazione pubblica per gli oggetti nella libreria Record cliente può essere impostata su *CHANGE. Le limitazioni del menu impediscono ai non autorizzati di modificare le informazioni sul cliente. Tuttavia, ciò deve essere valutato nuovamente se successivamente altri reparti vengono aggiunti al sistema.

Questo è un esempio di un approccio non rigoroso alle informazioni. In questo caso, le eccezioni vengono gestite tramite profili utente, piuttosto che utilizzando le limitazioni all'autorizzazione. Sharon ha completato la parte dell'autorizzazione pubblica del modulo Descrizione della libreria per la libreria Record cliente (CUSTLIB).

Tabella 41. Modulo Descrizione della libreria dell'Azienda di giocattoli JKL—Parte 1: esempio Record cliente

Nome libreria: CUSTLIB	Nome descrittivo (testo): Record cliente
Autorizzazione pubblica alla libreria:	*USE
Autorizzazione pubblica agli oggetti nella libreria:	*CHANGE
Autorizzazione pubblica per i nuovi oggetti (CRTAUT):	*CHANGE

Sharon Jones ha scoperto che alcuni file temporanei nella libreria Record cliente sono stati eliminati durante l'elaborazione di fine mese dell'applicazione Crediti a breve termine. Ha scelto di gestire l'autorizzazione per quei file singolarmente, piuttosto che correre il rischio che altri oggetti nella libreria venissero cancellati accidentalmente. Per tutte le attività di elaborazione, è sufficiente l'autorizzazione *CHANGE.

Anche se solo poche persone eseguono l'elaborazione di fine mese, Sharon non pensava che i file temporanei potessero porre dei rischi di sicurezza. Lei ha deciso di fornire l'autorizzazione pubblica *ALL a quei file, piuttosto che fornire quell'autorizzazione solo alle persone che eseguono l'elaborazione di fine mese. La tabella che segue mostra la seconda parte del modulo Descrizione della libreria per la libreria Record cliente:

Tabella 42. Modulo Descrizione della libreria dell'Azienda di giocattoli JKL—Parte 2: esempio Record cliente

Elencare le autorizzazioni specifiche per gli oggetti della libreria				
Profilo di gruppo o profilo utente	Nome oggetto	Tipo oggetto	Autorizzazione necessaria	Lista di autorizzazioni
PUBLIC	ARFILE01	*FILE	*ALL	
PUBLIC	ARFILE02	*FILE	*ALL	
PUBLIC	ARFILE03	*FILE	*ALL	

E' possibile ora stabilire l'autorizzazione pubblica alle librerie del programma che si desidera avere.

Scegliere l'autorizzazione pubblica per le librerie di programma

Spesso, i programmi dell'applicazione vengono collocati in un libreria separata dai file e dagli altri oggetti. Non è necessario utilizzare delle librerie separate per le applicazioni, ma molti programmatori utilizzano questa tecnica durante la progettazione delle applicazioni. Se l'applicazione dispone di librerie di programma separate, è necessario decidere l'autorizzazione pubblica a tali librerie. E' possibile utilizzare l'autorizzazione *USE sia per la libreria che per i programmi contenuti nella libreria per eseguire i programmi in modo adeguato, tuttavia le librerie di programma potrebbero contenere altri oggetti che richiedono un'altra autorizzazione. Porre alcune domande al programmatore:

- L’applicazione utilizza aree di dati o code di messaggi per la comunicazione tra programmi? Queste ultime si trovano nella libreria di programma? L’autorizzazione *CHANGE all’oggetto è necessaria per la gestione delle aree di dati e per le code di messaggi.
- Nella libreria di programma sono presenti degli oggetti, ad esempio aree di dati, cancellati durante l’elaborazione? L’autorizzazione *ALL ad un oggetto è necessaria per cancellare l’oggetto.
- Nella libreria di programma sono presenti degli oggetti, ad esempio aree di dati, creati durante l’elaborazione? L’autorizzazione *CHANGE relativa alla libreria è necessaria per creare nuovi oggetti nella libreria.

Inserire tutte le informazioni relative alla sicurezza delle risorse su entrambe le parti del modulo Descrizione della libreria eccetto il proprietario della libreria e la colonna della lista delle autorizzazioni. E’ dunque possibile determinare il proprietario delle librerie e degli oggetti.

E’ possibile esaminare i due seguenti esempi relativi al modo in cui Sharon Jones abbia determinato l’autorizzazione alle librerie di programma. Nel primo esempio, Sharon ha stabilito che un approccio non rigoroso fosse adatto per la libreria di programma Ordini cliente. Il secondo esempio mostra un approccio più rigoroso utilizzato da Sharon per la libreria del programma Crediti a breve termine.

Esempio: modulo Descrizione della libreria dell’Azienda di giocattoli JKL—approccio non restrittivo

Sharon Jones ha esaminato la libreria di programma Ordini cliente e ha annotato le seguenti informazioni:

- `Viene utilizzata una coda messaggi, COMSGQ01, per la comunicazione tra i programmi.`
- `Viene eliminato il contenuto della coda messaggi ma non viene mai cancellata. L'autorizzazione *CHANGE alla coda messaggi è sufficiente`

Sharon ha deciso di fornire l’autorizzazione *USE a tutti gli oggetti nella libreria di programma e di definire la coda messaggi COMSGQ01 separatamente. Le due tabelle che seguono mostrano il suo modulo Descrizione della libreria per la libreria COPGMLIB:

Tabella 43. Modulo Descrizione della libreria dell’Azienda di giocattoli JKL: esempio libreria di programma

Modulo Descrizione della libreria	**Parte 1 di 2**
Nome libreria: `COPGMLIB`	Nome descrittivo (testo): `Libreria di programma Ordini cliente`
Autorizzazione pubblica alla libreria: `*USE` Autorizzazione pubblica agli oggetti nella libreria: `*USE` Autorizzazione pubblica per i nuovi oggetti (CRTAUT): `*USE` Proprietario libreria:	

Tabella 44. Modulo Descrizione della libreria dell’Azienda di giocattoli JKL: esempio libreria di programma

Modulo Descrizione della libreria				**Parte 2 di 2**
Elencare le autorizzazioni ai singoli oggetti nella libreria				
Profilo di gruppo e profilo utente	Nome oggetto	Tipo oggetto	Autorizzazione necessaria	Liste di autorizzazioni
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

Utilizzare l’autorizzazione ad un programma per controllare l’accesso

Sebbene molte persone nell’Azienda di giocattoli JKL abbiano l’autorizzazione a modificare le informazioni sul cliente, solo pochi di loro possono impostare limiti di credito per i clienti. I limiti di credito vengono memorizzati nel file principale del cliente (CUSTMAS), ma vengono modificati con un programma separato

chiamato ARPGM12 in ARPGMLIB. Sharon può limitare tale programma per impedire ai non autorizzati di modificare i limiti di credito. Le tabelle riportate di seguito mostrano il modulo Descrizione della libreria per ARPGMLIB:

Tabella 45. Modulo Descrizione della libreria dell'Azienda di giocattoli JKL: esempio di singola autorizzazione

Modulo Descrizione della libreria	**Parte 1 di 2**
Nome libreria: ARPGMLIB	Nome descrittivo (testo): Libreria di programma Crediti a breve termine
Autorizzazione pubblica alla libreria: *USE Autorizzazione pubblica agli oggetti nella libreria: *USE Autorizzazione pubblica per i nuovi oggetti (CRTAUT): *USE Proprietario libreria:	

Tabella 46. Modulo Descrizione della libreria dell'Azienda di giocattoli JKL: esempio di singola autorizzazione

Modulo Descrizione della libreria				**Parte 2 di 2**
Elencare le autorizzazioni ai singoli oggetti nella libreria				
Profilo di gruppo e profilo utente	Nome oggetto	Tipo oggetto	Autorizzazione necessaria	Liste di autorizzazioni
PUBLIC	ARPGM12	*PGM	*EXCLUDE	
JACOBS	ARPGM12	*PGM	*USE	
DAVISP	ARPGM12	*PGM	*USE	
SMITHJ	ARPGM12	*PGM	*USE	

E' possibile che si desideri rivedere un esempio restrittivo che utilizzi l'autorizzazione prima di cominciare a determinare la proprietà delle librerie e degli oggetti.

Esempio: modulo Descrizione della libreria dell'Azienda di giocattoli JKL—approccio restrittivo

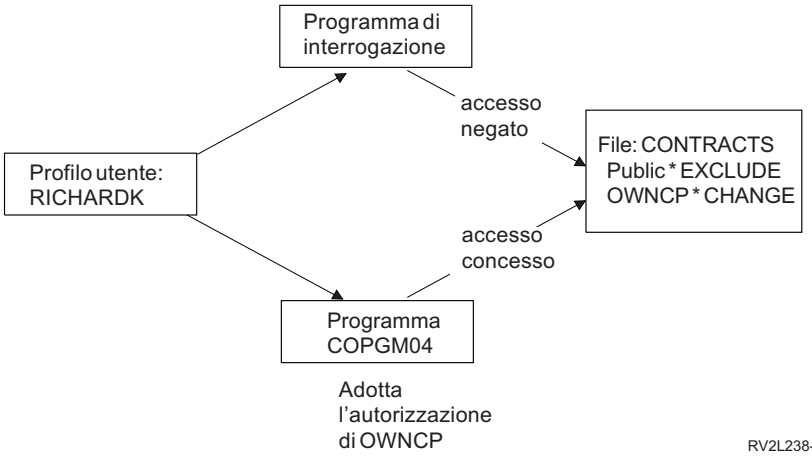
Gli esempi mostrati fino ad ora hanno visualizzato un approccio non rigoroso alla sicurezza, dove più persone hanno l'accesso alle informazioni in una libreria. Le informazioni sui contratti e sulle tariffe nell'Azienda di giocattoli JKL sono riservate e richiedono un approccio restrittivo. Fortunatamente, tutte queste informazioni vengono memorizzate in una libreria separata. Anche i programmi per aggiornare i contratti e le tariffe si trovano in una libreria speciale.

Sharon ha rivisto gli obiettivi sulla sicurezza per l'applicazione Contratti e Tariffe (consultare Determinare gli obiettivi per la sicurezza delle risorse). Ha rivisto anche il modulo Descrizione dell'applicazione e i moduli Descrizione della libreria. Sharon pensava fosse difficile soddisfare gli obiettivi della sicurezza per l'applicazione. Ha preso qualche appunto e ha discusso il problema con il fornitore dell'applicazione:

- Il personale addetto alle Vendite e Marketing e i dirigenti devono poter creare e modificare i contratti. Essi devono poter utilizzare sia i file che i programmi.
- Il personale addetto all'Elaborazione ordini modifica i contratti e visualizza le tariffe indirettamente quando inserisce ed invia gli ordini, ma non può visualizzare i contratti e le tariffe in un altro modo. Tuttavia, il personale può utilizzare Query per creare i prospetti sui clienti e sugli ordini. Se viene fornita l'autorizzazione ai file Contratti e Tariffe, il personale può creare programmi d'interrogazione per visualizzarli o stamparli.

Il fornitore dell'applicazione per l'Azienda di giocattoli JKL ha suggerito l'utilizzo della funzione di autorizzazione di sicurezza adottata per risolvere questo problema. L'**Autorizzazione adottata** consente ad un utente di adottare l'autorizzazione del proprietario del programma durante la sua esecuzione. L'utente non necessita dell'autorizzazione all'oggetto.

Il diagramma mostra un esempio di come funziona l'autorizzazione adottata. Karen Richards (RICHARDK) nel reparto Elaborazione ordini non dispone generalmente dell'autorizzazione all'utilizzo del file Contratti. Tuttavia, quando lei immette degli ordini, ha bisogno di controllare e di aggiornare il bilancio. Il programma di immissione ordini che gestisce i bilanci (COPGM04) adotta l'autorizzazione del profilo OWNCP. Mentre Karen esegue il programma COPGM04, ha l'autorizzazione all'utilizzo del file contratti:



Consultare l'argomento, ″Determinare la proprietà delle librerie e degli oggetti″ per dettagli sulla proprietà dell'oggetto. Il fornitore o il programmatore dell'applicazione può specificare che il programma adotta l'autorizzazione del proprietario quando crea (compila) un programma oppure un programmatore può specificare un'autorizzazione adottata per il programma utilizzando il comando Modifica programma (CHGPGM). Verificare di conoscere tutte le funzioni del programma prima di utilizzare questa tecnica.

Sharon ha deciso di utilizzare la funzione di autorizzazione adottata per fornire agli utenti esterni al reparto Vendite e Marketing l'accesso ai file Contratti e tariffe. Lei ha anche stabilito che l'accesso *CHANGE era sufficiente per tutti gli oggetti utilizzati dall'applicazione Contratti e tariffe. La tabella che segue mostra il modulo Descrizione della libreria per la libreria Contratti:

Tabella 47. Modulo Descrizione della libreria dell'Azienda di giocattoli JKL: esempio di autorizzazione restrittiva

Modulo Descrizione della libreria		**Parte 1 di 2**
Nome libreria: `CONTRACTS`	Nome descrittivo (Testo): `Libreria Contratti e tariffe`	
Autorizzazione pubblica alla libreria: `*EXCLUDE` Autorizzazione pubblica agli oggetti nella libreria: `*CHANGE` Autorizzazione pubblica per i nuovi oggetti (CRTAUT): `*CHANGE` Proprietario libreria:		

Tabella 48. Modulo Descrizione della libreria dell'Azienda di giocattoli JKL: esempio di autorizzazione restrittiva

Modulo Descrizione della libreria				**Parte 2 di 2**
Elencare le autorizzazioni ai singoli oggetti nella libreria				
Profilo di gruppo e profilo utente	Nome oggetto	Tipo oggetto	Autorizzazione necessaria	Liste di autorizzazioni
`DPTSM`	`CONTRACTS`	`*LIB`	`*USE`	
`DPTMG`	`CONTRACTS`	`*LIB`	`*USE`	

Non è necessario limitare l'autorizzazione agli oggetti nella libreria, perché viene limitato l'accesso alla libreria stessa. Inoltre, Sharon ha fornito l'autorizzazione ai dirigenti e al reparto Vendite e Marketing. Ha utilizzato l'autorizzazione di gruppo, invece di fornire l'autorizzazione ad ogni singolo individuo nei reparti.

Nota: un programmatore esperto che ha accesso ad una libreria può essere in grado di conservare l'accesso agli oggetti nella libreria anche dopo che gli è stata revocata l'autorizzazione alla libreria. Se una libreria contiene oggetti con requisiti di sicurezza elevati, limitare gli oggetti e la libreria per la protezione completa.

E' possibile che si desideri rivedere un esempio non restrittivo che utilizza l'autorizzazione pubblica prima di cominciare a determinare la proprietà delle librerie e degli oggetti.

Determinare la proprietà delle librerie e degli oggetti

Dopo aver pianificato la sicurezza per le librerie dell'applicazione, è possibile decidere la proprietà delle librerie e degli oggetti. Ad ogni oggetto viene assegnato un proprietario al momento della sua creazione. Il proprietario dell'oggetto dispone automaticamente della completa autorizzazione all'oggetto, la qual cosa include l'autorizzazione di altri ad utilizzare l'oggetto, a modificarlo e a cancellarlo. Il responsabile della riservatezza può eseguire queste funzioni per tutti gli oggetti presenti nel sistema.

Il sistema utilizza il profilo del proprietario dell'oggetto per tenere traccia di chi ha l'autorizzazione all'oggetto. Il sistema completa tale funzione internamente. Ciò potrebbe non influenzare direttamente il profilo utente. Tuttavia, se non si pianifica correttamente la proprietà dell'oggetto, alcuni profili degli utenti potrebbero diventare troppo grandi.

Quando il sistema salva un oggetto, il sistema salva anche il nome del profilo del proprietario. Il sistema utilizza queste informazioni in caso di ripristino dell'oggetto. Se il profilo del proprietario per un oggetto ripristinato non è nel sistema, il sistema trasferisce la proprietà su un profilo fornito dall'IBM denominato QDFTOWN.

Suggerimenti

I seguenti suggerimenti si applicano a molte, ma non a tutte, le situazioni. Dopo aver esaminato i suggerimenti, discutere le idee relative alla proprietà dell'oggetto con il programmatore o con il fornitore dell'applicazione. Se si acquistano le applicazioni, si potrebbe non essere in grado di controllare a quale profilo appartengano le librerie e gli oggetti. L'applicazione può essere progettata in modo da impedire modifiche di proprietà.

- Evitare di utilizzare un profilo fornito dall'IBM, ad esempio QSECOFR o QPGMR, come proprietario dell'applicazione. A tali profili appartengono molti oggetti contenuti nelle librerie fornite dall'IBM e sono già di dimensione elevata.
- Generalmente, ad un profilo di gruppo non dovrebbe appartenere un'applicazione. Ogni membro del gruppo ha la stessa autorizzazione del profilo di gruppo, a meno che non si assegni specificatamente un'autorizzazione più bassa. In effetti, ad ogni membro del gruppo verrà assegnata l'autorizzazione completa per l'applicazione.
- Se si ha intenzione di delegare la responsabilità del controllo delle applicazioni ai dirigenti dei vari reparti, tali dirigenti potrebbero essere proprietari di tutti gli oggetti dell'applicazione. Il gestore di un'applicazione, tuttavia, potrebbe modificare le responsabilità. In tal caso, la proprietà di tutti gli oggetti dell'applicazione verrà trasferita ad un nuovo gestore.
- Molte persone utilizzano la tecnica di creare uno speciale profilo del proprietario per ogni applicazione con la parola d'ordine impostata su *NONE. Il profilo del proprietario viene utilizzato dal sistema per gestire le autorizzazioni per l'applicazione. Il responsabile della riservatezza (o qualcuno con tale autorizzazione) esegue l'effettiva gestione dell'applicazione oppure essa viene delegata ai gestori con autorizzazione *ALL per particolari applicazioni.

Decidere a quali profili apparterranno le applicazioni. Immettere le informazioni relative al profilo del proprietario in ogni modulo Descrizione della libreria.

E' possibile esaminare un esempio del modo in cui l'Azienda di giocattoli JKL abbia determinato la proprietà dell'applicazione prima di iniziare a decidere la proprietà e l'accesso per le librerie dell'utente.

Esempio: proprietà dell'applicazione dell'Azienda di giocattoli JKL

Sharon Jones ha deciso di creare un profilo proprietario speciale per ogni applicazione. Lei e Ken Harrison, il sostituto del responsabile della riservatezza, avranno la responsabilità della gestione della sicurezza delle applicazioni. Successivamente, se i requisiti della sicurezza dell'azienda diventano più complessi, Sharon può delegare parte della responsabilità della gestione delle autorizzazioni ai gestori dei reparti.

Sharon ha aggiunto una nuova voce al modulo Convenzioni di denominazione:

Tabella 49. Modulo Convenzioni di denominazione dell'Azienda di giocattoli JKL: esempio di profilo proprietario

Tipo di oggetto	Convenzione di denominazione
Profilo proprietario	Verrà creato un profilo proprietario per ogni applicazione. Questo profilo conterrà tutte le librerie e gli oggetti. Il profilo proprietario verrà denominato OWN più l'abbreviazione dell'applicazione. Il profilo proprietario Controllo inventario sarà OWNIC.

Sharon ha stabilito che il nome del profilo proprietario inizi con OWN in modo che tutti i profili proprietario vengano visualizzati insieme sui pannelli e sulle liste.

Sharon ha assegnato ai proprietari tutte le librerie dell'applicazione e ha inserito tali informazioni sui moduli Convenzioni di denominazione. L'unica libreria che aveva più di un proprietario applicazione possibile era la libreria Record cliente. Poiché l'applicazione Crediti a breve termine viene utilizzata per creare nuovi clienti e per impostare i limiti di credito, Sharon ha deciso che tale applicazione deve far parte dei file dei clienti. Questi sono i proprietari assegnati:

Nome libreria	Nome proprietario
ICPGMLIB	OWNIC
ITEMLIB	OWNIC
CONTRACTS	OWNCP
CPPGMLIB	OWNCP
COPGMLIB	OWNCO
CUSTLIB	OWNAR
ARPGMLIB	OWNAR

E' possibile ora stabilire la proprietà e l'accesso per le librerie utente.

Stabilire la proprietà e l'accesso per le librerie utente

Se il sistema dispone del programma su licenza IBM Query per iSeries o un altro programma di supporto di scelta, gli utenti necessiteranno di una libreria per memorizzare i programmi d'interrogazione creati. Generalmente, questa libreria è la **libreria corrente** nel profilo utente. Per ulteriori informazioni sulla creazione di una libreria corrente per ogni utente, consultare ″Scegliere i valori che influenzano il collegamento.″ Sharon Jones ha intenzione di utilizzare le librerie correnti per il reparto Vendite e Marketing e le librerie di gruppo per gli altri reparti:

- Il personale del reparto Vendite e Marketing utilizzerà moltissimo Query. E' necessario che ogni utente abbia una libreria privata. In caso contrario, dovranno preoccuparsi di assegnare dei nomi alle loro interrogazioni e potrebbero accidentalmente eliminare l'uno i programmi dell'altro.

- Per cominciare, gli altri reparti avranno delle librerie di gruppo. Se questi creano molti programmi d'interrogazione, è possibile prendere in considerazione singole librerie.

Se un utente appartiene ad un gruppo, si utilizza un campo del profilo utente per specificare se all'utente o al gruppo appartengono tutti gli oggetti creati dall'utente. Se gli oggetti appartengono all'utente, è possibile specificare quale autorizzazione ad utilizzare gli oggetti abbiano i membri del gruppo. E' inoltre possibile specificare se l'autorizzazione del gruppo sia l'autorizzazione principale del gruppo o un'autorizzazione privata. E' possibile che l'autorizzazione principale del gruppo consenta di ottenere migliori prestazioni del sistema. Sharon ha preso ulteriori appunti relativi alle librerie dell'utente:

- Gli oggetti creati dovrebbero appartenere al personale del reparto Vendite e Marketing, anziché al gruppo. Non è necessario che essi modifichino reciprocamente i programmi d'interrogazione.
- Ogni membro del gruppo dovrebbe essere in grado di eseguire i programmi d'interrogazione dell'altro, poiché in tal modo il gruppo assume l'autorizzazione *USE per ogni oggetto creato da un membro del gruppo.
- L'autorizzazione del gruppo dovrebbe essere l'autorizzazione principale del gruppo.
- Il pubblico non dovrebbe avere accesso a queste librerie. E' possibile che il personale del reparto Vendite e Marketing abbia dei file di emissione derivanti dalle proprie interrogazioni. Tali file potrebbero contenere dei dati riservati.
- Per gli altri reparti, al gruppo apparterrà la libreria del gruppo e tutto ciò che è stato creato nella libreria. Ciò significa che ogni membro del gruppo può modificare o cancellare qualsiasi elemento contenuto della libreria. Se ciò causa dei problemi, potrebbe rivelarsi necessario tentare con un altro metodo.

Nella seguente tabella è riportato il modulo Singolo profilo utente per il reparto Vendite e Marketing che utilizza oggetti appartenenti all'utente:

Tabella 50. Modulo Singolo profilo utente dell'Azienda di giocattoli JKL: esempio di oggetti appartenenti all'utente

Nomi del profilo di gruppo: DPTSM	
Proprietario degli oggetti creati: *USRPRF	Autorizzazione di gruppo agli oggetti creati: *USE
Tipo di autorizzazione di gruppo: *PGP	

Nella seguente tabella è riportato il modulo Singolo profilo utente per un reparto che dispone degli oggetti appartenenti al gruppo:

Tabella 51. Modulo Singolo profilo utente dell'Azienda di giocattoli JKL: esempio di oggetti appartenenti al gruppo

Nomi del profilo di gruppo: DPTxx	
Proprietario degli oggetti creati: *GRPPRF	Autorizzazione di gruppo agli oggetti creati:

Il campo **Autorizzazione di gruppo agli oggetti creati** non viene utilizzato se il proprietario degli oggetti creati è il gruppo. I membri del gruppo dispongono automaticamente dell'autorizzazione *ALL a tutti gli oggetti creati.

Decidere a chi debbano appartenere e chi debba avere accesso alle librerie dell'utente. Immettere le scelte nei campi **Proprietario degli oggetti creati** e **Autorizzazione di gruppo agli oggetti** del modulo Singolo profilo utente. A questo punto si è pronti per iniziare a raggruppare gli oggetti.

Raggruppare gli oggetti

Dopo aver determinato la proprietà delle librerie e degli oggetti, è possibile iniziare a raggruppare gli oggetti nel sistema. Per semplificare la gestione delle autorizzazioni, utilizzare una lista di autorizzazioni per raggruppare gli oggetti con gli stessi requisiti. E' quindi possibile assegnare l'autorizzazione pubblica, dei profili di gruppo e dei profili utente alla lista di autorizzazioni invece che ai singoli oggetti contenuti nella lista. Il sistema tratta ogni oggetto protetto da una lista di autorizzazioni nello stesso modo, ma è possibile assegnare a diversi utenti diverse autorizzazioni nell'intera lista.

Una lista di autorizzazioni rende più facile ristabilire le autorizzazioni quando si ripristinano gli oggetti. Se si proteggono gli oggetti con una lista di autorizzazioni, il processo di ripristino collegherà automaticamente gli oggetti alla lista.

E' possibile assegnare ad un gruppo o ad un utente l'autorizzazione a gestire una lista di autorizzazioni (*AUTLMGT). La gestione della lista di autorizzazioni consente all'utente di aggiungere e eliminare altri utenti dalla lista e di modificare le autorizzazioni per quegli utenti.

Suggerimenti

- Utilizzare le liste di autorizzazioni per gli oggetti che richiedono protezione della sicurezza e che hanno requisiti di sicurezza simili. Le liste di autorizzazioni facilitano l'utilizzo di categorie di autorizzazioni piuttosto che singole autorizzazioni. Le liste di autorizzazioni, inoltre, facilitano il ripristino di oggetti ed il controllo delle autorizzazioni nel sistema.
- Evitare schemi complicati con combinazioni di liste di autorizzazioni, autorizzazioni di gruppo e singole autorizzazioni. Scegliere il metodo che si adatti meglio ad un determinato requisito, invece di utilizzare tutti i metodi contemporaneamente.

Potrebbe inoltre essere necessario aggiungere la convenzione di denominazione per le liste di autorizzazioni al modulo Convenzioni di denominazione.

Dopo aver preparato un modulo Lista di autorizzazioni, tornare indietro ed aggiungere tali informazioni al modulo Descrizione della libreria. Il programmatore o il fornitore dell'applicazione potrebbero avere già creato delle liste di autorizzazioni. Verificare con loro tale ipotesi.

Potrebbe risultare utile esaminare un esempio del modo in cui Sharon Jones dell'Azienda di giocattoli JKL ha pianificato le liste di autorizzazioni prima di pianificare la sicurezza delle stampanti e dell'emissione di stampa.

Esempio: modulo Lista di autorizzazioni dell'Azienda di giocattoli JKL

Sharon ha rivisto la Descrizione della libreria per la libreria Record cliente e ha deciso di creare una lista di autorizzazioni per i file che vengono eliminati alla fine di ogni mese. Sebbene vengano eliminati solo tre file, Sharon ha deciso di utilizzare una lista di autorizzazioni per semplificare la gestione delle autorizzazioni. Se in seguito vengono aggiunti altri file all'elaborazione di fine mese, lei può semplicemente proteggere quei file con la lista di autorizzazioni. Sharon ha deciso di escludere il pubblico dai file per impedire problemi non intenzionali durante l'elaborazione di fine mese. Lei ha fornito l'autorizzazione *ALL solo agli utenti che eseguono l'elaborazione. Rose Willis, l'operatore di sistema in serata, potrebbe avere la necessità di visualizzare le informazioni sui file per controllare l'elaborazione di fine mese. Lei necessita dell'autorizzazione *USE.

La tabella riportata di seguito mostra la convenzione di denominazione che Sharon ha utilizzato per le liste di autorizzazioni.

Tabella 52. Modulo Convenzioni di denominazione dell'Azienda di giocattoli JKL: esempio Lista di autorizzazioni

Modulo Convenzioni di denominazione	
Preparato da: Sharon Jones	Data: 9/5/99

Tabella 52. Modulo Convenzioni di denominazione dell'Azienda di giocattoli JKL: esempio Lista di autorizzazioni (Continua)

Tipo di oggetto	Convenzione di denominazione
Liste di autorizzazioni	Per le liste che proteggono gli oggetti di una libreria, utilizzare parte del nome della libreria più LST e un numero. Una lista di oggetti in CUSTLIB potrebbe essere CUSTLST1. Per una lista che protegge gli oggetti che derivano da più di una libreria, utilizzare un'abbreviazione dell'applicazione se possibile: ARLST1. Se la lista si applica a più applicazioni, selezionare un nome valido qualsiasi. La descrizione della lista deve specificare il suo scopo principale.

La tabella che segue mostra il modulo Lista di autorizzazioni per la libreria CUSTLIB. Sharon ha preparato questo modulo utilizzando le informazioni del modulo Descrizione della libreria:

Tabella 53. Piano Lista di autorizzazioni dell'Azienda di giocattoli JKL: esempio

Modulo Lista di autorizzazioni					
Nome lista di autorizzazioni: CUSTLST1					
Descrizione: file eliminati durante l'elaborazione di fine mese.					
Elencare gli oggetti protetti dalla lista					
Nome oggetto	Tipo oggetto	Libreria oggetto	Nome oggetto	Tipo oggetto	Libreria oggetto
ARFILE01	*FILE	CUSTLIB	ARFFILE02	*FILE	CUSTLIB
ARFILE03	*FILE	CUSTLIB			
Elencare i gruppi e gli utenti che hanno accesso alla lista					
Gruppo o utente	Tipo di accesso consentito	Gestione liste?	Gruppo o utente	Tipo di accesso consentito	Gestione liste?
PUBLIC	*EXCLUDE	no	ROSSG	*ALL	no
SMITHJ	*ALL	no	JONESS	*ALL	sì
WILLISR	*USE	no			

Sharon ha aggiunto anche le informazioni sulla lista di autorizzazioni al modulo Descrizione della libreria per la libreria CUSTLIB:

Modulo Descrizione della libreria				Parte 2 di 2
Preparato da: Sharon Jones			Data: 9/9/99	
Nome libreria: CUSTLIB				
Elencare le autorizzazioni specifiche per gli oggetti della libreria				
Profilo di gruppo e profilo utente	Nome oggetto	Tipo oggetto	Autorizzazione necessaria	Lista di autorizzazioni
PUBLIC	ARFILE01	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE02	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE03	*FILE	*AUTL	CUSTLST1

Tenere presente che l'autorizzazione pubblica per ogni file deve essere modificata in *AUTL per il sistema in modo da utilizzare la lista di autorizzazioni per determinare l'autorizzazione pubblica.

Considerare le singole autorizzazioni e di gruppo presenti nei moduli Descrizione della libreria. Decidere se l'utilizzo delle liste di autorizzazioni è appropriato. In tal caso, preparare i moduli Lista di autorizzazioni

e aggiornare i moduli Descrizione della libreria con le informazioni sulla lista di autorizzazioni. E' possibile pianificare la sicurezza per le stampanti e l'emissione di stampa.

Pianificare la sicurezza per le stampanti e l'emissione di stampa

Dopo aver raggruppato gli oggetti, è necessario pianificare le modalità di protezione dell'emissione di stampa. Sono stati sviluppati dei piani per proteggere le informazioni memorizzate nel sistema. E' inoltre necessario un piano per proteggere le informazioni riservate durante la stampa o l'attesa della stampa. Verificare il Piano di sicurezza fisica per le stampanti utilizzato dall'azienda per le emissioni riservate.

Quando si esegue un programma che stampa una documentazione, generalmente tale documentazione non viene inviata direttamente alla stampante. Il programma crea una copia della documentazione, denominata **file di spool** o **emissione di stampa**. Il sistema memorizza il file di spool in un oggetto denominato **coda di emissione** sino a quando non sia disponibile una stampante. Quando una coda di emissione contiene un'emissione di stampa, è possibile visualizzare la documentazione sulla stazione di lavoro. E' inoltre possibile congelarla o indirizzarla ad una stampante specifica.

Lo spool facilita la pianificazione dei lavori di stampa e la condivisione delle stampanti. Lo spool consente inoltre di proteggere le emissioni riservate. E' possibile creare una o più code di emissione specifiche per conservare emissioni riservate e limitare la possibilità di visualizzare e gestire tali code di emissione. E' inoltre possibile controllare quando le emissioni riservate vengono inviate dalla coda alla stampante.

Completare il modulo Sicurezza dell'emissione di stampa e della stazione di lavoro via via che si procede in questo argomento.

Durante la creazione di una coda di emissione speciale, è possibile specificare diversi parametri relativi alla sicurezza:

- **Parametro DSPDTA (Visualizzazione dati)**: il parametro DSPDTA di una coda di emissione determina se un utente possa visualizzare, inviare o copiare un file di spool appartenente ad un altro utente.
- **Parametro AUTCHK (Autorizzazione da verificare)**: il parametro AUTCHK di una coda di emissione determina se un utente possa modificare o eliminare un file di spool appartenente ad un altro utente.
- **Parametro OPRCTL (Controllo operatore)**: il parametro OPRCTL di una coda di emissione determina se agli utenti con l'autorizzazione speciale *JOBCTL (o classe utente *SYSOPR) sia consentito controllare la coda di emissione.

I parametri della coda di emissione, l'autorizzazione dell'utente alla coda di emissione e l'autorizzazione speciale dell'utente interagiscono per determinare le funzioni che un utente può eseguire nei file di spool in una coda di emissione. La seguente tabella mostra quali combinazioni consentano agli utenti di eseguire diverse funzioni:

Funzioni di stampa	Parametri coda di emissione			Autorizzazione coda di emissione	Autorizzazione speciale
	DSPDTA	AUTCHK	OPRCTL		
Aggiungere file di spool alla coda [1]	Qualunque valore	Qualunque valore	Qualunque valore	*READ	Nessuna
	Qualunque valore	Qualunque valore	*Yes	Qualunque valore	*JOBCTL
Visualizzare la lista dei file di spool (comando WRKOUTQ)[2]	Qualunque valore	Qualunque valore	Qualunque valore	*READ	Nessuna
	Qualunque valore	Qualunque valore	*Yes	Qualunque valore	*JOBCTL

Visualizzare, copiare o inviare i file di spool (DSPSPLF, CPYSPFL, SNDNETSPLF, SNTCPSPLF)[2]	*YES	Qualunque valore	Qualunque valore	*READ	Nessuna
	*NO	*DTAAUT	Qualunque valore	*CHANGE	Nessuna
	*NO	*OWNER	Qualunque valore	Proprietario[3]	Nessuna
	*YES	Qualunque valore	*Yes	Qualunque valore	*JOBCTL
	*NO	Qualunque valore	*Yes	Qualunque valore	*JOBCTL
	*OWNER[5]	Qualunque valore	Qualunque valore	Qualunque valore	Qualunque valore
Modificare, cancellare, congelare, rilasciare il file di spool (CHGSPLFA, DLTSPLF, HLDSPLF, RLSSPLF)[2]	Qualunque valore	*DTAAUT	Qualunque valore	*CHANGE	Nessuna
	Qualunque valore	*OWNER	Qualunque valore	Proprietario[3]	Nessuna
Modificare, eliminare, congelare e rilasciare la coda di emissione (CHGOUTQ, CLROUTO, HLDOUTQ, RLSOUT)[2]	Qualunque valore	*DTAAUT	Qualunque valore	*CHANGE	Nessuna
	Qualunque valore	*OWNER	Qualunque valore	Proprietario[3]	Nessuna
	Qualunque valore	Qualunque valore	*YES	Qualunque valore	*JOBCTL
Avviare un programma di scrittura per la coda (STRPRTWTR, STRRMTWTR)[2]	Qualunque valore	*DTAAUT	*Any	*CHANGE[4]	Nessuna
	Qualunque valore	Qualunque valore	*YES	Ogni[4]	*JOBCTL

1 Questa è l'autorizzazione necessaria per indirizzare l'emissione alla coda di emissione.

2 Utilizzare questi comandi o le opzioni equivalenti da un pannello.

3 E' necessario essere il proprietario della coda di emissione.

4 Richiede inoltre l'autorizzazione *USE alla descrizione dell'unità di stampa.

5 E' necessario essere il proprietario del file di spool o disporre dell'autorizzazione speciale *SPLCTL per utilizzare questo comando.

Esaminare la parte relativa alla stampante nel Piano di sicurezza fisica. Riempire la sezione relativa alla coda di emissione del modulo Sicurezza dell'emissione di stampa e della stazione di lavoro via via che si procede in quest'argomento.

Potrebbe risultare utile esaminare un esempio del modo in cui Sharon Jones dell'Azienda di giocattoli JKL abbia determinato i valori per questi parametri della coda di emissione prima di pianificare la sicurezza delle risorse per le stazioni di lavoro.

Esempio: modulo Sicurezza della coda di emissione e della stazione di lavoro dell'Azienda di giocattoli JKL—parte relativa alla coda di emissione

Il reparto Vendite e Marketing nell'Azienda di giocattoli JKL ha due requisiti per la stampa riservata:

- Le liste delle tariffe preliminari vengono stampate quando vengono pianificate modifiche delle tariffe. Nessuno all'esterno del reparto Vendite e Marketing, fatta eccezione per i dirigenti dell'azienda, può visualizzare queste informazioni.

- I contratti sono riservati durante la negoziazione. La brutta copia del contratto può essere vista solo da chi sta negoziando il contratto stesso, da nessun altro del Reparto vendite e marketing.

Sharon ha deciso di creare due code di emissione speciali:

PRICEQ
Da utilizzare per le liste delle tariffe preliminari. Chiunque faccia parte del reparto Vendite e Marketing può eseguire funzioni su questa coda di emissione. Nessuno all'esterno di tale reparto può utilizzare la coda di emissione, inclusi gli operatori di sistema. PRICEQ si trova nella libreria CONTRACTS.

NEWCP
Da utilizzare per la stampa dei contratti in fase di negoziazione. La coda di emissione viene condivisa dai membri del reparto Vendite e Marketing, ma solo la persona che crea un file di spool sulla coda di emissione può controllare quel file. NEWCP si trova nella libreria CONTRACTS.

La tabella che segue mostra il modulo Sicurezza della coda di emissione e della stazione di lavoro che Sharon ha preparato per queste code di emissione:

Tabella 54. Modulo Sicurezza della coda di emissione e della stazione di lavoro dell'Azienda di giocattoli JKL: esempio Coda di emissione di stampa

Elencare i parametri per le code di emissione limitate:				
Nome coda di emissione	Libreria coda di emissione	Visualizzazione file (DSPDTA)	Autorizzazione da verificare (AUTCHK)	Controllo operatore (OPRCTL)
PRICEQ	CONTRACTS	*YES	*DTAAUT	*NO
NEWCP	CONTRACTS	*NO	*OWNER	*NO

L'argomento Decidere l'autorizzazione pubblica alle librerie del programma contiene un esempio che mostra l'autorizzazione alla libreria CONTRACTS nell'Azienda di giocattoli JKL. Solo i gestori e i membri del reparto Vendite e Marketing hanno accesso alla libreria. L'autorizzazione pubblica per gli oggetti nella libreria (incluse queste code di emissione) è *CHANGE.

Poiché il parametro AUTCHK sulla coda di emissione NEWCP è *OWNER, solo il proprietario di un file di spool può gestire quel file (consultare la tabella Autorizzazione necessaria per eseguire le funzioni di stampa sopra riportata). Ciò impedisce ai membri del reparto Vendite e Marketing di stampare ogni nuovo contratto dell'altra parte o di visualizzarli nella coda di emissione.

Dopo aver pianificato la sicurezza della coda di emissione di stampa, è possibile pianificare la sicurezza per le stazioni di lavoro.

Pianificare la sicurezza per le stazioni di lavoro

Dopo aver pianificato la sicurezza delle risorse per le stampanti e per l'emissione di stampa, è possibile iniziare a pianificare la sicurezza della stazione di lavoro. Nel piano di sicurezza fisica, sono state elencate le stazioni di lavoro che rappresentano un rischio per la sicurezza a causa della loro ubicazione. Utilizzare queste informazioni per determinare a quali stazioni di lavoro è necessario limitare l'accesso.

E' possibile incoraggiare il personale che utilizza queste stazioni di lavoro ad essere particolarmente attento alla sicurezza. E' necessario che essi si scolleghino ogni qualvolta si allontanano dalle stazioni di lavoro. E' possibile registrare le scelte relative alle procedure di scollegamento per le stazioni di lavoro a rischio nella normativa di sicurezza. E' inoltre possibile limitare le funzioni che è possibile eseguire su queste stazioni di lavoro per ridurre al minimo i rischi.

Il metodo più semplice per limitare la funzione sulla stazione di lavoro è quella di limitarla ai profili utente con funzione limitata. Sharon Jones ha utilizzato questa tecnica per il reparto Magazzino dell'Azienda di

giocattoli JKL. Sharon ha consentito a Ray Wagner e Janice Ames, che lavorano nella piattaforma di carico, di eseguire solo il programma di ricezione inventario. Anche Sharon ha reso loro gli unici utenti che possono collegarsi alla stazione di lavoro nella piattaforma di carico.

E' possibile scegliere di impedire a persone che dispongano dell'autorizzazione del responsabile della riservatezza o dell'autorizzazione di manutenzione di collegarsi da tutte le stazioni di lavoro. Se per farlo si utilizza il valore di sistema QLMTSECOFR, le persone dotate dell'autorizzazione del responsabile della riservatezza possono collegarsi solo a stazioni di lavoro autorizzate specificatamente.

Preparare la parte relativa alla stazione di lavoro del modulo Sicurezza della coda di emissione e della stazione di lavoro

E' possibile esaminare un esempio del modo in cui Sharon ha pianificato la sicurezza delle stazioni di lavoro nel preparare la parte relativa alla stazione di lavoro del modulo Sicurezza della coda di emissione e della stazione di lavoro. E' inoltre necessario esaminare una lista di suggerimenti relativi alla sicurezza delle risorse per verificare che il piano di sicurezza sia semplice e completo. Dopo aver esaminato l'esempio ed i suggerimenti è possibile iniziare a pianificare l'installazione dell'applicazione.

Esempio: modulo Sicurezza della coda di emissione e della stazione di lavoro dell'Azienda di giocattoli JKL—parte relativa alla stazione di lavoro

Sharon Jones ha rivisto il Piano di sicurezza fisica per determinare quali stazioni di lavoro corrono rischi di sicurezza. Nell'Azienda di giocattoli JKL, ad esempio, gli esterni all'azienda possono avere facile accesso alle stazioni di lavoro sulla piattaforma di carico e nell'ufficio vendite distaccato. Sharon ha indicato sul Piano di sicurezza fisica che quelle stazioni di lavoro rappresentano un potenziale rischio per la sicurezza.

Il metodo più semplice per limitare la funzione sulla stazione di lavoro è quella di limitarla ai profili utente con funzione limitata. Sharon Jones ha utilizzato questa tecnica per il reparto Magazzino dell'Azienda di giocattoli JKL. Sharon ha consentito a Ray Wagner e Janice Ames, che lavorano nella piattaforma di carico, di eseguire solo il programma di ricezione inventario. Anche Sharon ha reso loro gli unici utenti che possono collegarsi alla stazione di lavoro nella piattaforma di carico.

Sharon ha rivalutato la sua scelta per il valore di sistema QLMTSECOFR. Ha deciso di impostarlo su 1(Sì) come protezione aggiuntiva per le stazioni di lavoro vulnerabili nella piattaforma di carico e nell'ufficio vendite distaccato.

La tabella che segue mostra la parte della stazione di lavoro del modulo Sicurezza della coda di emissione e della stazione di lavoro preparato da Sharon.

Tabella 55. Modulo Sicurezza della coda di emissione e della stazione di lavoro dell'Azienda di giocattoli JKL: esempio di Stazione di lavoro

Stazioni di lavoro del responsabile della riservatezza: Se si limita il responsabile della riservatezza a stazioni di lavoro specifiche (il valore di sistema QLMTSECOFR è sì), elencare di seguito le stazioni di lavoro autorizzate per il responsabile della riservatezza e chiunque abbia l'autorizzazione *ALLOBJ: `Tutte le stazioni di lavoro fatta eccezione di quelle elencate di seguito.`	
Elencare le autorizzazioni per le stazioni di lavoro limitate:	
Nome stazione di lavoro	Gruppi o utenti autorizzati (autorizzazione *CHANGE)
`DSP10`	`AMESJ, WAGNERR`
`DSP11`	`AMESJ, WAGNERR`
`RMT01`	`UNGERJ, BELLB`
`RMT02`	`UNGERJ, BELLB`

E’ possibile che si desideri rivedere un riepilogo dei suggerimenti sulla sicurezza delle risorse prima di pianificare l’installazione dell’applicazione.

Riepilogo dei suggerimenti sulla sicurezza delle risorse

Dopo aver terminato la pianificazione della sicurezza della stazione di lavoro, è possibile esaminare i seguenti suggerimenti sulla sicurezza delle risorse. Il sistema iSeries offre molte opzioni per la protezione delle informazioni contenute nel sistema. Ciò conferisce la flessibilità per progettare il piano di sicurezza delle risorse più adatto all’azienda. Ma questa varietà di opzioni può anche risultare fonte di confusione.

Utilizzando l’Azienda di giocattoli JKL come esempio, questo argomento mostra un approccio di base alla pianificazione della sicurezza delle risorse che utilizza queste istruzioni:

- Passare dal generale al particolare:
  - Pianificare la sicurezza per le librerie. Occuparsi dei singoli oggetti solo quando necessario.
  - Pianificare prima di tutto l’autorizzazione pubblica, seguita dall’autorizzazione di gruppo e dalla singola autorizzazione.
- Per migliorare le prestazioni e semplificare le operazioni di copia di riserva e di ripristino, definire la sicurezza specifica solo per gli oggetti i cui requisiti di sicurezza non possono essere soddisfatti utilizzando l’autorizzazione pubblica.
- Rendere l’autorizzazione pubblica per i nuovi oggetti in una libreria (CRTAUT) uguale all’autorizzazione pubblica definita per la maggior parte degli oggetti esistenti nella libreria.
- Evitare di attribuire ai gruppi o ai singoli minore autorizzazione rispetto a quella di cui dispone il pubblico. Ciò potrebbe ridurre le prestazioni, comportare in seguito errori e rendere difficile il controllo. Se si sa che qualcuno detiene per un oggetto almeno la stessa autorizzazione di cui dispone il pubblico, la sicurezza della pianificazione e del controllo ne risultano facilitate.
- Utilizzare le liste di autorizzazioni per raggruppare gli oggetti con gli stessi requisiti di sicurezza. Le liste di autorizzazioni sono più facili da gestire rispetto alle singole autorizzazioni e forniscono assistenza nel ripristino delle informazioni relative alla sicurezza.
- Creare profili utente speciali in qualità di proprietari dell’applicazione. Impostare la parola d’ordine del proprietario su *NONE.
- Evitare di utilizzare applicazioni appartenenti ai profili forniti dall’IBM, ad esempio QSECOFR o QPGMR.
- Utilizzare code di emissione speciali per i documenti riservati. Inserire la coda di emissione nella stessa libreria in cui sono contenute le informazioni riservate.
- Limitare il numero di persone che dispongono dell’autorizzazione del responsabile della riservatezza.
- Prestare attenzione nell’assegnare l’autorizzazione *ALL agli oggetti e alle librerie. Chi detiene l’autorizzazione *ALL potrebbe involontariamente cancellare dei dati.

Per essere sicuri di aver pianificato con esito positivo l’impostazione della sicurezza delle risorse, è necessario raccogliere le seguenti informazioni:

- Compilare la Parte 1 e la Parte 2 dei moduli Descrizione della libreria per tutte le librerie dell’applicazione.
- Sui moduli Singolo profilo utente riempire i campi **Proprietario degli oggetti creati** e **Autorizzazione di gruppo agli oggetti creati**.
- Sul modulo Convenzioni di denominazione descrivere il modo in cui si ha intenzione di denominare le liste di autorizzazioni.
- Preparare i moduli Lista di autorizzazioni.
- Aggiungere le informazioni relative alla lista di autorizzazioni nei moduli Descrizione della libreria.
- Preparare un modulo Sicurezza della coda di emissione e della stazione di lavoro.

Si è ora pronti a pianificare l’installazione dell’applicazione.

Pianificare l’installazione dell’applicazione

Per completare la pianificazione della sicurezza delle risorse, è necessario preparare l’installazione dell’applicazione. I seguenti argomenti consentiranno di pianificare la proprietà e l’autorizzazione alle applicazioni dopo averle installate. I metodi qui descritti potrebbero non funzionare per tutte le applicazioni. Consultare il programmatore o il fornitore dell’applicazione per assistenza nello sviluppo di un buon piano di installazione.

Se si ha intenzione di acquistare un’applicazione da un fornitore dell’applicazione, utilizzare queste informazioni per pianificare le attività della sicurezza che è necessario eseguire prima e dopo aver caricato le librerie dell’applicazione.

Se si ha intenzione di installare un’applicazione sviluppata da programmatori appartenenti al proprio sistema, utilizzare queste informazioni per pianificare le attività della sicurezza necessarie a far passare l’applicazione dallo stato di verifica a quello di produzione.

Procedere con le fasi per un’applicazione. Tornare quindi indietro e preparare i moduli Installazione dell’applicazione per ogni ulteriore applicazione.

Quali moduli sono necessari?

Effettuare una copia dei seguenti moduli e riempirli via via che si procede in quest’argomento:

Tabella 56. Moduli di pianificazione necessari per pianificare l’installazione dell’applicazione

Nome modulo	Numero di copie necessarie
Modulo Installazione dell’applicazione	Uno per applicazione

Utilizzare questi moduli, sui quali si è in precedenza lavorato per raccogliere informazioni circa la pianificazione dell’installazione dell’applicazione:

Nome modulo	Pronto in:
Modulo Descrizione della libreria	Descrivere le informazioni sulla libreria
Modulo Lista di autorizzazioni	Raggruppare gli oggetti

Nell’argomento, Caricare le applicazioni viene spiegato come eseguire le fasi necessarie per installare le applicazioni.

Per pianificare le installazioni dell’applicazione, consultare questi argomenti:

- Determinare i profili utente e i valori di installazione per le applicazioni.
- Modificare i valori di installazione.

Determinare i profili utente e i valori di installazione per le applicazioni

Durante la pianificazione dell’installazione dell’applicazione, è necessario prima di tutto stabilire i profili utente ed i valori di installazione per ogni applicazione. Prima di installare un’applicazione creata su un altro sistema, potrebbe essere necessario creare uno o più profili utente. Il profilo utente cui appartengono le librerie e gli oggetti dell’applicazione dovrebbe essere presente nel sistema prima che le librerie vengano caricate nel sistema. Registrare nel modulo Installazione dell’applicazione i profili che è necessario creare per ogni libreria ed i parametri necessari ai profili.

Per determinare i valori di installazione necessari, porre le seguenti domande al programmatore o al fornitore dell’applicazione e registrare le risposte nel modulo Installazione dell’applicazione:

- A quale profilo appartiene la libreria dell’applicazione?

- A quale profilo appartengono gli oggetti contenuti nella libreria?
- Qual è l'autorizzazione pubblica alla libreria (AUT)?
- Qual è l'autorizzazione pubblica per i nuovi oggetti (CRTAUT)?
- Qual è l'autorizzazione pubblica per gli oggetti contenuti nella libreria?
- Quali programmi, se presenti, adottano l'autorizzazione del proprietario?

Scoprire se i programmatori o il fornitore dell'applicazione abbiano creato delle liste di autorizzazioni per l'applicazione. Preparare un modulo Lista di autorizzazioni per ogni lista di autorizzazioni creata o richiedere al programmatore le informazioni relative alla lista.

E' possibile determinare se sia necessario modificare qualche valore di installazione.

Modificare i valori di installazione per le applicazioni

Confrontare le informazioni del modulo Installazione dell'applicazione con il piano di sicurezza delle risorse per la libreria nel Modulo Descrizione della libreria. Nel caso in cui risultino diverse, è necessario decidere quali modifiche apportare dopo aver installato l'applicazione.

Modificare la proprietà dell'applicazione

Se il programmatore o il fornitore dell'applicazione ha creato un profilo speciale al quale appartengono le librerie e gli oggetti dell'applicazione, utilizzare tale profilo, anche nel caso in cui non corrisponde alle proprie convenzioni di denominazione. Il trasferimento della proprietà degli oggetti può richiedere parecchio tempo, quindi si consiglia di evitarlo.

Se l'applicazione appartiene ad uno dei profili di gruppo forniti dalla IBM, ad esempio QSECOFR o QPGMR, è necessario trasferire la proprietà ad un altro profilo dopo aver installato l'applicazione.

Talvolta i programmatori progettano le applicazioni in modo da impedire modifiche alla proprietà dell'oggetto. E' necessario tentare di applicare le limitazioni continuando comunque a soddisfare le proprie esigenze di gestione della sicurezza. Tuttavia, se l'applicazione appartiene ad un profilo fornito dalla IBM, ad esempio QSECOFR, è necessario che il programmatore o il fornitore dell'applicazione sviluppino un piano per modificare la proprietà. La soluzione migliore sarebbe quella di modificare la proprietà prima di installare l'applicazione.

Modificare l'autorizzazione pubblica

Quando si salvano gli oggetti, insieme a loro si salva anche l'autorizzazione pubblica. Quando si ripristina una libreria dell'applicazione nel sistema, la libreria e tutti i relativi oggetti avranno le stesse autorizzazioni pubbliche che avevano quando sono stati salvati. Ciò è valido anche se si è salvata la libreria su un altro sistema.

Il valore CRTAUT per una libreria (autorizzazione pubblica per nuovi oggetti) non influenza gli oggetti ripristinati. Essi vengono infatti ripristinati con l'autorizzazione pubblica salvata, senza tenere conto del valore CRTAUT per la libreria.

E' necessario modificare l'autorizzazione pubblica delle librerie e degli oggetti in modo che corrisponda al piano contenuto nel modulo Descrizione della libreria.

Nel pianificare l'installazione dell'applicazione, è possibile esaminare un esempio che mostra il modo in cui Sharon Jones dell'Azienda di giocattoli JKL ha pianificato l'installazione dell'applicazione.

Per essere sicuri di aver pianificato completamente l'installazione dell'applicazione è necessario:

- Finire di compilare il modulo iniziale Installazione dell'applicazione. Tornare quindi indietro e preparare i moduli per ogni ulteriore applicazione.

- Esaminare tutti i moduli e verificare che siano completi. Effettuare delle copie dei moduli e conservarle in un luogo sicuro fino a che non si siano installati il sistema ed i programmi su licenza.

Dopo aver terminato queste attività di pianificazione, si è pronti a impostare la sicurezza dell'utente.

Esempio: modulo Installazione dell'applicazione dell'Azienda di giocattoli JKL

L'Azienda di giocattoli JKL ha acquistato le applicazioni Ordini cliente e Crediti a breve termine da un fornitore dell'applicazione. Essi hanno chiamato un programmatore esterno per sviluppare l'applicazione Contratti e Tariffe e per collegarla all'applicazione Ordini cliente.

Sharon Jones ha utilizzato informazioni tratte dai moduli Descrizione della libreria per preparare il modulo Installazione dell'applicazione. La tabella riportata di seguito mostra una copia del modulo Descrizione della libreria di Sharon per CUSTLIB: (Consultare l'argomento ″Descrivere le informazioni sulla libreria.″)

Tabella 57. Modulo Descrizione della libreria dell'Azienda di giocattoli JKL: esempio

Modulo Descrizione della libreria	**Parte 1 di 2**
Preparato da: `Sharon Jones`	Data: `9/9/99`
Nome libreria: `CUSTLIB`	Nome descrittivo (testo): `Libreria record cliente`
Descrivere brevemente la funzione di questa libreria: `Conserva tutti i file del cliente, compresi gli ordini e i conti.`	
Definire gli obiettivi della sicurezza per la libreria, ad esempio se le informazioni sono riservate: `Oggi, viene consentito a tutti all'interno dell'azienda di visualizzare gli ordini del cliente. Per proteggere la precisione delle informazioni, è necessario limitare il numero di utenti abilitati alla modifica.`	
Autorizzazione pubblica alla libreria: `*USE` Autorizzazione pubblica agli oggetti nella libreria: `*CHANGE` Autorizzazione pubblica per i nuovi oggetti (CRTAUT): `*CHANGE` Proprietario libreria: `OWNAR`	

La tabella riportata di seguito mostra il modulo Installazione dell'applicazione che Sharon ha preparato per l'applicazione Ordini cliente. Tenere presente che Sharon ha deciso di utilizzare il profilo proprietario creato dal fornitore dell'applicazione. Il profilo COWNER avrà la proprietà del file e delle librerie di programma.

Dopo l'installazione dell'applicazione, Sharon deve effettuare quanto segue:

- Modificare le autorizzazioni pubbliche per le librerie in modo tale che corrispondano al piano di sicurezza delle risorse nei moduli Descrizione della libreria.
- Modificare la classe utente del profilo COWNER in *USER ed eliminare tutte le autorizzazioni speciali.
- Modificare la parola d'ordine del profilo COWNER in *NONE.

Tabella 58. Modulo Installazione dell'applicazione dell'Azienda di giocattoli JKL: esempio

Nome applicazione: `Ordini cliente (CO)`		Descrizione: `Immettere, tenere traccia e inviare gli ordini.`
Elencare e spiegare tutti i profili che devono essere creati per installare l'applicazione: `La libreria che contiene i file è di proprietà di un profilo denominato COWNER. La libreria di programma è di proprietà di QPGMR.`		
Nome libreria: `CUSTLIB`		
	Prima dell'installazione	**Dopo l'installazione**
Proprietario libreria	`COWNER`	`COWNER`
Proprietario oggetto	`COWNER`	`COWNER`
Autorizzazione pubblica alla libreria	`*EXCLUDE`	`*USE`

Tabella 58. Modulo Installazione dell'applicazione dell'Azienda di giocattoli JKL: esempio (Continua)

Autorizzazione pubblica all'oggetto	*ALL	*CHANGE
Autorizzazione pubblica per i nuovi oggetti	*CHANGE	*CHANGE
Nome libreria: COPGMLIB		
	Prima dell'installazione	**Dopo l'installazione**
Proprietario libreria	QPGMR	COWNER
Proprietario oggetto	QPGMR	COWNER
Autorizzazione pubblica alla libreria	*EXCLUDE	*USE
Autorizzazione pubblica all'oggetto	*ALL	*CHANGE
Autorizzazione pubblica per i nuovi oggetti	*CHANGE	*CHANGE

Al termine delle attività di pianificazione, l'utente è pronto per impostare la sicurezza dell'utente.

Capitolo 6. Impostare la sicurezza dell'utente

Questo argomento fornisce istruzioni circa le attività necessarie per impostare la sicurezza dell'utente nel sistema utilizzando l'interfaccia della riga comandi. Se si sta configurando un nuovo sistema, è necessario completare queste fasi in sequenza. Il sistema utilizza le informazioni di ogni istruzione via via che si passa alla fase successiva. Per impostare la sicurezza di base del sistema, è necessario completare due serie di attività. E' necessario prima di tutto definire la sicurezza dell'utente ed in seguito proteggere le risorse presenti nel sistema. Le due seguenti tabelle evidenziano ognuna delle fasi necessarie per impostare la sicurezza dell'utente e delle risorse.

Nota: è **NECESSARIO** completare tutte le fasi di impostazione della sicurezza dell'utente, prima di iniziare a impostare la sicurezza delle risorse.

Tabella 59. Fasi di impostazione della sicurezza dell'utente

Fase	Cosa fare in questa fase	Quali moduli utilizzare
Impostare l'ambiente globale	Impostare i valori di sistema iniziali e gli attributi di rete. Creare un profilo utente del responsabile della riservatezza.	Modulo Selezione valori di sistema
Impostare i valori di sistema per la sicurezza	Impostare i valori di sistema aggiuntivi.	Modulo Selezione valori di sistema
Preparare le fasi della sicurezza di base per il caricamento delle applicazioni	Creare i profili del proprietario. Caricare le applicazioni. E' necessario che le librerie e gli oggetti dell'applicazione siano presenti nel sistema prima di completare le fasi successive.	Modulo Installazione dell'applicazione
Impostare i gruppi di utenti	Creare le descrizioni lavoro, le librerie di gruppo ed i profili di gruppo.	Modulo Descrizione del gruppo di utenti
Impostare i singoli utenti	Creare le singole librerie e i profili utente.	Modulo Singolo profilo utente

Tabella 60. Fasi di impostazione della sicurezza delle risorse

Fase	Cosa fare in questa fase	Quali moduli utilizzare
Impostare l'autorizzazione pubblica e la proprietà	Stabilire l'autorizzazione pubblica e la proprietà per le librerie e gli oggetti.	Modulo Installazione dell'applicazione
Creare una lista di autorizzazioni	Creare delle liste di autorizzazioni.	Modulo Lista di autorizzazioni
Impostare delle autorizzazioni specifiche	Impostare l'accesso alle librerie e ai singoli oggetti.	Modulo Descrizione della libreria
Proteggere l'emissione di stampa	Proteggere l'emissione di stampa tramite la creazione di code di emissione e l'assegnazione dell'emissione.	Modulo Sicurezza della coda di emissione e della stazione di lavoro
Proteggere le stazioni di lavoro	Proteggere le stazioni di lavoro.	Modulo Sicurezza della coda di emissione e della stazione di lavoro

Oltre agli argomenti elencati nella precedente tabella, consultare i seguenti argomenti per la gestione della sicurezza del sistema:

- Verificare la sicurezza.
- Modificare le informazioni relative alla sicurezza.
- Salvare le informazioni relative alla sicurezza.
- Monitorare la sicurezza.

Prima di iniziare

Se si sta installando un nuovo sistema, eseguire le operazioni consigliate prima di iniziare a impostare la sicurezza:

- Verificare che l'unità di sistema e le varie unità siano installate e funzionino in modo corretto. Se non si ha intenzione di utilizzare la denominazione di iSeries per le unità, attendere prima di collegare le stazioni di lavoro e le stampanti fino alla modifica del valore di sistema che determina quali unità vengono denominate (QDEVNAMING). L'applicazione dei nuovi valori di sistema indica quando collegare le unità.
- Caricare tutti i programmi su licenza che si ha intenzione di utilizzare.

Impostare l'ambiente globale

Per iniziare l'impostazione della sicurezza dell'utente, è necessario impostare l'ambiente globale per gli utenti. In questo argomento, utilizzare Menu SETUP per impostare i valori di sistema e creare il proprio profilo utente. E' inoltre necessario modificare gli ID utente e le parole d'ordine per i profili DST (Dedicated Service Tools).

Nelle seguenti procedure, si trovano degli esempi di pannelli della riga comandi che illustrano queste istruzioni. Tuttavia, questi non mostrano l'intero pannello. Essi riportano solo le informazioni necessarie per completare l'attività.

Quali moduli sono necessari?

Immettere le informazioni dal modulo Selezione valori di sistema preparato in ″Pianificare la strategia di sicurezza globale.″

Per impostare l'ambiente globale, è necessario completare le seguenti attività:

1. Collegarsi al sistema.
2. Selezionare il livello di assistenza corretto.
3. Impedire il collegamento ad altri utenti.
4. Immettere i valori di sistema per la sicurezza.
5. Applicare i nuovi valori di sistema.
6. Creare un profilo responsabile della riservatezza

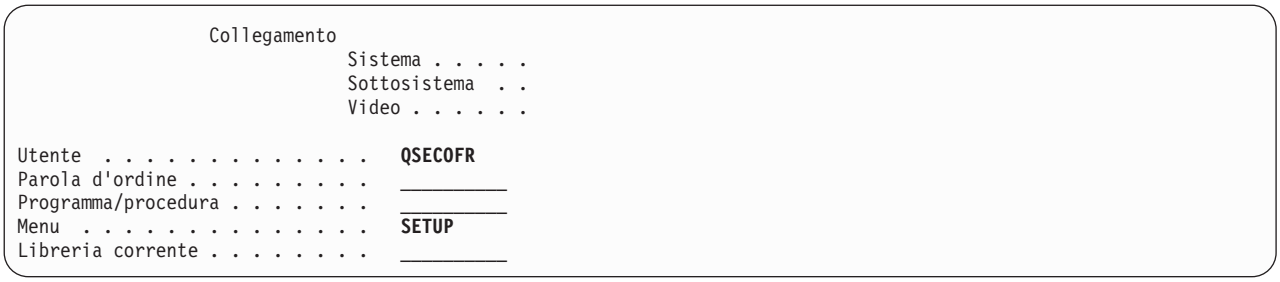
Dopo aver completato le precedenti istruzioni, è necessario modificare le parole d'ordine degli strumenti di manutenzione per evitare un loro eventuale utilizzo improprio. Consultare Strumenti di manutenzione per ulteriori dettagli.

Collegarsi al sistema

Per iniziare l'impostazione dell'ambiente di sistema, è necessario collegarsi al sistema.

1. Sulla console, collegarsi in qualità di responsabile della riservatezza (QSECOFR). Se ci si collega per la prima volta, utilizzare la parola d'ordine QSECOFR. Dal momento che il sistema fornisce questa parola d'ordine come scaduta, verrà richiesto di modificarla. E' necessario modificare questa parola d'ordine per collegarsi con esito positivo.
2. Immettere `SETUP` nel campo *Menu* nel pannello di collegamento.

Nota: il Menu SETUP viene denominato Personalizzazione sistema, utenti e unità. In tutto questo testo vi si fa riferimento come Menu SETUP.



Dopo essersi collegati al sistema, è necessario selezionare il livello di assistenza appropriato.

Selezionare il livello di assistenza corretto

Dopo essersi collegati al sistema, è possibile scegliere il livello di assistenza appropriato per gli utenti. Il **livello di assistenza** determina quale versione del pannello viene visualizzata. Molti pannelli di sistema presentano due diverse versioni:

- Una versione livello di assistenza di base, che contiene un minor numero di informazioni e non utilizza terminologia tecnica.
- Una versione livello di assistenza intermedio, che riporta maggiori informazioni ed utilizza termini tecnici.

Alcuni campi o funzioni sono disponibili solo in una versione particolare di un pannello. Le istruzioni indicano la versione da utilizzare. Per passare da un livello di assistenza ad un altro, utilizzare **F21** (Selezione livello assistenza). **F21** non è disponibile da tutti i pannelli.

Dopo aver selezionato il livello di assistenza, è necessario impedire ad altri utenti di collegarsi al sistema durante l'impostazione della sicurezza.

Impedire il collegamento ad altri utenti

Dopo aver selezionato il livello di assistenza corretto, è necessario impedire che altri utenti si colleghino al sistema. Se si è preoccupati che qualcuno possa manomettere il sistema prima di averlo protetto, è possibile impedire che qualsiasi altro utente si colleghi da un'altra stazione di lavoro. Tale precauzione è facoltativa. Applicarla solo se si ritiene necessaria una sicurezza temporanea:

1. Dal Menu SETUP, premere **F9** per visualizzare una riga comandi
2. Nella riga comandi, immettere `GO DEVICESTS`.
3. Il pannello mostra il menu Attività stato unità. Se viene visualizzato il menu Gestione stato configurazione, utilizzare **F21** (Selezione livello assistenza) per passare al livello di assistenza di base.
4. Selezionare l'opzione **1** (Gestione unità video).
5. Nel pannello Gestione unità video, disattivare tutte le stazioni di lavoro eccetto quella che si sta utilizzando. Effettuare tale operazione immettendo **2** prima del nome di ogni stazione di lavoro e premendo il tasto **Invio**.
6. Tornare al Menu SETUP premendo due volte **F3** (Fine).
7. Premere **F12** (Annullamento) per eliminare la riga comandi.

```
                          Gestione unità video

Immettere le seguenti opzioni, quindi premere Invio.
  1=Rendere disponibile    2=Rendere non disponibile   5=Visualizz.
  7=Visualizz. messaggio   8=Gestione programma e riga controllo
  13=Modifica descrizione

Opz  Unità       Tipo    Stato
__   DSP01       3196    QSECOFR
2_   DSP02       3196    Disponibile per l'utilizzo
2_   DSP03       3196    Disponibile per l'utilizzo
2_   DSP04       3196    Disponibile per l'utilizzo
```

Quando si rende non disponibile un'unità, questa non dispone di un pannello di collegamento, anche se viene attivata. Le stazioni di lavoro rimangono non disponibili solo fino a che non si arresta e non si riavvia il sistema. Potrebbe essere necessario ripetere questa operazione.

Dopo aver impedito che qualsiasi altro utente si colleghi al sistema, è possibile immettere i valori di sistema per la sicurezza.

Immettere i valori di sistema per la sicurezza

Dopo aver impedito il collegamento ad altri utenti, è necessario immettere i valori di sistema nel sistema.

Utilizzare questa procedura per immettere le informazioni dalla Parte 1 del modulo Selezione valori di sistema:

1. Dal Menu SETUP, selezionare l'opzione **1** (Modifica opzioni di sistema).
2. Immettere le informazioni dal modulo Selezione valori di sistema nel pannello Modifica opzioni di sistema. Se non si desidera modificare una delle scelte contenute nel pannello, è possibile utilizzare il tasto Tab per passare oltre.
3. Immettere la data e l'ora corrette in questo pannello, se non sono state impostate quando si è avviato il sistema.
4. Dopo aver immesso le informazioni in questa pagina, andare alla pagina successiva. *Segue...* nell'angolo inferiore destro del pannello indica che il pannello ha almeno una pagina in più.

```
                           Modifica opzioni di sistema
Sistema:
Immettere le seguenti scelte e quindi premere Invio.

Nome sistema  . . . . . .   JKLTOY     Nome

Opzioni data e ora:
  Data sistema  . . . . . .   09/21/99     MM/DD/YY
  Ora sistema . . . . . .   10:52:57     HH:MM:SS
  Separatore data . . . . . .   1            1=/
                                             2=-
                                             3=.
                                             4=,
                                             5=vuoto
  Formato data. . . . . .   MDY          YMD, MDY, DMY, JUL
  Separatore ora  . . . . . .   1            1=:
                                             2=.
                                             3=,
                                             4=vuoto


                                                                  Segue..
F1=Aiuto  F3=Fine   F5=Rivisual. F12=Annullamento
```

5. Immettere le scelte contenute nella seconda pagina del pannello ed andare alla pagina successiva.

```
                            Modifica opzioni di sistema

Immettere le seguenti scelte e quindi premere Invio.

Opzioni sicurezza:
  livello sicurezza  . . . . . .   40
   :
  Consentire ai responsabili della riservatezza di
    collegarsi a tutte le stazioni
    video . . . . . .   N
```

6. Immettere le scelte nella terza pagina del pannello e premere il tasto **Invio**.

```
                            Modifica opzioni di sistema

Immettere le seguenti scelte e quindi premere Invio.

Opzioni unità:
  Formato denominazione unità per nuove
  unità . . . . . .   1


  Stampante di sist. predefinita  PRT01

Ulteriori opzioni:
  Inserire utenti in ambiente S/36
    al collegamento . . . . . .   N
  Salvare informazioni account
    lavoro sull'emissione di stampa
    completata  . . . . . .   Y
```

7. Dovrebbe essere visualizzato nuovamente il Menu SETUP. Notare il messaggio nella parte inferiore del pannello: **Opzioni di sistema modificate con esito positivo. IPL richiesto**.

   Nota: il sistema richiede un IPL solo si è modificato il livello di sicurezza.

Alla fine della maggior parte degli argomenti delle attività di sistema si trova una tabella che descrive i possibili errori e le istruzioni di correzione. Utilizzare tali tabelle come supporto se i risultati sono diversi da quelli descritti. Tali tabelle potrebbero non prevedere tutti i problemi. Lo scopo delle tabelle consiste nel fornire assistenza nella risoluzione dei problemi e nel rendere più agevole l'utilizzo del sistema.

Possibile errore	Correzione
Viene visualizzato il menu PRINCIPALE.	Si è premuto **F3** (Fine) o **F12** (Annullamento). Immettere `GO SETUP` e ripetere l'operazione.
Viene visualizzato un altro pannello, ad esempio il pannello Modifica opzioni di ripulitura.	Si è selezionata l'opzione errata dal Menu SETUP. Premere **F3** (Fine) per tornare al menu e ripetere l'operazione.
Viene nuovamente visualizzato il pannello Modifica opzioni di sistema dopo aver premuto il tasto **Invio**.	Cercare un messaggio di errore nella parte inferiore del pannello. Probabilmente è stato immesso un valore non consentito. Ricordarsi di utilizzare **F1** (Aiuto) se si desiderano ulteriori informazioni. Utilizzare **F5** (Rivisualizzazione) se si desidera che il sistema ripristini tutti i valori al loro stato precedente all'inizio dell'immissione. Ripetere l'operazione.

Possibile errore	Correzione
E' stato premuto il tasto **Invio** prima dell'immissione di tutte le scelte contenute nel pannello.	E' possibile utilizzare questo pannello ogni qualvolta sia necessario modificare i valori di sistema. Selezionare l'opzione **1** dal Menu SETUP ed immettere i valori mancanti la prima volta. **Attenzione: una volta che il sistema è operativo, non modificare il livello di sicurezza senza consultare un programmatore. Inoltre, non modificare il nome del sistema se si sta utilizzando iSeries Access o se si sta comunicando con un altro computer.**
E' stato premuto il tasto **Invio** invece di andare alla pagina successiva.	Selezionare nuovamente l'opzione **1** dal Menu SETUP ed andare alla pagina successiva per visualizzare la seconda pagina. Immettere le scelte e premere il tasto **Invio**.

Dopo aver immesso i valori di sistema, è necessario applicare i nuovi valori di sistema.

Applicare i nuovi valori di sistema

Dopo aver immesso i valori di sistema, è necessario applicare alcuni di questi valori. La maggior parte delle modifiche ai valori di sistema diventa immediatamente operativa. Tuttavia, durante la modifica del livello di sicurezza nel sistema, la modifica non diventa operativa fino a che non si arresta il sistema e lo si riavvia. Dopo aver verificato di aver immesso correttamente tutti i valori nel pannello Modifica opzioni di sistema, si è pronti ad applicare i nuovi valori.

Nota: collegare le stazioni di lavoro al sistema, se non lo si è già fatto. Quando si avvia il sistema, si configurano automaticamente le unità che utilizzano il formato di denominazione scelto nel pannello Modifica opzioni di sistema.

Utilizzare la seguente procedura per arrestare il sistema e riavviarlo. Quando si avvia il sistema, si attivano i valori immessi nel pannello Modifica opzioni di sistema.

1. Verificare di essersi collegati alla console e che nessun'altra stazione di lavoro sia collegata.
2. Verificare che l'interruttore della chiave di blocco sull'unità processore si trovi nella posizione Normal.
3. Dal Menu SETUP, selezionare l'opzione per le attività di attivazione e disattivazione.
4. Selezionare subito l'opzione di disattivazione del sistema, quindi quella di attivazione. Premere il tasto **Invio**.
5. Il sistema mostra un pannello che richiede di confermare la richiesta di spegnimento. Premere **F16** (Conferma).

Ciò causa l'arresto ed il riavvio automatico del sistema. Il pannello diventa vuoto per pochi minuti. Quindi dovrebbe visualizzarsi nuovamente il pannello di collegamento.

Dopo aver applicato i nuovi valori di sistema, è necessario creare un proprio profilo responsabile della riservatezza nel sistema.

Creare un profilo responsabile della riservatezza

Un **responsabile della riservatezza** nel sistema indica qualunque utente con la classe utente *SECOFR o con le autorizzazioni speciali *ALLOBJ e *SECADM.

Dopo aver applicato i valori di sistema dal pannello Modifica opzioni di sistema, creare un proprio profilo utente ed uno per l'altro responsabile della riservatezza. Per il futuro, utilizzare il proprio profilo, invece del profilo QSECOFR, quando si eseguono le funzioni del responsabile della riservatezza.

1. Collegarsi al sistema come QSECOFR e richiedere il Menu SETUP.

Si noti che il nome del sistema scelto viene visualizzato nella parte superiore destra del pannello di collegamento.

```
                  Collegamento
                              Sistema . . . . .
                              Sottosistema  . .
                              Video . . . . . .

Utente  . . . . . . . . . . . .   QSECOFR
Parola d'ordine . . . . . . . .   _________
Programma/procedura . . . . . .   _________
Menu  . . . . . . . . . . . . .   SETUP
Libreria corrente . . . . . . .   _________
```

2. Dal Menu SETUP, selezionare l'opzione *Gestione iscrizione utente*. Il pannello Gestione iscrizione utente elenca i profili attualmente presenti nel sistema.

   Nota: se viene visualizzato il pannello Gestione profili utente, premere **F21** (Selezione livello assistenza) e passare al livello di assistenza di base.
3. Per creare un nuovo profilo, immettere **1** (Aggiunta) nella colonna *Opz* (opzione) ed immettere il nome del profilo nella colonna *Utente*. Premere il tasto **Invio**.

```
                          Gestione iscrizione utente

Immettere le seguenti opzioni, quindi premere Invio.
  1=Aggiunta   2=Modifica   3=Copia   4=Elimin.   5=Visualizzaz.

Opz     Utente            Descrizione
1       JONESS
QDOC                          Profilo utente documento
QSECOFR                       Profilo utente responsabile riservatezza
```

4. Nel pannello Aggiunta utente, assegnarsi una parola d'ordine.
5. Riempire i campi mostrati nel pannello di esempio con le corrette informazioni.
6. Andare alla pagina successiva del pannello.

```
                          Aggiunta utente

Immettere le seguenti scelte e quindi premere Invio.

Utente  . . . . . . . . .   JONESS
Descrizione utente  . . .   Jones, Sharon
Parola d'ordine . . . . .   segreta
Tipo di utente  . . . . .   *SECOFR
Gruppo utente   . . . . .   *NONE

Limit. util. riga comandi   ______
Libreria predefinita  . .
Stampante predefinita . .   *WRKSTN
Programma di collegamento   *NONE
Libreria  . . . . . . .

Primo menu  . . . . . . .
Libreria  . . . . . . .
```

7. Riempire la seconda pagina del pannello e premere il tasto **Invio**.
8. Verificare i messaggi di conferma nella parte inferiore del pannello Gestione iscrizione utente.
9. Premere **F3** (Fine) per tornare al Menu SETUP.

```
                          Aggiunta utente

Immettere le seguenti scelte e quindi premere Invio.

Prog. tasto attenzione  .   *SYSVAL
  Libreria  . . . . . .
```

Possibile errore	Correzione
E' stato premuto il tasto **Invio** prima dell'immissione delle informazioni in tutti i campi.	Utilizzare l'opzione *Modifica* dal pannello Gestione iscrizione utente per modificare il profilo appena creato. Se il profilo non viene visualizzato nella lista, premere **F5** (Rivisualizzazione) ed andare alla pagina successiva per cercarlo.

Dopo aver creato un proprio profilo responsabile della riservatezza, è necessario modificare l'ID utente e le parole d'ordine per gli utenti degli strumenti di manutenzione. Consultare l'argomento Strumenti di manutenzione nell'Information Center.

Impostare i valori di sistema per la sicurezza

In questo argomento, utilizzare il comando Gestione valore di sistema (WRKSYSVAL) per modificare e visualizzare i valori di sistema.

Quali moduli sono necessari?

Immettere le informazioni dal modulo Selezione valori di sistema preparato in ″Pianificare la strategia di sicurezza globale.″

Per configurare i valori di sistema, completare le seguenti attività:

1. Modificare i valori di sistema per la sicurezza.
2. Modificare i singoli valori di sistema.

Collegarsi all'interfaccia della riga comandi

Utilizzare queste informazioni per collegarsi al sistema:

Profilo
Il proprio (E' richiesta l'autorizzazione *SECADM e *ALLOBJ)

Menu PRINCIPALE

Dopo essersi collegati, è possibile modificare i valori di sistema per la sicurezza.

Modificare i valori di sistema per la sicurezza

Dopo essersi collegato al sistema, utilizzare questa procedura per immettere i valori di sistema per la sicurezza visualizzati nella Parte 2 del modulo Selezione valori di sistema.

1. Nella riga comandi, immettere `WRKSYSVAL *SEC` e premere il tasto **Invio**. *SEC dopo il nome del comando indica che si desidera visualizzare solo i valori di sistema relativi alla sicurezza.
2. Nel pannello Gestione valore di sistema, immettere **2** (Modifica) nella colonna *Opzione* prima del valore di sistema che si desidera modificare. Se il valore di sistema che si desidera modificare non viene visualizzato nel pannello, andare alla pagina successiva fino a trovarlo.

```
                          Gestione valore di sistema

Inizio elenco da . . . .               Carattere iniziale valore di sistema
Sottoinsieme per tipo . . . . .   *SEC         F4 per lista

Immettere le opzioni e premere Invio.
  2=Modifica   5=Visualizzazione

        Valore di
Opz.    sistema      Tipo       Descrizione
        QINACTMSGQ   *SEC       Coda messaggi lavori inattivi
2       QLMTDEVSSN   *SEC       Limite sessioni unità
        QLMTSECOFR   *SEC       Limite accesso unità respons. riser.
        QMAXSGNACN   *SEC       Azione per tentativi non validi di collegamento
   .
   .
   .
```

3. Immettere la scelta per i valori di sistema e premere il tasto **Invio**. Viene nuovamente visualizzato il pannello Gestione valore di sistema.

```
                             Modifica valore di sistema
Val. di sistema  . . . :    QLMTDEVSSN
Descrizione  . . . . . :    Limite sessioni unità


Immettere la scelta e premere Invio.

  Limite sessione unità . . . .   0         0=Non
                                            1=Limite
```

4. Selezionare il messaggio di conferma nella parte inferiore del pannello.

Possibile errore	Correzione
Vengono visualizzati dei valori di sistema diversi da quelli mostrati nell'esempio del pannello Gestione valore di sistema.	Si è dimenticato di immettere *SEC. Confrontare il campo *Sottoinsieme per tipo* nella parte superiore del pannello con il pannello di esempio. Spostare il cursore nel campo *Sottoinsieme per tipo*. Immettere *SEC e premere il tasto **Invio**.
Il sistema non ha elaborato il comando. E' ancora visualizzato un menu.	Controllare i messaggi di errore nella parte inferiore del pannello. Probabilmente non è stato immesso correttamente il nome del comando. Ripetere l'operazione. Se il messaggio avvisa che non si ha l'autorizzazione, scollegarsi e ricollegarsi utilizzando un profilo con l'autorizzazione del responsabile della riservatezza.
Viene nuovamente visualizzato il pannello Modifica valore di sistema, dopo aver premuto il tasto **Invio**.	Controllare i messaggi di errore nella parte inferiore del pannello. Probabilmente non è stata immessa correttamente la scelta o è stato scelto un valore al di fuori dell'intervallo consentito. Utilizzare **F1** (Aiuto) per ulteriori informazioni.
Viene visualizzato un menu invece del pannello Gestione valore di sistema.	Probabilmente è stato premuto due volte il tasto **Invio**. Immettere WRKSYSVAL *SEC.
E' stato selezionato un valore di sistema che non si desidera modificare.	Premere **F12** (Annullamento) per tornare al pannello Gestione valore di sistema.

Che cosa indica * (Asterisco)?

Si è probabilmente notato che alcuni valori hanno un asterisco (*) che li precede. Il sistema utilizza l'asterisco per indicare la differenza fra i valori speciali e le parole normali. Ad esempio, quando si

specifica che la parola d'ordine in un profilo utente è *NONE, si intende che il sistema non consentirà a nessuno di collegarsi utilizzando tale profilo. Se si specifica che la parola d'ordine è NONE, è necessario che l'utente immetta i caratteri NONE come parola d'ordine.

Durante l'impostazione della sicurezza sul sistema, fare attenzione all'utilizzo dell'asterisco nelle istruzioni nei moduli.

Dopo aver modificato i valori di sicurezza per il sistema, è possibile modificare i singoli valori di sistema.

Modificare i singoli valori di sistema

Dopo aver modificato i valori di sistema per la sicurezza, è possibile modificare i singoli valori di sistema.

Ad esempio, il valore di sistema Intervallo supero tempo lavori scollegati (QDSCJOBITV) non è incluso come valore di sistema per la sicurezza. Non viene visualizzato nel sottoinsieme *SEC del pannello Gestione valore di sistema. Utilizzare tale procedura per modificare il valore di sistema QDSCJOBITV o qualunque singolo valore di sistema:

1. Immettere WRKSYSVAL QDSCJOBITV e premere il tasto **Invio**.
2. Nel pannello Gestione valore di sistema, immettere **2** (Modifica) nella colonna *opzione* prima di QDSCJOBITV.
3. Immettere la scelta per QDSCJOBITV.
4. Selezionare il messaggio di conferma.

```
                           Modifica valore di sistema
Val. di sistema  . . . :   QDSCJOBITV
Descrizione  . . . . . :   Intervallo prima chius. lav. scollegati


Immettere la scelta e premere Invio.

  Intervallo prima chius. lav. scollegati .........  300
```

Lista dei valori di sistema

Dopo aver immesso tutte le informazioni dal modulo Selezione valori di sistema, è possibile stampare una lista di tutti i valori di sistema per la sicurezza. Immettere WRKSYSVAL *SEC OUTPUT(*PRINT). Archiviare una copia della lista con il modulo Selezione valori di sistema. Ristampare la lista ogni qualvolta si modifichi un valore di sistema per la sicurezza.

Dopo aver immesso tutte le scelte per i valori di sistema dal modulo Selezione valori di sistema, è possibile prepararsi a caricare le applicazioni.

Eseguire le istruzioni relative alla sicurezza per il caricamento delle applicazioni

Dopo aver impostato i valori di sistema, è possibile prepararsi a caricare le applicazioni. Questo argomento tratta le istruzioni relative alla sicurezza necessarie per caricare le librerie dell'applicazione nel sistema. Dopo aver creato i profili e gli altri oggetti relativi alla sicurezza, ″Impostare l'autorizzazione pubblica e la proprietà″ e ″Impostare la sicurezza delle risorse″ mostrano il modo in cui stabilire la proprietà e l'autorizzazione per le applicazioni.

Se possibile, è necessario caricare le librerie dell'applicazione nel sistema prima di impostare i gruppi di utenti e i singoli profili. E' necessario fare riferimento agli oggetti dell'applicazione durante la creazione delle descrizioni lavoro e dei profili.

Nel caso in cui non sia possibile caricare le applicazioni prima di creare i profili di gruppo e singoli, potrebbero riceversi dei messaggi di avvertenza, simili ai seguenti:

- Il sistema non trova le librerie iniziali durante la creazione delle descrizioni lavoro.
- Il sistema non trova il programma o il menu iniziale durante la creazione dei profili.

Non è possibile verificare con esito positivo le descrizioni lavoro ed i profili fino a che non si carichino le librerie dell'applicazione.

Utilizzare i moduli Installazione dell'applicazione preparati in ″Pianificare l'installazione dell'applicazione.″

Per caricare ognuna delle applicazioni, completare queste attività:

1. Creare un profilo proprietario.
2. Caricare l'applicazione.

Collegarsi al sistema

- Per creare i profili proprietario:

  Profilo
  Il proprio (E' richiesta l'autorizzazione *SECADM)

  Menu PRINCIPALE

- Per caricare le librerie dell'applicazione:

  Verificare con il fornitore dell'applicazione se sia necessario collegarsi come responsabile della riservatezza o come proprietario dell'applicazione quando si caricano le librerie dell'applicazione.

Dopo essersi collegati, è possibile creare un profilo proprietario per le applicazioni.

Creare un profilo proprietario

Dopo essersi collegati al sistema, verificare con il Piano di installazione dell'applicazione se sia necessario creare dei profili prima di caricare l'applicazione. Per creare un profilo:

1. Immettere `CRTUSRPRF` (Creazione profilo utente) e premere **F4** (Richiesta).
2. Nel pannello Creazione profilo utente, riempire i campi secondo le istruzioni del programmatore o del fornitore dell'applicazione.
3. Utilizzare **F10** (Altri campi) ed andare alla pagina successiva per visualizzare gli ulteriori campi.

```
                      Creazione profilo utente (CRTUSRPRF)

Immettere le scelte e premere Invio.

Profilo utente . . . . . >
Parola d'ordine utente . . . . .   *USRPRF
Impost. parola d'ord. come scad.   *NO
Stato  . . . . . .   *ENABLED
Classe utente  . . . . . .   *USER
Livello di assistenza  . . . . .   *SYSVAL
Libreria corrente  . . . . . .   *CRTDFT
Progr. iniziale da richiamare. .   *NONE
  Libreria   . . . . . .
Menu iniziale  . . . . . .   PRINCIPALE
  Libreria   . . . . . .   *LIBL
Possibilità limitate . . . . . .   *NO
Testo 'descrizione'  . . . . . .   Proprietario di xxxxxx
```

4. Controllare i messaggi nella parte inferiore del pannello.

Nota: creare un profilo di gruppo esamina più dettagliatamente la creazione dei profili.

Dopo aver creato un proprietario per l'applicazione, è possibile iniziare a caricare l'applicazione.

Caricare l'applicazione

Seguire le istruzioni del fornitore dell'applicazione per caricare le librerie dell'applicazione. In ″Impostare l'autorizzazione pubblica e la proprietà,″ si sono apprese nozioni sull'impostazione della proprietà e dell'autorizzazione pubblica alle applicazioni.

Dopo aver caricato tutte le applicazioni, è possibile impostare i gruppi di utenti.

Impostare i gruppi di utenti

Dopo aver eseguito le istruzioni relative alla sicurezza per caricare le applicazioni è possibile impostare i gruppi di utenti. Si creano le librerie dei gruppi, le descrizioni lavoro ed i profili di gruppo. eseguire le istruzioni dell'intero argomento con uno dei gruppi di utenti, quindi tornare indietro e ripetere le istruzioni per ogni ulteriore gruppo. I pannelli di esempio mostrano le informazioni dai moduli Descrizione gruppi di utenti per il reparto Vendite e Marketing e per il Magazzino alla Azienda di giocattoli JKL.

Utilizzare i moduli Descrizione gruppo di utenti preparati in ″Pianificare i gruppi di utenti.″

Completare queste attività per impostare i gruppi di utenti:

1. Creare una libreria per il gruppo di utenti.
2. Creare una descrizione lavoro.
3. Creare un profilo di gruppo.

Collegarsi al sistema

Profilo
Il proprio (E' richiesta l'autorizzazione *SECADM)

Menu PRINCIPALE

Dopo essersi collegati, è possibile creare una libreria per il gruppo di utenti.

Creare una libreria per il gruppo

Dopo essersi collegati al sistema, è necessario creare una libreria per il gruppo di utenti. Se si ha intenzione di far condividere al gruppo una libreria per gli oggetti creati, ad esempio programmi d'interrogazione, creare la libreria prima di creare il profilo di gruppo:

1. Immettere `CRTLIB` (Creazione libreria) e premere **F4** (Richiesta).
2. Riempire il pannello. Il nome libreria deve essere il nome del profilo di gruppo.
3. Premere **F10** (Altri parametri).
4. Riempire l'autorizzazione pubblica per la libreria e per i nuovi oggetti creati nella libreria.
5. Premere il tasto **Invio**. Selezionare il messaggio di conferma.

```
                          Creazione libreria

Immettere le scelte e premere Invio.

Libreria  . . . . . .  DPTWH
Tipo libreria . . . . . .  *PROD
Testo 'descrizione' . . . . . .  Libreria magazzino

                          Parametri aggiuntivi

Autorizzazione . . . . . .  *USE
ID lotto memoria ausiliaria  . . .  1
Creazione autorizzazione . . . . .  *CHANGE
Creazione controllo oggetto  . . .  *SYSVAL
```

Possibile errore	Correzione
E' stato premuto il tasto **Invio** prima dell'immissione di una descrizione per la libreria.	Immettere **CHGLIB** e premere **F4** (Richiesta). Immettere il nome della libreria nel pannello di richiesta e premere il tasto **Invio**. Immettere la descrizione nel pannello Modifica libreria.
E' stato assegnato un nome errato alla libreria.	Utilizzare il comando Ridenominazione oggetto (RNMOBJ).

Dopo aver creato una libreria per il gruppo, è possibile creare una descrizione lavoro.

Creare una descrizione lavoro

Dopo aver creato una libreria per il gruppo, è possibile creare una descrizione lavoro per ogni gruppo.

Se le librerie necessarie per la lista iniziale delle librerie non sono ancora presenti nel sistema, si riceve un messaggio di avvertenza durante la creazione della descrizione lavoro.

1. Immettere **CRTJOBD** (Creazione descrizione lavoro) e premere **F4** (Richiesta).
2. Riempire questi campi:

   Descrizione lavoro:
   Uguale al nome del profilo di gruppo.

   Nome libreria:
   QGPL

   Testo:
   Descrizione gruppo
3. Premere **F10** (Altri parametri).
4. Andare alla pagina successiva al campo *Lista iniziale librerie*.

```
                  Creazione descrizione lavoro

Immettere le scelte e premere Invio.

Descrizione lavoro . . . . . .   DPTSM
  Libreria . . . . . . . . . .   QGPL
Coda lavoro  . . . . . . . . .   QBATCH
  Libreria . . . . . . . . . .     *LIBL
Priorità lavoro (su JOBQ)  . . .   5
Priorità emissione (su OUTQ) . . .   5
Unità di stampa  . . . . . . .   *USRPRF
Coda di emissione  . . . . . .   *USRPRF
  Libreria . . . . . . . . . .
Testo 'descrizione'  . . . . . .   Vendite e Marketing
```

5. Immettere un **+** (più) al posto di *SYSVAL nel campo *Lista iniziale librerie* per specificare che si desidera immettere una lista di valori. Premere il tasto **Invio**.

```
Codice contabile  . . . . . .   *USRPRF
   :
Controllo sintassi CL . . . . . .   *NOCHK
Lista iniziale librerie . . . . . .   +
              + per altri valori
```

6. Nel campo *Lista iniziale librerie*, immettere i nomi delle librerie contrassegnate (✓) dal modulo Descrizione gruppo di utenti:
   - Immettere un nome libreria per riga.
   - Includere QGPL e QTEMP. Ogni lavoro utilizza una libreria denominata QTEMP per memorizzare gli oggetti temporanei. **E' necessario che tutte le liste iniziali delle librerie siano dotati della libreria QTEMP**. Per la maggior parte delle applicazioni, è inoltre necessario che la libreria QGPL si trovi nella lista iniziale delle librerie.
   - Non è necessario includere la libreria corrente (predefinita) nella lista librerie. Il sistema aggiunge automaticamente tale libreria al collegamento.
7. Premere il tasto **Invio**. Controllare i messaggi. (Andare alla pagina successiva per visualizzare tutti i messaggi.)

```
Specificare più valori per

Immettere le scelte e premere Invio.

Lista iniziale librerie . . . . . .   CUSTLIB
                                      ITEMLIB
                                      COPGMLIB
                                      ICPGMLIB
                                      QGPL
                                      QTEMP
```

Possibile errore	Correzione
E' stato premuto il tasto **Invio** invece di **F10**.	Per inserire le librerie corrette nella lista iniziale delle librerie, immettere **CHGJOBD** (Modifica descrizione lavoro) e premere **F4**.

Possibile errore	Correzione
Si ricevono dei messaggi di errore quando si tenta di creare la descrizione lavoro.	Il messaggio di errore più comune ricorre quando si tenta di includere una libreria che non si trova nel sistema. Questo è un messaggio di avvertenza. La descrizione lavoro viene ancora creata con la libreria nella lista iniziale delle librerie. Non è possibile collegarsi con un profilo che specifichi la descrizione lavoro sino a quando la libreria non si trovi nel sistema. Se la libreria non si trova nel sistema, potrebbe non essere stato immesso correttamente il nome. Verificare il nome della libreria e ripetere l'operazione.

Dopo aver creato una descrizione lavoro, è possibile creare un profilo di gruppo.

Creare un profilo di gruppo

Dopo aver creato una descrizione lavoro, è possibile creare il profilo di gruppo. Per effettuare ciò, utilizzare le informazioni contenute nella Parte 2 del modulo Descrizione del gruppo di utenti.

1. Utilizzare il comando Gestione profili utente. Immettere `WRKUSRPRF *ALL`. Inizialmente, il pannello elenca i profili forniti dalla IBM.

   Nota: se viene visualizzato il pannello Gestione iscrizione utente, premere **F21** per passare al livello di assistenza intermedio.

2. Per creare un nuovo profilo, immettere **1** nella colonna *Opz* (opzione) ed il nome del profilo nella colonna *Profilo utente*. Premere il tasto **Invio**.

```
                         Gestione profili utente

Immettere le opzioni e premere Invio.
  1=Creaz. 2=Modifica   3=Copia   4=Eliminaz. 5=Visualizzaz.
  12=Gestione oggetti per proprietario

     Profilo
Opz  utente      Testo
1    DPTSM
     QDOC        Profilo utente documento
     QSECOFR     Profilo utente responsabile riservatezza
```

3. Immettere nel campo appropriato le informazioni contenute nel modulo Descrizione del gruppo di utenti.
4. Utilizzare il tasto **Tab** per ignorare tutti i campi per i quali si desidera utilizzare il valore predefinito.
5. Premere **F10** (Altri parametri).
6. Andare alla pagina successiva.

```
                      Creazione profilo utente (CRTUSRPRF)

Immettere le scelte e premere Invio.

Profilo utente . . . . . > DPTSM
Parola d'ordine utente . . . . .   *none
Impost. parola d'ord. come scad.   *NO
Stato  . . . . . .   *ENABLED
Classe utente  . . . . . .   *USER
Livello di assistenza  . . . . .   *SYSVAL
Libreria corrente  . . . . . .   *CRTDFT
Programma iniziale da richiam. .   cpsetup
  Libreria . . . . . .   cppgmlib
Menu iniziale  . . . . . .   cpmain
  Libreria   . . . . . .   cppgmlib
Possibilità limitate . . . . . .   *yes
Testo 'descrizione'  . . . . . .   Vendite e Marketing
```

7. Immettere i restanti campi contenuti nel modulo Descrizione del gruppo di utenti nelle altre pagine del pannello e premere il tasto **Invio**.

```
                        Creazione profilo utente

                           Parametri aggiuntivi

Autorizzazione speciale  . . . .   *USRCLS

   ⋮
Descrizione lavoro . . . . . .   DPTSM
  Libreria . . . . . .   QGPL
```

```
                      Creazione profilo utente

Autorizzazione gruppo  . . . . .   *NONE

   ⋮
Unità di stampa  . . . . . .   PRT03
```

8. Controllare i messaggi.

Importante

Un profilo di gruppo è semplicemente un tipo speciale di profilo utente. Molti messaggi e pannelli fanno riferimento ai profili di gruppo come utenti o profili utente. Il sistema sa solo che si è creato un profilo di gruppo se gli si aggiungono dei membri o gli si assegna un gid (numero identificazione gruppo).

Possibile errore	Correzione
E' stato premuto il tasto **Invio** prima dell'immissione di tutti i valori nel profilo di gruppo.	Premere **F5** (Rivisualizzazione) per aggiungere il profilo creato nel pannello Gestione profili utente. Utilizzare l'opzione **2** (Modifica) per correggere il profilo.
Si è creato un profilo con il nome errato.	Non è possibile modificare il nome di un profilo. Utilizzare l'opzione Copia (**3**) per creare un nuovo profilo con il nome corretto. Cancellare quindi (opzione **4**) il profilo con il nome errato.

Possibile errore	Correzione
Alcuni campi del modulo Descrizione del gruppo di utenti non vengono visualizzati nel pannello.	Verificare che si stia utilizzando il livello di assistenza intermedio. La versione livello di assistenza di base di Creazione profilo utente viene denominata pannello Aggiunta utente. Per modificare i livelli di assistenza, premere **F12** (Annullamento) per tornare al pannello Gestione iscrizione utente. Utilizzare **F21** per modificare i livelli di assistenza. Consultare ″Selezionare il livello corretto di assistenza.″
Alcune delle informazioni predefinite sono state involontariamente cancellate dal pannello Creazione profilo utente.	Se si lascia un campo vuoto, il sistema utilizza il valore predefinito durante la creazione del profilo utente. Se si desidera visualizzare i valori predefiniti, premere **F5** (Rivisualizzazione) per ripristinare l'intero pannello. Immettere nuovamente le informazioni.

Elencare i risultati

Elencare i nomi e le descrizioni di tutti i profili presenti nel sistema utilizzando il comando Visualizzazione utenti autorizzati (DSPAUTUSR). Immettere `DSPAUTUSR OUTPUT(*PRINT)`. Verificare che tutti i profili di gruppo abbiano una parola d'ordine *NONE.

Completare le seguenti attività prima di impostare i singoli utenti:

- Creare una descrizione lavoro per ogni gruppo di utenti.
- Se lo si desidera, creare una libreria per ogni gruppo.
- Creare un profilo di gruppo per ogni gruppo di utenti.

Impostare i singoli utenti

Durante l'impostazione dei gruppi di utenti, sono state completate le istruzioni per la creazione dei profili di gruppo. A questo punto, si creano i singoli profili per i membri dei gruppi.

Eseguire le istruzioni dell'intero argomento con i membri di un gruppo di utenti, quindi tornare indietro e ripetere le istruzioni per ogni ulteriore gruppo. I pannelli di esempio mostrano gli utenti dal Modulo Singolo profilo utente preparato da Sharon Jones per il reparto Vendite e Marketing e per il reparto Magazzino della Azienda di giocattoli JKL. E' possibile trovare copie di questi moduli in ″Pianificare i singoli profili utente.″

Utilizzare i moduli Singolo profilo utente preparati in ″Pianificare i singoli profili utente.″

Per creare i singoli profili per i membri dei gruppi, completare queste attività:

1. Creare una libreria personale. (facoltativo)
2. Copiare il profilo di gruppo.
3. Impostare la scadenza della parola d'ordine.
4. Creare ulteriori utenti. (facoltativo)

   Nota: ripetere le attività Creare una libreria personale e Creare ulteriori utenti fino a che ogni membro del gruppo non abbia un profilo utente.
5. Modificare le informazioni relative all'utente, se necessario.
6. Visualizzare i risultati.

Collegarsi al sistema

Profilo

Il proprio (E' richiesta l'autorizzazione *SECADM)

Menu SETUP

Creare una libreria personale

Per iniziare l'impostazione dei singoli utenti, potrebbe essere necessario creare una libreria personale per ogni membro per gli oggetti, ad esempio per i programmi d'interrogazione. Creare delle librerie personali prima di creare i singoli profili utente.

1. Immettere **CRTLIB** e premere **F4** (Richiesta).
2. Assegnare alla libreria lo stesso nome del profilo utente.
3. Premere **F10** (Altri parametri).
4. Riempire l'autorizzazione pubblica per la libreria e per i nuovi oggetti creati nella libreria.
5. Premere il tasto **Invio**. Selezionare il messaggio di conferma.

```
                          Creazione libreria

Immettere le scelte e premere Invio.

Libreria  . . . . . .   DPTSM
Tipo libreria . . . . . .   *PROD
Testo 'descrizione' . . . . . .   Libreria magazzino

                           Parametri aggiuntivi

Autorizzazione . . . . . .   *EXCLUDE
ID lotto memoria ausiliaria  . .   1
Creazione autorizzazione . . . .   *CHANGE
Creazione controllo oggetto  . .   *SYSVAL
```

Dopo aver creato una libreria personale, è possibile creare il singolo profilo copiando il profilo di gruppo.

Copiare il profilo di gruppo

Il profilo di gruppo ha un doppio ruolo:

1. Il sistema lo utilizza per determinare se un membro del gruppo abbia l'autorizzazione ad utilizzare un oggetto.
2. E' possibile utilizzarlo come modello per la creazione di profili utente per i singoli membri del gruppo.

Durante l'impostazione dei gruppi di utenti, sono stati creati i profili di gruppo. A questo punto, è possibile copiare un profilo di gruppo per creare un singolo profilo e copiarlo per creare altri profili nel gruppo.

1. Selezionare l'opzione Gestione iscrizione utente dal Menu SETUP.

   Nota: se viene visualizzato il pannello Gestione profili utente, utilizzare **F21** (Selezione livello assistenza) per passare al livello di assistenza di base.
2. Immettere **3** (Copia) nella colonna *Opz* che precede il gruppo utente. Il pannello mostra il pannello Copia utente. (Se il gruppo utente che si desidera copiare non è presente nel pannello, andare alla pagina successiva per trovarlo.) Il sistema lascia vuoto il campo del nome utente e riempie i restanti campi contenuti nel profilo di gruppo copiato.

```
                        Gestione iscrizione utente

Immettere le seguenti opzioni e quindi premere Invio.
  1=Aggiunta   2=Modifica   3=Copia   4=Elimin.   5=Visualizzaz.

Opz     Utente            Descrizione

        DPTSM          Reparto Vendite e Marketing
3       DPTWH          Reparto Magazzino
```

3. Immettere il nome e la descrizione del profilo utente che si sta creando.
4. Lasciare vuota la parola d'ordine. Il sistema utilizza automaticamente la stessa parola d'ordine del nuovo nome del profilo utente.
5. Immettere il nome del profilo di gruppo nel campo *Gruppo di utenti*.
6. Esaminare il modulo Singolo profilo utente per controllare se questo utente abbia altri valori diversi da quelli del gruppo. Immettere tali valori.
7. Andare alla pagina successiva.

```
                               Copia utente

Copia da utente  . . . . :   DPTWH

Immettere le seguenti scelte e quindi premere Invio.

Utente  . . . . . . . . . .   WILLISR
Descrizione utente  . . . .   Willis, Rose
Parola d'ordine . . . . . .
Tipo di utente  . . . . . .   *SYSOPR
Gruppo di utenti  . . . . .   DPTWH

Limitare utilizzo riga comandi   N

Libreria predefinita . . . . .   DPTWH
Stampante predefinita  . . . .   PRT04
Programma di collegamento  . .   *NONE
  Libreria . . . . . .

Primo menu  . . . . . .   ICMAIN
  Libreria  . . . . . .     ICPGMLIB
```

8. Apportare tutte le modifiche necessarie nella pagina successiva del pannello e premere il tasto **Invio**.
9. Verificare i messaggi di conferma nella parte inferiore del pannello Gestione iscrizione utente.

```
                               Copia utente

Copia da utente  . . . . :   DPTWH

Immettere le seguenti scelte e quindi premere Invio.

Prog. tasto attenzione  .   *SYSVAL
  Libreria  . . . . . .
```

Possibile errore	Correzione
Viene visualizzato il pannello Creazione profilo utente invece del pannello Copia utente.	Utilizzare **F12** (Annullamento) per tornare al pannello Gestione profili utente. Utilizzare **F21** per passare al livello di assistenza di base. Avviare nuovamente l'operazione di copia.

Possibile errore	Correzione
Il nome del profilo utente selezionato non corrisponde alla richiesta dell'utente.	Sebbene i nomi del profilo utente possano avere fino a 10 caratteri, i pannelli Copia utente e Aggiunta utente non supportano nomi con più di 8 caratteri. Scegliere un nome utente più breve o utilizzare il livello di assistenza intermedio per creare i singoli profili utente.

Verificare il profilo utente

Quando si crea il primo profilo singolo in un gruppo, è necessario verificarlo collegandosi con tale profilo. Verificare che venga visualizzato il primo menu corretto e che sia in esecuzione il programma di collegamento.

Se non si riesce ad effettuare il collegamento con il profilo, probabilmente il sistema non è riuscito a trovare qualche dato specificato nel profilo. Potrebbe trattarsi del programma di collegamento, della descrizione lavoro o di una delle librerie contenute nella lista iniziale librerie. Utilizzare il pannello Gestione emissione di stampa per trovare la registrazione lavori scritta quando si è tentato di effettuare il collegamento. La registrazione lavori indica quali errori si sono verificati.

Per le informazioni relative alla verifica ed alla diagnosi dei problemi durante l'effettuazione di modifiche relative alla sicurezza, consultare ″Verificare la sicurezza.″

Dopo aver verificato il profilo utente, è possibile impostare la scadenza della parola d'ordine.

Impostare la scadenza della parola d'ordine

Impostare i singoli profili in modo che agli utenti venga richiesto di modificare le proprie parole d'ordine la prima volta che si collegano. Il campo *Impostare parola d'ordine per scadere* non viene visualizzato nella versione livello di assistenza di base del pannello Copia utente. E' necessario modificarlo separatamente, dopo aver creato il profilo utente con la funzione di copia. Per modificare il campo *Impostare parola d'ordine per scadere*, immettere `CHGUSRPRF` *`nome-profilo`* `PWDEXP(*YES)`.

Nota: se si desidera verificare il profilo utente collegandosi con esso, effettuare la verifica *prima* di impostare la scadenza della parola d'ordine.

Possibile errore	Correzione
E' stato verificato un profilo e si è stati costretti a modificare la parola d'ordine.	Immettere **CHGUSRPRF** *nome-profilo* e premere **F4** (Richiesta). Impostare nuovamente la parola d'ordine sul nome del profilo utente. (Immettere il nome del profilo utente nel campo della parola d'ordine.) Immettere ***YES** nel campo *Impostare parola d'ordine per scadere*. E' necessario un livello di assistenza intermedio per effettuare questa operazione.

Dopo aver creato il primo singolo profilo utente, è possibile creare ulteriori utenti.

Creare altri utenti

Dopo aver copiato un profilo di gruppo per creare il primo singolo profilo, è possibile creare altri utenti. Copiare il primo singolo profilo utente per creare ulteriori membri del gruppo. Prestare attenzione ad ogni singolo profilo quando lo si crea tramite il metodo di copia. Esaminare il modulo Singolo profilo utente e verificare che siano stati modificati tutti i campi univoci per il nuovo profilo utente.

1. Nel pannello Gestione iscrizione utente, immettere **3** (Copia) prima del profilo utente che si desidera copiare.
2. Nel pannello Copia utente, immettere il nome e la descrizione del profilo.

3. Immettere le informazioni in tutti i campi univoci per il nuovo utente.

```
                        Gestione iscrizione utente

Immettere le seguenti opzioni e quindi premere Invio.
  1=Aggiunta   2=Modifica   3=Copia   4=Elimin.   5=Visualizzaz.

Opz     Utente            Descrizione

        DPTSM          reparto Vendite e Marketing
        DPTWH          reparto Magazzino
3       WILLISR        Willis, Rose
```

Possibile errore	Correzione
Il profilo che si desidera copiare non viene visualizzato nel pannello Gestione iscrizione utente.	Premere **F5** (Rivisualizzazione). Andare alla pagina precedente e a quella successiva. La lista è in ordine alfabetico per nome profilo.

Se si desidera modificare le informazioni relative ad un utente, consultare Modificare le informazioni relative ad un utente.

Modificare le informazioni relative ad un utente

Per alcuni utenti, potrebbe essere necessario impostare dei valori che non vengono visualizzati nel pannello Copia utente. Ad esempio, alcuni utenti potrebbero appartenere a più di un profilo di gruppo. Dopo aver creato un profilo utente utilizzando il metodo di copia, è possibile modificarlo.

1. Nel pannello Gestione iscrizione utente, premere **F21** per passare al livello di assistenza intermedio.
2. Nel pannello Gestione profili utente immettere **2** (Modifica) nella colonna *Opz* (opzione) accanto al profilo che si desidera modificare. Premere il tasto **Invio**.

```
                        Gestione profili utente

Immettere le opzioni e premere Invio.
  1=Creaz. 2=Modifica   3=Copia   4=Eliminaz. 5=Visualizzaz.
  12=Gestione oggetti per proprietario

     Profilo
Opz  utente         Testo
2    AMESJ       Ames, Janice
     DPTSM       Reparto Vendite e Marketing
     QDOC        Profilo utente documento
     QSECOFR     Profilo utente responsabile riservatezza
     WAGNERR     Wagner, Ray
     WILLISR     Willis, Rose
```

3. Nel pannello Modifica profilo utente, premere **F10** (Altri parametri).
4. Andare alla pagina successiva fino a trovare i campi che si desidera modificare. Ad esempio, se si desidera rendere l'utente un membro di ulteriori profili di gruppo, andare alla pagina successiva fino a quando non si trova il campo *gruppi aggiuntivi*.
5. Immettere i valori desiderati e premere il tasto **Invio**. Si ricevono dei messaggi di conferma, quindi viene visualizzato nuovamente il pannello Gestione profili utente.

```
                        Modifica profilo utente (CHGUSRPRF)

Immettere le scelte e premere Invio.

Memoria massima consentita . . .   *NOMAX
Priorità pianific. massima . . .   3
Descrizione lavoro . . . . . .   DPTWH
  Libreria   . . . . . .     QGPL
Profilo gruppo . . . . . .   DPTWH
Proprietario   . . . . . .   *GRPPRF
Autorizzazione gruppo. . . . . .   *USEE
Tipo autorizzazione gruppo . . .   *PGP
Gruppi aggiuntivi  . . . . . .   DPTIC
              + per altri valori
```

Dopo aver modificato le informazioni relative all'utente, è possibile visualizzare i risultati per verificare i profili.

Visualizzare i profili utente

Sono disponibili diversi metodi per visualizzare i profili creati.

Visualizzare un profilo
Utilizzare l'opzione **5** (Visualizzazione) contenuta nel pannello Gestione iscrizione utente o Gestione profili utente.

Lista di profili
Utilizzare il comando Visualizzazione profilo utente: DSPUSRPRF *nome-profilo* DETAIL(*BASIC) OUTPUT(*PRINT).

Visualizzare i membri del gruppo
Immettere DSPUSRPRF *nome-profilo-gruppo* *GRPMBR. E' possibile utilizzare OUTPUT(*PRINT) per stampare la lista.

Elencare tutti i profili
Per elencare i nomi e le descrizioni di tutti i profili, ordinati per gruppo, utilizzare il comando Visualizzazione utenti autorizzati: DSPAUTUSR SEQ(*GRPPRF) OUTPUT(*PRINT).

Prima di impostare l'autorizzazione pubblica e la proprietà, verificare che siano state completate queste attività:

- Terminare la creazione di tutti i singoli profili utente.
- Impostare la scadenza della parola d'ordine per ogni profilo.
- Stampare una lista di tutti i profili ordinati per gruppo e conservarla insieme ai moduli Descrizione del gruppo di utenti. Stampare nuovamente la lista quando si aggiungono nuovi utenti.

Capitolo 7. Impostare la sicurezza delle risorse

In questo argomento, si stabilisce l'autorizzazione pubblica e la proprietà agli oggetti, nonché l'autorizzazione specifica per le applicazioni. E' inoltre possibile impostare la sicurezza delle risorse per le stazioni di lavoro e le stampanti. Eseguire le istruzioni dell'intero argomento con una libreria, quindi tornare indietro e ripetere le istruzioni per ogni ulteriore libreria utilizzata da un'applicazione. Dopo aver completato l'impostazione della sicurezza delle risorse per un'applicazione, ripetere le istruzioni per le altre applicazioni.

Utilizzare queste procedure ogni qualvolta si installi una nuova applicazione nel sistema o durante l'impostazione della sicurezza delle risorse per un'applicazione esistente.

I pannelli di esempio riportati in questo argomento mostrano i moduli Lista di autorizzazioni, i moduli Descrizione della libreria e il modulo Sicurezza della coda di emissione e della stazione di lavoro per l'Azienda di giocattoli JKL. E' possibile trovare esempi di questi moduli in ″Impostare l'autorizzazione pubblica e la proprietà.″

Quali moduli sono necessari?

- I moduli Installazione dell'applicazione preparati in ″Pianificare l'installazione dell'applicazione.″
- I moduli Lista di autorizzazioni preparati in ″Raggruppare gli oggetti.″
- I moduli Descrizione della libreria preparati in ″Determinare la proprietà delle librerie e degli oggetti.″
- Il modulo Sicurezza della coda di emissione e della stazione di lavoro preparato in ″Proteggere l'emissione di stampa″ e in ″Proteggere le stazioni di lavoro.″
- Il modulo Responsabilità del sistema preparato in ″Pianificare la strategia di sicurezza globale.″

E' possibile impostare la sicurezza delle risorse in vari modi. La sequenza delle istruzioni di questo argomento corrisponde all'ordine delle informazioni contenute nei moduli Installazione dell'applicazione, nei moduli Lista di autorizzazioni e nel modulo Descrizione della libreria:

1. Impostare l'autorizzazione pubblica e la proprietà.
2. Creare le liste di autorizzazioni.
3. Proteggere gli oggetti con una lista di autorizzazioni.
4. Aggiungere gli utenti alle liste di autorizzazioni.
5. Impostare tutte le autorizzazioni specifiche.
6. Proteggere l'emissione di stampa.
7. Proteggere le stazioni di lavoro.
8. Limitare l'accesso alla coda messaggi dell'operatore di sistema.

Impostare l'autorizzazione pubblica e la proprietà

In questo argomento, si stabilisce l'autorizzazione pubblica e la proprietà per le librerie dell'applicazione, per le librerie di gruppo e per le librerie personali. Eseguire le istruzioni dell'intero argomento con un'applicazione, quindi tornare indietro e ripetere le istruzioni per ogni ulteriore applicazione. I pannelli di esempio mostrano i moduli Installazione dell'applicazione preparati da Sharon Jones per l'applicazione Ordini cliente in ″Pianificare l'installazione dell'applicazione.″

Utilizzare le procedure contenute in questo argomento ogni qualvolta si installi una nuova applicazione nel sistema o quando si imposta la sicurezza per un'applicazione esistente.

Utilizzare i moduli Installazione dell'applicazione preparati in ″Pianificare l'installazione dell'applicazione.″

Per impostare la proprietà e l'autorizzazione pubblica, completare queste attività:

1. Creare il profilo proprietario.
2. Modificare la proprietà della libreria.
3. Impostare la proprietà degli oggetti dell'applicazione.
4. Impostare l'accesso pubblico ad una libreria.
5. Impostare l'autorizzazione pubblica per tutti gli oggetti di una libreria.
6. Impostare l'autorizzazione pubblica per i nuovi oggetti.
7. Gestire le librerie di gruppo e le librerie personali.

Collegarsi al sistema

Profilo
Il proprio (E' richiesta l'autorizzazione *ALLOBJ)

Menu PRINCIPALE

Creare un profilo proprietario

Se il profilo proprietario non esiste ancora, effettuare le seguenti operazioni:

- Utilizzare il comando CRTUSRPRF (Creazione profilo utente) per crearlo. Impostare la parola d'ordine su *NONE.

Se il profilo proprietario esiste già, effettuare le seguenti operazioni:

- Utilizzare il comando Modifica profilo utente (CHGUSRPRF) per impostare la parola d'ordine su *NONE.

Dopo aver creato il profilo utente, è possibile modificare la proprietà della libreria.

Modificare la proprietà della libreria

Questa operazione modifica la proprietà di una libreria, non gli oggetti in essa contenuti.

Attenzione: consultare il fornitore dell'applicazione prima di modificare la proprietà degli oggetti dell'applicazione. Alcune applicazioni utilizzano funzioni che si basano su una specifica proprietà oggetto.

1. Immettere CHGOBJOWN (Modifica proprietario oggetto) e premere **F4** (Richiesta).
2. Immettere il nome della libreria, il tipo di oggetto (*LIB) ed il nuovo proprietario.
3. Controllare i messaggi di conferma.

```
                      Modifica proprietario oggetto (CHGOBJOWN)

Immettere le scelte e premere Invio.

Oggetto  . . . . . . . . . . . . > COPGMLIB
  Libreria . . . . . . . . . . . >   *LIBL       Nome,
Tipo oggetto . . . . . . . . . . > *LIB
Nuovo proprietario . . . . . . .   COWNER
Autoriz. proprietario corrente .   *REVOKE
```

Possibile errore	Correzione
Si ricevono dei messaggi di errore.	Il messaggio più comune indica che non è stata trovata la libreria o che non è stato trovato il nuovo profilo proprietario. Controllare gli errori di immissione e ripetere l'operazione.

Dopo aver modificato la proprietà della libreria, è possibile impostare la proprietà per gli oggetti dell'applicazione.

Impostare la proprietà degli oggetti dell'applicazione

La modifica della proprietà degli oggetti dell'applicazione è un'attività monotona, poiché è necessario modificare ogni oggetto singolarmente. Se possibile, chiedere al programmatore o al fornitore dell'applicazione di stabilire la proprietà.

Elencare gli oggetti contenuti in una libreria

Prima di modificare la proprietà, stampare una lista di tutti gli oggetti contenuti nella libreria, utilizzando il comando Visualizzazione libreria. E' possibile utilizzarlo sotto forma di lista di controllo. Immettere `DSPLIB` *`nome-libreria`* `*PRINT`.

Scegliere il metodo migliore

Scegliere uno di questi due metodi per modificare la proprietà degli oggetti contenuti nelle librerie dell'applicazione:

Tabella 61. Metodi per la modifica della proprietà dell'oggetto

Metodo	Funzioni	Occasioni di utilizzo
Il comando Gestione oggetti per proprietario	Mostra un pannello che elenca tutti gli oggetti appartenenti ad un profilo. Si utilizza un'opzione presente nel pannello per modificare il proprietario di un oggetto.	Questo metodo è più facile da utilizzare. Tuttavia, se gli oggetti appartengono a QPGMR o a QSECOFR, l'IBM non consiglia tale metodo. A tali profili appartengono molti oggetti, per cui il pannello della lista risulterebbe molto grande.
Il comando Modifica proprietà oggetto	Richiede l'utilizzo di un comando separato per ogni oggetto. Tuttavia, è possibile utilizzare *Duplicazione* (**F9**) per ripetere il comando precedente e ridurre l'immissione richiesta.	Questo metodo è più veloce se gli oggetti appartengono a QPGMR o a QSECOFR.

Utilizzare il comando Gestione oggetti per proprietario (WRKOBJOWN)

Utilizzare questo metodo per modificare la proprietà degli oggetti contenuti in una libreria se ai profili forniti dalla IBM, ad esempio QPGMR o QSECOFR, *non* appartengono gli oggetti:

1. Immettere `WRKOBJOWN` *`nome-profilo-proprietario`*. Il pannello visualizza una lista di tutti gli oggetti che appartengono a quel profilo utente.
2. Immettere **9** (Modifica proprietario) prima di ogni oggetto contenuto nella libreria nella quale si sta lavorando.
3. Nella riga *parametri o comandi* nella parte inferiore del pannello, immettere `NEWOWN(`*`nome-profilo-proprietario`*`)` e premere il tasto **Invio**.
4. Il sistema modifica il proprietario di ogni oggetto indicato con il nuovo proprietario immesso nella parte inferiore. Si ricevono dei messaggi di conferma nella parte inferiore del pannello. Gli oggetti non vengono più visualizzati nel pannello perché non appartengono più al profilo.
5. Ripetere le operazioni 2 e 4 fino a che non si sia modificata la proprietà di tutti gli oggetti presenti nella libreria.

```
                          Gestione oggetti per proprietario

Profilo utente . . . . . :   OLDOWNER

Immettere le opzioni e premere Invio.
  2=Modifica autorizzazione  4=Eliminaz.   5=Visualizzaz. autore
  8=Visualizza descrizione   9=Modifica proprietario

Opz  Oggetto       Libreria       Tipo      Attributo
     COPGMMSG      COPGMLIB      *MSGQ
9    CUSTMAS       CUSTLIB       *FILE
9    CUSTMSGQ      CUSTLIB       *MSGQ
     ITEMMSGQ      ITEMLIB       *MSGQ


   :

Parametri o comandi
===> NEWOWN(COWNER)
F3=Fine   F4=Richies. F5=Rivisual. F9=Duplicazione
F18=Fine
```

Possibile errore	Correzione
Viene visualizzato il pannello Modifica proprietario oggetto.	Viene visualizzato questo pannello se si specifica l'opzione **9** (Modifica proprietario) e non si immette alcun parametro nella parte inferiore del pannello Gestione oggetti per proprietario. Questo pannello viene visualizzato anche se non si immettono correttamente i parametri. Premere **F12** (Annullamento) per tornare al pannello Gestione oggetti per proprietario. Ripetere l'operazione. Verificare di aver immesso il parametro secondo quanto riportato nell'esempio.

E' possibile utilizzare il comando modifica proprietario oggetto per modificare la proprietà degli oggetti appartenenti a QPGMR o a QSECOFR.

Utilizzare il comando Modifica proprietario oggetto

Utilizzare questo metodo per modificare il proprietario degli oggetti contenuti in una libreria se a QPGMR o a QSECOFR *appartengono* gli oggetti.

1. Immettere CHGOBJOWN e premere **F4** (Richiesta).
2. Immettere le informazioni contenute nel pannello per il primo oggetto della lista e premere il tasto **Invio**.

```
                      Modifica proprietario oggetto (CHGOBJOWN)

Immettere le scelte e premere Invio.

Oggetto . . . . . > CUSTMAS
  Libreria  . . . . . >   CUSTLIB
Tipo oggetto  . . . . . > *FILE
Nuovo proprietario  . . . . . .   COWNER
Autoriz. proprietario corrente  .   *REVOKE
```

3. Si riceve un messaggio di conferma indicante che la proprietà dell'oggetto è stata modificata. Controllare che la voce sia presente nella lista.
4. Premere **F9** (Duplicazione) per richiamare il comando immesso.
5. Premere **F4** (Richiesta). Nel pannello Modifica proprietario oggetto, immettere le informazioni per l'oggetto successivo nella libreria e premere il tasto **Invio**.

6. Ripetere le istruzioni quattro e cinque per ogni oggetto presente nella libreria.

Verificare il lavoro

Per verificare che sia stata modificata la proprietà di tutti gli oggetti della libreria, utilizzare il comando Gestione oggetti per proprietario. Immettere WRKOBJOWN *nuovo-profilo-proprietario*. Confrontare il pannello con la lista degli oggetti della libreria.

Dopo aver modificato la proprietà degli oggetti della libreria, è possibile impostare l'accesso pubblico alla libreria.

Impostare l'accesso pubblico alla libreria

Dopo aver impostato la proprietà degli oggetti dell'applicazione, è possibile utilizzare il comando Editazione autorizzazione oggetto (EDTOBJAUT) per modificare l'autorizzazione pubblica alla libreria:

1. Immettere EDTOBJAUT *nome-libreria* *LIB.
2. Spostare il cursore giù fino alla riga **PUBLIC*.
3. Immettere l'autorizzazione alla libreria che si desidera assegnare al pubblico e premere il tasto **Invio**.

```
                          Editazione autorizzazione oggetto

Oggetto . . . . . :   CUSTLIB         Proprietario  . . . . . :   COWNER
  Libreria  . . . . :     QSYS        Gruppo principale  . . . :   *NONE
Tipo oggetto  . . . :   *LIB

Immettere le modifiche apportate alle autorizzazioni correnti, quindi premere Invio.

  Oggetto protetto dalla lista di autorizzazioni . . . . . .   *NONE

                        Autorizzazione
Utente      Gruppo      oggetto
COWNER                  *ALL
*PUBLIC                 *CHANGE
```

4. Il pannello mostra la nuova autorizzazione.

E' ora possibile impostare l'autorizzazione pubblica per tutti gli oggetti di una libreria.

Impostare l'autorizzazione pubblica per tutti gli oggetti di una libreria

Utilizzare il comando Revoca autorizzazione oggetto (RVKOBJAUT) per eliminare l'autorizzazione pubblica corrente per gli oggetti di una libreria. Utilizzare il comando Concessione autorizzazione oggetto (GRTOBJAUT) per impostare l'autorizzazione pubblica per tutti gli oggetti di una libreria:

1. Immettere RVKOBJAUT e premere **F4** (Richiesta).
2. Compilare il pannello come mostrato, sostituendo il nome della libreria dell'applicazione, e premere il tasto **Invio**.

```
                    Revoca autorizzazione oggetto (RVKOBJAUT)

Immettere le scelte e premere Invio.

Oggetto . . . . . .   *all
  Libreria  . . . . . .   custlib
Tipo oggetto  . . . . . .   *all
Utenti  . . . . . .   *public
              + per altri valori
Autorizzazione  . . . . . .   *all
```

Nota: se la libreria contiene molti oggetti, il sistema potrebbe impiegare alcuni minuti per l'elaborazione la richiesta.

3. Immettere GRTOBJAUT e premere **F4** (Richiesta).
4. Compilare il pannello come mostrato, sostituendo il nome della libreria dell'applicazione e l'autorizzazione desiderata e premere il tasto **Invio**.

```
                    Concessione autorizzazione oggetto (GRTOBJAUT)

Immettere le scelte e premere Invio.

Oggetto . . . . . .   *all
  Libreria  . . . . . .   custlib
Tipo oggetto  . . . . . .   *all
Utenti  . . . . . .   *public
             + per altri valori
Autorizzazione  . . . . . .   *use
```

Nota: se la libreria contiene molti oggetti, il sistema potrebbe impiegare alcuni minuti per l'elaborazione la richiesta.

Dopo aver completato l'impostazione dell'autorizzazione pubblica per tutti gli oggetti di una libreria, è dunque possibile utilizzare la registrazione lavori per verificare il lavoro.

Utilizzare la registrazione lavori per verificare il lavoro

Quando si utilizza il comando GRTOBJAUT per apportare più modifiche all'autorizzazione, esaminare la registrazione lavori per verificare che le modifiche siano state effettivamente apportate.

1. Immettere DSPJOBLOG (Visualizzazione registrazione lavori).
2. Premere **F10** (Visualizzazione messaggi dettagliati).
3. E' necessario disporre di un messaggio relativo alla modifica dell'autorizzazione per ogni oggetto della libreria. Verificare gli oggetti presenti nella lista man mano che si esaminano i messaggi.

```
                          Visualizzazione messaggi
    Sistema:   RCHASxxx
Lavoro . . :   QPADEV0010    Utente . . :   JCHEIDEL      Numero . . . :   025457

7 > GRTOBJAUT OBJ(CUSTLIB/*ALL) OBJTYPE(*ALL) USER(*PUBLIC) AUT(*USE)
  Autorizzazione assegnata all'utente *PUBLIC per l'oggetto CUSTMAS nel tipo oggetto CUSTLIB
    *FILE.
  Autorizzazione assegnata all'utente *PUBLIC per l'oggetto CUSTMSGQ nel tipo oggetto CUSTLIB
    *MSGQ.
  Autorizzazione assegnata a 2 oggetti. Non assegnata a 0 oggetti. Parzialmente assegnata a 0
    oggetti.
  Autorizzazione oggetto concessa.
7>> dspjoblog
```

Possibile errore	Correzione
La registrazione lavori indica che tale autorizzazione non è stata modificata per alcuni oggetti della libreria.	Utilizzare Aiuto (**F1**) per ulteriori informazioni sul messaggio. Utilizzare EDTOBJAUT per impostare l'autorizzazione per tali oggetti singolarmente.

E' ora possibile impostare l'autorizzazione pubblica per i nuovi oggetti.

Impostare l'autorizzazione pubblica per i nuovi oggetti

La descrizione della libreria ha un parametro denominato Creazione autorizzazione (CRTAUT), che determina l'autorizzazione pubblica per i nuovi oggetti creati nella libreria. I comandi che creano oggetti

utilizzano l'autorizzazione CRTAUT della libreria degli oggetti come impostazione predefinita. E' necessario rendere l'autorizzazione CRTAUT per una libreria uguale all'autorizzazione pubblica per la maggior parte degli oggetti esistenti nella libreria.

1. Immettere `CHGLIB` *`nome-libreria`* e premere **F4** (Richiesta).
2. Premere **F10** (Altri parametri).
3. Immettere la scelta nel campo *Creazione autorizzazione*.

```
                     Modifica libreria (CHGLIB)

Immettere le scelte e premere Invio.

Libreria  . . . . . . . . . . . . > CUSTLIB
Tipo libreria . . . . . . . . . .   *PROD
Testo 'descrizione' . . . . . . .   'Record cliente'


                            Parametri aggiuntivi

Creazione autorizzazione . . . .   *CHANGE
Creazione controllo oggetto  . .   *SYSVAL
```

Se si imposta CRTAUT su *SYSVAL, il sistema utilizza l'impostazione corrente per il valore di sistema QCRTAUT durante la creazione di un nuovo oggetto nella libreria. L'impostazione di un'autorizzazione CRTAUT specifica per ogni libreria consente di proteggere da future modifiche al valore di sistema QCRTAUT.

E' ora possibile gestire le librerie di gruppo e personali.

Gestire le librerie di gruppo e personali

Al profilo appartengono le librerie di gruppo e personali create durante l'impostazione dei gruppi di utenti e dei singoli utenti.

Utilizzare le procedure appena trattate per modificare la proprietà delle librerie di gruppo con il profilo di gruppo e per modificare la proprietà delle librerie personali con i singoli profili utente. Utilizzare il comando EDTOBJAUT.

Impostare il parametro Creazione autorizzazione per ogni libreria di gruppo e personale per determinare l'autorizzazione pubblica per ogni nuovo oggetto presente in quelle librerie. Utilizzare il comando CHGLIB.

Prima di avviare la creazione delle liste di autorizzazioni, completare queste attività:

- Utilizzare i moduli Installazione dell'applicazione ed i moduli Descrizione della libreria, per verificare di aver stabilito la proprietà e l'autorizzazione pubblica per tutte le librerie dell'applicazione.
- Impostare la proprietà e creare l'autorizzazione per tutte le librerie di gruppo e personali create.

  Nota: è possibile visualizzare una lista di tutte le librerie presenti nel sistema immettendo `DSPOBJD *ALL *LIB *PRINT`.

Creare una lista di autorizzazioni

Dopo aver impostato l'autorizzazione pubblica e la proprietà, si è pronti a impostare le liste di autorizzazioni. Utilizzando le informazioni contenute nei moduli Lista di autorizzazioni, creare tutte le liste di autorizzazioni necessarie per la protezione della libreria. Utilizzare il comando Creazione lista di autorizzazione (CRTAUTL):

1. Immettere `CRTAUTL` e premere **F4** (Richiesta).

2. Immettere le informazioni contenute nel modulo Lista di autorizzazioni.
3. Premere **F10** (Altri parametri).
4. Utilizzare il parametro delle autorizzazioni per specificare l'autorizzazione pubblica per gli oggetti protetti dalla lista.
5. Controllare i messaggi di conferma.

```
                    Creazione lista di autorizzazione (CRTAUTL)

Immettere le scelte e premere Invio.

Lista di autorizzazione  . . . .   custlst1
Testo 'descrizione'  . . . . . .   File cancellati a

                             Parametri aggiuntivi

Autorizzazione  . . . . . . . . . .   *ALL
```

Possibile errore	Correzione
Il nome della lista non è stato immesso correttamente.	Non è possibile modificare il nome di una lista, se è stata creata dal sistema. Eliminare la lista (DLTAUTL) e ripetere l'operazione.
Si è dimenticato di specificare l'autorizzazione pubblica per la lista.	Utilizzare il comando Editazione lista di autorizzazione (EDTAUTL).

E' ora possibile proteggere gli oggetti con una lista di autorizzazioni.

Proteggere gli oggetti con una lista di autorizzazioni

Dopo aver creato una lista di autorizzazioni, utilizzare il comando Editazione autorizzazione oggetto (EDTOBJAUT) per proteggere le voci elencate nel modulo Lista di autorizzazioni:

1. Immettere EDTOBJAUT e premere **F4** (richiesta).
2. Riempire il pannello di richiesta e premere il tasto **Invio**.
3. Nel pannello Editazione autorizzazione oggetto, immettere il nome lista di autorizzazioni.
4. Se l'autorizzazione pubblica per l'oggetto proviene dalla lista di autorizzazioni, modificare l'autorizzazione pubblica in *AUTL.
5. Ripetere queste istruzioni per ogni oggetto contenuto nel modulo Lista di autorizzazioni.

```
                          Editazione autorizzazione oggetto

Oggetto . . . . . :   ARFILE01        Proprietario  . . . . . OWNAR
Libreria .  . . . . :   CUSTLIB         Gruppo principale  . . .    *NONE
Tipo oggetto  . . . . :   *FILE

Immettere le modifiche alle autorizzazioni correnti e premere Invio.

Oggetto protetto dalla lista di autorizzazioni . . . . . CUSTLST1

                         Autorizzazione
Utente      Gruppo       oggetto
OWNER                    *ALL
*PUBLIC                  *AUTL
```

E' ora possibile aggiungere utenti ad una lista di autorizzazioni.

Aggiungere utenti ad una lista di autorizzazioni

Dopo aver protetto gli oggetti con una lista di autorizzazioni, utilizzare il comando Editazione lista di autorizzazione (EDTAUTL) per aggiungere gli utenti elencati nel modulo Lista di autorizzazioni:

1. Immettere EDTAUTL *nome-lista-autorizzazioni*.
2. Nel pannello Editazione lista di autorizzazione, premere **F6** (Aggiunta nuovi utenti).
3. Immettere i nomi degli utenti o dei gruppi e l'autorizzazione necessarie per le voci contenute nella lista e premere il tasto **Invio**.
4. I nuovi utenti dovrebbero comparire nella lista.

```
                            Aggiunta nuovi utenti

Oggetto  . . . . . :   WSLST1          Propr. . .
  Libreria . . . . . :     QSYS

Immettere nuovi utenti e premere Invio.

             Autor.    Gest.
Utente       oggetto   elenco
QSECOFR     *CHANGE
```

Possibile errore	Correzione
All'utente o al gruppo è stata assegnata l'autorizzazione errata per la lista.	E' possibile modificare l'autorizzazione nel pannello Editazione lista di autorizzazione.
E' stato aggiunto un utente o un gruppo errato alla lista.	E' possibile eliminare un utente o un gruppo utilizzando il comando Eliminazione voce lista autorizzazioni (RMVAUTLE o è possibile immettere degli spazi vuoti nell'autorizzazione dell'utente nel pannello Editazione lista di autorizzazione.

Verificare il lavoro

Utilizzare il comando Visualizzazione lista di autorizzazione (DSPAUTL) per elencare tutte le autorizzazioni dell'utente nella lista di autorizzazioni. Utilizzare **F15** dal pannello per elencare tutti gli oggetti protetti dalla lista di autorizzazioni.

Prima di configurare le autorizzazioni specifiche, completare queste attività:

- Utilizzare il comando CRTAUTL per creare le liste di autorizzazioni necessarie per l'applicazione.
- Proteggere gli oggetti con le liste di autorizzazioni utilizzando il comando EDTOBJAUT.
- Aggiungere gli utenti alle liste di autorizzazioni utilizzando il comando EDTAUTL.

Impostare le autorizzazioni specifiche

In ″Impostare l'autorizzazione pubblica e la proprietà,″ si è appreso come utilizzare il comando GRTOBJAUT per impostare l'autorizzazione pubblica per tutti gli oggetti di una libreria, in base alle informazioni contenute nella Parte 1 del modulo Descrizione della libreria. A questo punto, è possibile utilizzare il comando Editazione autorizzazione oggetto (EDTOBJAUT) per impostare l'autorizzazione specifica per la librerie e gli oggetti della libreria, in base alle informazioni contenute nella Parte 2 del modulo Descrizione della libreria.

Consultare questi argomenti per impostare le autorizzazioni specifiche:

- Impostare l'autorizzazione specifica per una libreria.
- Impostare l'autorizzazione specifica per un oggetto.
- Impostare l'autorizzazione per più di un oggetto alla volta.

Impostare l'autorizzazione specifica per una libreria

Una libreria è in realtà un tipo di oggetto speciale. Si imposta l'autorizzazione per una libreria nello stesso modo in cui si imposta l'autorizzazione per ogni altro oggetto, utilizzando il comando EDTOBJAUT. Tutte le librerie sono ubicate nella libreria fornita dall'IBM denominata QSYS. I pannelli contenuti nei seguenti esempi utilizzano la Parte 2 del modulo Descrizione della libreria per la libreria CONTRACTS della Azienda di giocattoli JKL:

Elencare le autorizzazioni specifiche per gli oggetti della libreria				
Profilo di gruppo o profilo utente	Nome oggetto	Tipo oggetto	Autorizzazione necessaria	Lista di autorizzazioni
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

1. Immettere EDTOBJAUT e premere **F4** (Richiesta).
2. Riempire il pannello di richiesta e premere il tasto **Invio**.

```
                    Editazione autorizzazione oggetto (EDTOBJAUT)
Immettere le scelte e premere Invio.

Oggetto . . . . . .   CONTRACTS
  Libreria  . . . . .   QSYS
Tipo oggetto  . . . . .   *LIB
```

3. Nel pannello Editazione autorizzazione oggetto, premere **F6** (Aggiunta nuovi utenti) per assegnare l'autorizzazione agli utenti che non sono elencati nel pannello.
4. Premere il tasto **Invio**.

```
                              Aggiunta nuovi utenti

Oggetto . . . . . :   CONTRACTS       Proprietario  . . . . . :   OWNCP
  Libreria  . . . . :     QSYS        Gruppo principale . . . . :   *NONE
Tipo oggetto  . . . :   *LIB


Immettere nuovi utenti e premere Invio.

                    Autorizzazione
Utente              oggetto
DPTSM       *USE
DPTMG       *USE
```

5. Il pannello Editazione autorizzazione oggetto dovrebbe corrispondere alle informazioni contenute nelle Parti 1 e 2 del modulo Descrizione della libreria.

```
                            Editazione autorizzazione oggetto

Oggetto . . . . . :   CONTRACTS       Proprietario  . . . . . :   OWNCP
  Libreria  . . . . :     QSYS        Gruppo principale . . . . :   *NONE
Tipo oggetto  . . . :   *LIB

Immettere le modifiche apportate alle autorizzazioni correnti, quindi premere Invio.

  Oggetto protetto dalla lista di autorizzazioni . . . . . .   *NONE

                         Autorizzazione
Utente        Gruppo     oggetto
OWNCP                    *ALL
DPTSM                    *USE
DPTMG                    *USE
*PUBLIC                  *EXCLUDE
```

L'autorizzazione Autorizzazione pubblica per nuovi oggetti (CRTAUT) non viene visualizzata nel pannello Editazione autorizzazione oggetto per una libreria. Utilizzare il comando Visualizzazione libreria (DSPLIB) per visualizzare CRTAUT per una libreria.

E' inoltre possibile utilizzare tale procedura per impostare l'autorizzazione specifica per un oggetto presente nel sistema.

E' ora possibile impostare l'autorizzazione specifica per un oggetto.

Impostare l'autorizzazione specifica per un oggetto

La procedura per l'impostazione dell'autorizzazione specifica per un oggetto contenuto in una libreria dell'applicazione è la stessa dell'impostazione dell'autorizzazione specifica per una libreria. L'esempio utilizza la Parte 2 del modulo Descrizione della libreria per la libreria COPGMLIB dell'Azienda di giocattoli JKL:

Tabella 62. Modulo Descrizione della libreria dell'Azienda di giocattoli JKL

Profilo di gruppo o profilo utente	Nome oggetto	Tipo oggetto	Autorizzazione necessaria	Lista di autorizzazioni
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

1. Immettere `EDTOBJAUT` e premere **F4** (Richiesta).
2. Inserire le informazioni nel pannello di richiesta e premere il tasto **Invio**.
3. Inserire le informazioni relative all'autorizzazione nel pannello Editazione autorizzazione oggetto e premere il tasto **Invio**.

```
                          Editazione autorizzazione oggetto

Oggetto . . . . . :   COMSGQ01        Proprietario  . . . . . :   OWNCO
  Libreria  . . . . :     COPGMLIB      Gruppo principale  . . . :   *NONE
Tipo oggetto  . . . . :   *MSGQ

Immettere le modifiche apportate alle autorizzazioni correnti, quindi premere Invio.

  Oggetto protetto dalla lista di autorizzazioni . . . . . .   *NONE

                      Autorizzazione
Utente        Gruppo   oggetto
OWNCO                   *ALL
*PUBLIC                 *CHANGE
```

E' ora possibile impostare l'autorizzazione per più di un oggetto alla volta.

Impostare l'autorizzazione per più di un oggetto alla volta

Gli esempi hanno finora utilizzato il comando EDTOBJAUT per impostare l'autorizzazione specifica per un singolo oggetto. Utilizzare il comando Concessione autorizzazione (GRTOBJAUT) per impostare la sicurezza per più oggetti. Immettere GRTOBJAUT e premere **F4** (Richiesta). Qui di seguito vengono riportati alcuni esempi di come apportate più modifiche all'autorizzazione.

- I campi immessi nel seguente pannello impostano l'autorizzazione pubblica per tutte le code messaggi della libreria CUSTLIB su *CHANGE.

```
                     Concessione autorizzazione oggetto (GRTOBJAUT)

Immettere le scelte e premere Invio.

Oggetto . . . . . .   *all
  Libreria  . . . . . .   custlib
Tipo oggetto  . . . . . .   *msgq
Utenti  . . . . . .   *public
              + per altri valori
Autorizzazione  . . . . . .   *change
```

- I campi immessi nel seguente pannello assegnano l'autorizzazione *ALL a tutti i file i cui nomi iniziano con i caratteri WRK nella libreria CUSTLIB per l'utente AMES.

```
                     Concessione autorizzazione oggetto

Immettere le scelte e premere Invio.

Oggetto . . . . . .   WRK*
  Libreria  . . . . . .     custlib
Tipo oggetto  . . . . . .   *file
Utenti  . . . . . .   AMES
              + per altri valori
Autorizzazione  . . . . . .   *all
```

Questo esempio utilizza una tecnica per specificare i parametri di chiamata a denominazione **generica**. Molti comandi consentono di specificare i primi caratteri seguiti da un asterisco (*) per un parametro. Il sistema esegue l'operazione per ogni oggetto il cui nome inizi con tali caratteri. Le informazioni in linea per un comando indicano i parametri che consentono nomi generici.

- Potrebbe essere necessario effettuare due operazioni per proteggere tutti i file che iniziano con i caratteri AR utilizzando una lista di autorizzazioni denominata ARLST1 e per fare in modo che i file derivino l'autorizzazione pubblica dalla lista. Questi pannelli mostrano le operazioni necessarie.

```
                    Concessione autorizzazione oggetto

Immettere le scelte e premere Invio.

Oggetto . . . . . .   AR*
  Libreria  . . . . . .    CUSTLIB
Tipo oggetto  . . . . . .   *FILE

   :
Lista autorizzazioni  . . . . . .   ARLST1
```

```
                     Concessione autorizzazione oggetto

Immettere le scelte e premere Invio.

Oggetto . . . . . .   AR*
  Libreria  . . . . . .    CUSTLIB
Tipo oggetto  . . . . . .   *FILE
Utenti  . . . . . .   *PUBLIC
              + per altri valori
Autorizzazione  . . . . . .   *AUTL
              + per altri valori
```

Utilizzare il comando DSPJOBLOG come descritto in ″Utilizzare la registrazione lavori per la verifica del lavoro″ per verificare che il sistema abbia effettuato le modifiche dell'autorizzazione richieste.

Prima di andare su ″Proteggere l'emissione di stampa,″ utilizzare il comando EDTOBJAUT o GRTOBJAUT per autorizzazioni le autorizzazioni specifiche nella Parte 2 del modulo Descrizione della libreria.

Proteggere l'emissione di stampa

Dopo aver impostato le autorizzazioni specifiche, è possibile proteggere l'emissione di stampa riservata utilizzando le informazioni contenute in questi argomenti:

- Creare la coda di emissione e controllare chi può gestirla.
- Assegnare l'emissione di stampa speciale alla coda.

Creare una coda di emissione

1. Immettere CRTOUTQ (Creazione coda emissione) e premere **F4** (Richiesta).
2. Riempire il nome della coda di emissione e della libreria.
3. Premere **F10** (Altri parametri).
4. Andare alla pagina successiva per trovare le informazioni relative alla sicurezza della coda di emissione.

```
                    Creazione coda emissione (CRTOUTQ)
Immettere le scelte e premere Invio.

Coda emissione . . . . . >   NEWCP
  Libreria  . . . . . .      CONTRACTS
Dimensione massima file spool:
  Numero di pagine   . . . . . .   *NONE         Numero, *NONE
  Ora di avviamento  . . . . . .                 Ora
  Ora di fine  . . . . . .                       Ora
              + per altri valori
Ordine di file in coda .  . . . .   *FIFO
Sistema remoto  . . . . . .   *NONE

   :
Testo 'descrizione' . . . . . .   Coda nuovi contratti
```

5. Inserire le informazioni contenute nel modulo Sicurezza della coda di emissione e della stazione di lavoro per controllare chi può utilizzare e gestire la coda di emissione.
6. Premere il tasto **Invio** e controllare i messaggi di conferma.

```
                    Creazione coda emissione (CRTOUTQ)
Immettere le scelte e premere Invio.


                           Parametri aggiuntivi

Visualizzare ogni file . . . . .   *NO
Separatori lavoro. . . . . .   0
Operatore controllato. . . . . .   *NO
Coda dati  . . . . . .   *NONE
  Libreria . . . . . .
Autoriz. da verificare . . . . .   *OWNER
Autorizzazione . . . . . .   *LIBCRTAUT
```

Possibile errore	Correzione
E' stato premuto il tasto **Invio** invece di **F10**.	Utilizzare il comando Modifica coda emissione (CHGOUTQ) per immettere ulteriori informazioni.
La coda di emissione è stata creata nella libreria errata.	Utilizzare il comando Trasferimento oggetto (MOVOBJ) per spostarlo nella libreria corretta.

E' ora possibile assegnare l'emissione di stampa a una coda di emissione.

Assegnare l'emissione di stampa ad una coda di emissione

Dopo aver creato una coda di emissione, è possibile assegnare un'emissione di stampa ad una coda di emissione. Generalmente un file di stampa controlla la destinazione dell'emissione di stampa. Consultare il fornitore dell'applicazione per conoscere i nomi e le librerie dei file di stampa per la documentazione riservata.

Se non si ha accesso a queste informazioni, stampare la documentazione e congelarla nella coda di emissione. Utilizzare l'opzione attributo contenuta nel pannello Gestione file di spool per conoscere il nome del file di stampa. Il file di stampa viene visualizzato nel campo *File di unità* nel pannello Gestione attributi dei file di spool.

Per modificare la destinazione (coda di emissione) di un file di stampa, utilizzare il comando Modifica file di stampa (CHGPRTF):

```
CHGPRTF FILE(nome-libreria/nome-file-stampante)
        OUTQ(nome-libreria/nome-coda-emissione)
```

La documentazione si trova nella nuova destinazione ogni volta che viene richiesta. Per modificare la destinazione per un file di spool già presente nella coda di emissione, utilizzare l'opzione di modifica contenuta nel pannello Gestione file di spool.

Ad esempio, Sharon Jones dell'Azienda di giocattoli JKL desidera assegnare il file di stampa PRCLST1 per il listino prezzi alla coda di emissione PRICEQ. Ella immette:

```
CHGPRTF FILE(CONTRACTS/PRCLST1) OUTQ(CONTRACTS/PRICEQ)
```

Per assegnare tutta la documentazione relativa al listino prezzi alla coda di emissione PRICEQ, Sharon potrebbe utilizzare un nome generico per il file di stampa:

```
CHGPRTF FILE(CONTRACTS/PRCLST*) OUTQ(CONTRACTS/PRICEQ)
```

Per indirizzare tutti i nuovi contratti alla coda di emissione NEWCP, Sharon potrebbe modificare la coda di emissione associata al documento di esempio utilizzato per creare i contratti.

Verificare il lavoro

Il miglior modo per verificare la strategia di protezione per l'emissione di stampa riservata è stamparla. Verificare che essa vada alla corretta coda di emissione. Collegarsi in qualità di operatore di sistema e verificare se sia possibile consultare o gestire i file presenti nella coda.

Prima di proteggere le stazioni di lavoro, verificare di:

- Creare tutte le code di emissione elencate nel modulo Sicurezza della coda di emissione e della stazione di lavoro utilizzando il comando CRTOUTQ.
- Assegnare l'emissione di stampa alle nuove code di emissione utilizzando il comando CHGPRTF.

Proteggere le stazioni di lavoro

Dopo aver protetto l'emissione di stampa, è necessario proteggere le stazioni di lavoro. Si assegna l'autorizzazione per le stazioni di lavoro nello stesso modo in cui si assegna l'autorizzazione per gli altri oggetti presenti nel sistema. Utilizzare il comando EDTOBJAUT per assegnare agli utenti l'autorizzazione per le stazioni di lavoro.

E' necessario che gli utenti dispongano dell'autorizzazione *CHANGE per collegarsi alla stazione di lavoro. Se il valore di sistema QLMTSECOFR è no (0), il responsabile della riservatezza o chiunque disponga dell'autorizzazione *ALLOBJ può collegarsi a qualsiasi stazione di lavoro.

Se il valore di sistema QLMTSECOFR è sì (1), utilizzare queste istruzioni per impostare l'autorizzazione alle stazioni di lavoro:

Utenti che possono collegarsi alla stazione di lavoro	Autorizzazione pubblica	Autorizzazione QSECOFR	Autorizzazione singolo utente
Tutti gli utenti	*CHANGE	*CHANGE	Non necessaria
Solo utenti selezionati	*EXCLUDE	Nessuna autorizzazione	*CHANGE
Utenti selezionati ed utenti con autorizzazione a tutti gli oggetti	*EXCLUDE	*CHANGE	*CHANGE
Tutti gli utenti eccetto quelli con autorizzazione a tutti gli oggetti	*CHANGE	Nessuna autorizzazione	Non necessaria

Prima di limitare l'accesso alla coda messaggi dell'operatore di sistema, utilizzare il comando EDTOBJAUT per proteggere le stazioni di lavoro, in base alle informazioni contenute nel modulo Sicurezza della coda di emissione e della stazione di lavoro.

Limitare l’accesso alla coda messaggi dell’operatore di sistema

E’ possibile migliorare la sicurezza proteggendo l’emissione di stampa, proteggendo le stazioni di lavoro e limitando l’accesso alla coda messaggi dell’operatore di sistema.

L’opzione per la gestione dei messaggi del menu ASSIST consente agli utenti di utilizzare un tasto funzionale per visualizzare la coda messaggi dell’operatore di sistema (QSYSOPR). Risposte non corrette ai messaggi dell’operatore di sistema possono causare problemi al sistema. Gli utenti necessitano dell’autorizzazione *CHANGE per rispondere e cancellare i messaggi di una coda messaggi. E’ necessario assegnare tale autorizzazione solo agli operatori di sistema. Consultare il modulo Responsabilità del sistema per visualizzare a chi è necessario assegnare l’autorizzazione *CHANGE alla coda messaggi dell’operatore di sistema.

Utilizzare il comando EDTOBJAUT:

1. Immettere `EDTOBJAUT QSYSOPR *MSGQ` e premere il tasto **Invio**.
2. Premere **F11** per visualizzare le informazioni dettagliate relative all’autorizzazione all’oggetto.
3. Assegnare l’autorizzazione *OBJOPR pubblica, come mostrato nel pannello di esempio e premere il tasto **Invio**.

```
                          Editazione autorizzazione oggetto

Oggetto . . . . . :   QSYSOPR         Proprietario  . . . . . :   QSYS
  Libreria  . . . . :     QSYS         Gruppo principale  . . . :   *NONE
Tipo oggetto  . . . . :   *MSGQ

Immettere le modifiche apportate alle autorizzazioni correnti, quindi premere Invio.

  Oggetto protetto dalla lista di autorizzazioni . . . . . .   *NONE

                        Autor.    ----------Oggetto----------
Utente      Gruppo      oggetto   Opr  Gest.Esist. Alter. Rif.
*PUBLIC                USER DEF    X
```

4. Il sistema modifica la colonna *Autorizzazione oggetto* in USER DEF (Definito dall’utente).
5. Premere nuovamente **F11** per visualizzare le informazioni dettagliate relative all’autorizzazione ai dati.
6. Assegnare l’autorizzazione *ADD pubblica, come mostrato nel pannello di esempio e premere il tasto **Invio**.

```
                          Editazione autorizzazione oggetto

Oggetto . . . . . :   QSYSOPR         Proprietario  . . . . . :   QSYS
  Libreria  . . . . :     QSYS         Gruppo principale  . . . :   *NONE
Tipo oggetto  . . . . :   *MSGQ

Immettere le modifiche apportate alle autorizzazioni correnti, quindi premere Invio.

  Oggetto protetto dalla lista di autorizzazioni . . . . . .   *NONE

                        Autorizz.  ---------------Dati---------------
Utente      Gruppo      oggetto   Lett. Agg. Aggior. Canc.   Esecuz.
*PUBLIC                USER DEF          X
```

7. Utilizzare **F6** (Aggiunta utenti) per aggiungere utenti che hanno necessità di rispondere ai messaggi QSYSOPR. Assegnare loro l’autorizzazione *CHANGE.

Attenzione: non assegnare all’autorizzazione pubblica il valore *EXCLUDE. E’ necessario che tutti i lavori (e gli utenti) siano in grado di aggiungere messaggi alla coda messaggi QSYSOPR.

Per verificare che sia stata completata l’impostazione della sicurezza delle risorse, è necessario:

- Utilizzare i moduli Lista di autorizzazioni ed i moduli Descrizione della libreria per verificare che sia stata stabilita la sicurezza per tutte le librerie dell’applicazione.

- Controllare il modulo Sicurezza della coda di emissione e della stazione di lavoro per verificare che si siano protette le stazioni di lavoro e si siano create delle code di emissione speciali.
- Limitare l'accesso alla coda messaggi dell'operatore di sistema (QSYSOPR).
- Salvare le librerie dell'applicazione secondo le istruzioni fornite con le applicazioni. Il sistema salva le informazioni relative alla proprietà e all'autorizzazione pubblica insieme all'applicazione.
- Utilizzare il comando Salvataggio dati sicurezza (SAVSECDTA) per salvare le informazioni create relative alla sicurezza. Consultare ″Salvare le informazioni relative alla sicurezza″ per ulteriori informazioni sulle modalità di salvataggio delle informazioni relative alla sicurezza.

E' ora possibile iniziare a verificare l'impostazione della sicurezza.

Capitolo 8. Verificare la sicurezza

Questo argomento descrive le tecniche di verifica della sicurezza impostate sul proprio sistema. In questo contesto verifica significa accertarsi che i lavori siano stati impostati nel modo desiderato. L'argomento ″Monitorare la sicurezza″ descrive come valutare l'efficacia della sicurezza sul proprio sistema.

Verificare la sicurezza ogni volta che si apportano modifiche significative al proprio sistema. Le modifiche possono essere diverse, ad esempio l'aggiunta di una nuova applicazione, impostazione della sicurezza delle risorse per un'applicazione esistente, aggiunta di un nuovo gruppo di utenti oppure modifica del livello di sicurezza.

Consultare questi argomenti per informazioni sui metodi di verifica e per la diagnosi dei problemi che possono verificarsi nel momento in cui si apportano delle modifiche:

- Verificare i profili utente.
- Verificare la sicurezza delle risorse.

Verificare i profili utente

Per iniziare la verifica della sicurezza, sarà necessario controllare un profilo utente ogni volta che un nuovo gruppo viene impostato sul proprio sistema. Provare uno dei singoli profili copiati dal profilo di gruppo.

- E' possibile effettuare il collegamento con esito positivo con il profilo utente? Se non è possibile, controllare la registrazione lavori relativa ai tentativi di collegamento non riusciti. Per ulteriori informazioni, utilizzare l'opzione Gestione emissione di stampa dal menu ASSIST per individuare la registrazione del lavoro.

  Possibili problemi:

  – Uno degli oggetti necessari, ad esempio il menu iniziale, la libreria corrente o il programma iniziale, non esiste.
  – La lista librerie specificata nella descrizione lavoro provoca errori. La libreria non esiste oppure l'utente ha dimenticato di inserire QGPL e QTEMP nella lista librerie.
  – L'utente non dispone dell'autorizzazione alla stazione di lavoro.
- Quando si effettua il collegamento, lo schermo visualizza il menu o il programma iniziale corretto?
- Se si immette un menu iniziale o una libreria corrente sul pannello di collegamento, cosa succede? Se il profilo utente è Possibilità limitate (SI'), viene ricevuto un messaggio di errore.
- Si apre il pannello corretto quando si preme il tasto Attn?
- L'emissione viene indirizzata alla stampante corretta? Se la risposta è negativa, utilizzare l'opzione Gestione emissione di stampa dal menu ASSIST per verificare il percorso dell'emissione. Controllare il profilo utente e una descrizione lavoro per stabilire il motivo per cui l'emissione è stata indirizzata ad una stampante differente.
- E' possibile richiamare una riga comandi?
- E' possibile eseguire le funzioni dell'applicazione richiesta senza errori di sicurezza? Per ulteriori dettagli, consultare ″Verificare la sicurezza delle risorse″.
- E' possibile eseguire le attività di sistema necessarie, ad esempio la gestione della stampante o il salvataggio delle librerie?

Se il sistema ha richiesto l'assegnazione di una nuova parola d'ordine nel momento in cui è stato effettuato il collegamento con un profilo, al termine della verifica impostare nuovamente la parola d'ordine sul nome profilo utente:

1. Effettuare il collegamento con il proprio profilo (con l'autorizzazione del responsabile della riservatezza).
2. Immettere `CHGUSRPRF` *`nome-profilo`* `PASSWORD(`*`nome-profilo`*`) PWDEXP(*YES).`

Una volta verificati i profili utente, è possibile verificare la sicurezza delle risorse.

Verificare la sicurezza delle risorse

Dopo la verifica dei profili utente, è necessario controllare anche la sicurezza delle risorse. Quando si controlla la sicurezza delle risorse, si effettua una ricerca degli:

- utenti che non dispongono di un'autorizzazione sufficiente per i rispettivi lavori;
- utenti che dispongono di un'autorizzazione maggiore rispetto al previsto.

Verificare l'autorizzazione insufficiente

Verificare le funzioni interattive e batch per vedere se i profili utente dispongono di autorizzazione sufficiente.

Verifica interattiva

Per verificare la sicurezza delle risorse per un'applicazione, è necessario collegarsi a diversi profili utente. L'obiettivo è quello di sottoporre a verifica un campione di utenti per accertarsi che l'autorizzazione assegnata sia sufficiente.

- Verificare le funzioni che richiedono diversi livelli di autorizzazione: visualizzazione, modifica e cancellazione.
- Verificare i programmi, non solo i menu. La selezione di un'opzione menu potrebbe non essere sufficiente per verificare l'autorizzazione. A volte il sistema non accede ad un file fino a quando non si tenta realmente di eseguire un'operazione, come ad esempio la cancellazione di un record. Il controllo dell'autorizzazione si verifica quando il sistema apre un file. E' il progetto dell'applicazione che determina quando il sistema apre il file.
- Conservare un record degli errori di sicurezza e risolverli. Se si verifica un errore di autorizzazione, sul proprio schermo viene visualizzato un messaggio che indica che non si dispone dell'autorizzazione sufficiente per l'operazione e per l'oggetto si stava tentando di utilizzare.

Verifica batch

- Eseguire i lavori batch di esempio dall'applicazione utilizzando i profili degli utenti che inoltreranno i lavori.
- Verificare i lavori batch che richiedono diversi livelli di autorizzazione, come: stampa delle informazioni, modifica delle informazioni o eliminazione dei file alla fine del mese.
- Controllare la coda messaggi QSYSOPR e la registrazione QHST per gli errori di sicurezza. Utilizzare il comando DSPLOG per visualizzare la registrazione QHST. I messaggi di sicurezza sono compresi entro questi intervalli: CPF2200, CPI2200, CPC2200, CPD2200, CPF4A00, CPI4A00, CPC4A00 e CPD4A00.

  E' possibile inoltre utilizzare la funzione di controllo della sicurezza per registrare gli errori di autorizzazione e altri eventi relativi alla sicurezza.

Verificare una eccessiva autorizzazione

Se si imposta la sicurezza delle risorse per proteggere le informazioni riservate, verificare i profili utente di esempio per accertarsi che tale sicurezza funzioni. Effettuare il collegamento utilizzando il profilo di un utente che non può accedere al file riservato.

- Viene visualizzato un menu che consente l'accesso al file?
- Cosa succede se si seleziona un'opzione di menu che utilizza il file?
- E' possibile richiamare una riga comandi?
- E' possibile eseguire un comando per inserire il file nella lista, ad esempio `CPYF FROMFILE(`*`nome-file`*`) TOFILE(QSYSPRT)`?
- E' possibile utilizzare uno strumento di interrogazione per esaminare il file?

I risultati della verifica potrebbero indicare la necessità di modificare le informazioni sulla sicurezza.

Capitolo 9. Modificare le informazioni sulla sicurezza

Una volta pianificata la sicurezza per il proprio sistema, è necessario verificare che la pianificazione rimanga tale anche quando cambiano le necessità dell'azienda.

Questo argomento pone l'accento sulla semplicità come obiettivo essenziale nella progettazione della sicurezza. I gruppi di utenti sono stati progettati come modelli per i singoli utenti. Si è tentato di utilizzare l'autorizzazione pubblica, le liste di autorizzazioni e l'autorizzazione alla libreria piuttosto che autorizzazioni singole specifiche. Avvalersi di tale approccio quando si gestisce la sicurezza:

- Quando si aggiunge un nuovo gruppo di utenti o una nuova applicazione, utilizzare le tecniche utilizzate per pianificare la sicurezza.
- Se si devono apportare delle modifiche alla sicurezza, tentare un approccio generico piuttosto che creare un'eccezione per risolvere un problema specifico.

L'argomento Comandi di sicurezza descrive i comandi da utilizzare per visualizzare, modificare e cancellare le informazioni sulla sicurezza.

Consultare i seguenti argomenti per suggerimenti relativi a diversi tipi di modifiche:

- aggiungere un nuovo utente al sistema;
- creare un nuovo gruppo di utenti;
- modificare un gruppo di utenti;
- aggiungere una nuova applicazione;
- aggiungere una nuova stazione di lavoro;
- modificare la responsabilità di un utente;
- eliminare un utente dal sistema.

Comandi di sicurezza

La seguente tabella mostra i comandi utilizzati per gestire gli oggetti di sicurezza sul sistema. E' possibile utilizzare tali comandi per eseguire queste attività:

- Visualizzare ed elencare le informazioni sulla sicurezza.
- Modificare le informazioni sulla sicurezza.
- Cancellare le informazioni sulla sicurezza.

Tabella 63. Comandi di sicurezza

Oggetto di sicurezza	Come visualizzare	Come modificare	Come cancellare
Valore di sistema	WRKSYSVAL DSPSYSVAL	WRKSYSVAL CHGSYSVAL	Impossibile effettuare la cancellazione
Descrizione lavoro	WRKJOBD DSPJOBD	WRKJOBD CHGJOBD	DLTJOBD
Profilo di gruppo	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF	DLTUSRPRF[1],[2]
Profilo utente	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF CHGUSRAUD	DLTUSRPRF[1]
Autorizzazioni oggetto	DSPAUT DSPOBJAUT DSPUSRPRF TYPE(*OBJAUT)	CHGAUT EDTOBJAUT GRTOBJAUT WRKAUT	EDTOBJAUT RVKOBJAUT WRKAUT

Tabella 63. Comandi di sicurezza (Continua)

Oggetto di sicurezza	Come visualizzare	Come modificare	Come cancellare
Proprietà oggetto	WRKOBJOWN DSPOBJAUT DSPUSRPRF TYPE(*OBJOWN)	CHGOBJOWN CHGOWN	CHGOBJOWN CHGOWN consente di revocare i diritti del proprietario precedente.
Gruppo primario	DSPOBJAUT WRKOBJPGP DSPUSRPRF TYPE(*OBJPGP)	CHGOBJPGP CHGPGP	CHGOBJPGP CHGPGP imposta il gruppo primario su *NONE
Controllo oggetto	DSPOBJD	CHGOBJAUD CHGAUD	CHGOBJAUD (impostato su *NONE) CHGAUD
Lista di autorizzazioni	DSPAUTL DSPAUTLOBJ	EDTAUTL (autorizzazione utente per una lista) EDTOBJAUT (oggetto protetto dalla lista) ADDAUTLE CHGAUTLE GRTOBJAUT	DLTAUTL (lista intera)[3] RMVAUTLE (eliminare l'autorizzazione utente nella lista) EDTOBJAUT (oggetto protetto dalla lista) RVKOBJAUT

1. Per la cancellazione di un profilo IBM consiglia di utilizzare l'opzione di eliminazione dal pannello Gestione registrazione utente. Utilizzando questa opzione, è possibile cancellare tutti gli oggetti dal profilo o assegnarli nuovamente ad un nuovo proprietario. Alcuni parametri comando DLTUSRPRF consentono di cancellare tutti gli oggetti di proprietà dell'utente o di assegnarli ad un nuovo proprietario. Non è possibile cancellare un profilo a meno che non si cancellino o assegnino nuovamente gli oggetti di proprietà. Non è possibile, inoltre, cancellare un profilo che funge da gruppo primario per qualsiasi oggetto.
2. Non è possibile cancellare un profilo di gruppo che contenga membri. Utilizzare l'opzione *GRPMBR del comando DSPUSRPRF per elencare i membri del gruppo. Modificare il campo *profilo di gruppo* in ogni singolo profilo di gruppo prima di cancellare il profilo di gruppo.
3. Non è possibile cancellare una lista di autorizzazioni utilizzata per proteggere gli oggetti. Utilizzare il comando DSPAUTLOBJ per elencare gli oggetti protetti dalla lista. Modificare l'autorizzazione di tutti gli oggetti protetti dalla lista utilizzando il comando EDTOBJAUT.

Visualizzare ed elencare le informazioni sulla sicurezza

E' possibile elencare le informazioni sulla sicurezza utilizzando un comando DSP (Visualizzazione) con un'opzione di stampa *PRINT. Ad esempio, per visualizzare una lista di autorizzazioni definita MYLIST, immettere `DSPAUTL MYLIST *PRINT`.

Alcuni comandi di visualizzazione forniscono opzioni per diversi tipi di liste. Ad esempio, quando si creano singoli profili utente, viene utilizzata l'opzione *GRPMBR del comando DSPUSRPRF per elencare tutti i membri di un profilo di gruppo. Utilizzare la richiesta (**F4**) e le informazioni in linea per individuare le liste disponibili per gli oggetti sicurezza.

E' possibile utilizzare i comandi di visualizzazione per visualizzare le informazioni sulla sicurezza sulla propria stazione video. Inoltre, è possibile utilizzare i comandi WRK (Gestione...), che forniscono ulteriori funzioni. I comandi Gestione... forniscono una visualizzazione della lista. E' possibile utilizzare questo pannello per modificare, cancellare e visualizzare le informazioni.

Inoltre, è possibile utilizzare i comandi sulla sicurezza per elencare o visualizzare le informazioni utilizzando un nome generico. Se si immette `WRKUSRPRF DPT*`, il pannello Gestione registrazione utente o Gestione profili utente mostra solo i profili che iniziano con i caratteri *DPT*. Utilizzare le informazioni in linea relative ad un comando per individuare i parametri che consentono l'utilizzo di nomi generici.

Modificare le informazioni sulla sicurezza

E' possibile modificare le informazioni sulla sicurezza in modo interattivo utilizzando il comando WRK (Gestione...) o EDT (Modifica...). Si possono visualizzare le informazioni, modificarle e visualizzarle nuovamente dopo la modifica.

E' possibile inoltre modificare le informazioni sulla sicurezza senza visualizzarle prima e dopo la modifica utilizzando un comando CHG (Modifica...) o GRT (Concessione...). Questo metodo è particolarmente utile per apportare una modifica a più oggetti contemporaneamente. Ad esempio, viene utilizzato il comando GRTOBJAUT per impostare l'autorizzazione pubblica per tutti gli oggetti in una libreria (consultare "Impostare l'autorizzazione pubblica per tutti gli oggetti di una libreria" a pagina 111).

Cancellare le informazioni sulla sicurezza

E' possibile cancellare o eliminare determinati tipi di informazioni sulla sicurezza in modo interattivo utilizzando il comando WRK (Gestione...) o EDT (Modifica...). E' possibile inoltre utilizzare i comandi DLT (Cancellazione...), RMV (Eliminazione...) e RVK (Revoca...) per cancellare le informazioni sulla sicurezza. Spesso, è necessario soddisfare determinate condizioni prima che il sistema consenta di cancellare le informazioni sulla sicurezza. Le note che si trovano in Comandi sulla sicurezza descrivono alcune di quelle condizioni.

Aggiungere un nuovo utente al sistema

Quando si deve aggiungere un nuovo utente al sistema, utilizzare la seguente procedura:

1. Assegnare la persona ad un gruppo di utenti. Per riferimenti, utilizzare il modulo Descrizione del gruppo di utenti.
2. Stabilire se il nuovo utente necessita di eseguire le funzioni di sistema. In questo caso, aggiungere le informazioni al modulo Responsabilità del sistema.
3. Aggiungere l'utente al modulo Singolo profilo utente.
4. Rivedere il modulo Responsabilità del sistema e il modulo Descrizione del gruppo di utenti per stabilire se il nuovo utente necessita di valori diversi da quelli del gruppo.
5. Creare un profilo utente copiando il profilo di gruppo o il profilo di un membro del gruppo. Verificare di aver impostato la scadenza della parola d'ordine. (Consultare ″Copiare il profilo di gruppo.″)
6. Fornire al nuovo utente una copia della memo di sicurezza.

Per informazioni su come creare un nuovo gruppo di utenti, consultare ″Creare un nuovo gruppo di utenti.″

Creare un nuovo gruppo di utenti

Potrebbe essere necessario creare nuovi gruppi di utenti per diversi motivi:

- E' possibile che diversi reparti richiedano l'utilizzo del sistema.
- Risulta necessario rendere più specifici i gruppi di utenti in modo che soddisfino le esigenze di sicurezza delle risorse.
- L'azienda ha riorganizzato alcuni reparti.

Per creare un nuovo gruppo di utenti, effettuare quanto segue:

1. Compilare un Modulo Descrizione del gruppo di utenti seguendo le istruzioni contenute in ″Pianificare i gruppi di utenti.″
2. Aggiungere il gruppo di utenti al proprio diagramma di applicazioni, librerie e gruppi di utenti.
3. Valutare se ogni membro del gruppo deve eseguire le funzioni di sistema. Aggiornare il modulo Responsabilità del sistema. (Consultare ″Determinare i responsabili delle funzioni di sistema.″)
4. Utilizzare le informazioni dal modulo Descrizione del gruppo di utenti e dal modulo Responsabilità del sistema per completare un modulo Singolo profilo utente.

5. Creare una libreria di gruppo.
6. Creare una descrizione lavoro per il gruppo.
7. Creare un profilo di gruppo.

   Nota: consultare ″Impostare i gruppi di utenti″ per istruzioni sull'esecuzione delle fasi cinque, sei e sette.
8. Creare i singoli profili utente per i membri del gruppo. (Consultare ″Impostare i singoli utenti.″)
9. Valutare i moduli Descrizione della libreria per tutte le applicazioni necessarie per il gruppo. Eseguire tutte le istruzioni necessarie per consentire al gruppo l'accesso agli oggetti dell'applicazione utilizzando le tecniche descritte in ″Impostare la sicurezza delle risorse.″
10. Fornire a tutti i membri del gruppo una copia della memo sulla sicurezza.

Per informazioni su come modificare un gruppo di utenti, consultare ″Modificare un gruppo di utenti.″

Modificare un gruppo di utenti

Sarà necessario gestire diversi tipi di modifiche apportate alle caratteristiche di un gruppo in modi differenti. Seguono alcuni esempi di modifiche e informazioni su come gestirle:

Modificare l'autorizzazione del gruppo

Per il gruppo potrebbe rivelarsi necessaria un'autorizzazione ad oggetti non contemplata nella pianificazione iniziale. Effettuare quanto segue:

1. Utilizzare il comando Editazione autorizzazione oggetto (EDTOBJAUT) per fornire al gruppo l'accesso corretto agli oggetti o ad una lista di autorizzazioni appropriate. “Impostare le autorizzazioni specifiche” a pagina 116 visualizza un esempio di come sia possibile fare ciò. Ogni membro del gruppo riceve l'autorizzazione all'oggetto quando viene fornita l'autorizzazione di gruppo.
2. Se si fornisce l'autorizzazione di gruppo ad una risorsa riservata, potrebbe essere opportuno controllare i membri correnti del gruppo. Utilizzare il comando Visualizzazione profilo utente (DSPUSRPRF *nome-profilo-gruppo* *GRPMBR) per elencare i membri del gruppo.

Modificare la personalizzazione del gruppo

Potrebbe essere necessario modificare l'impostazione dell'ambiente dell'utente per i membri di un gruppo. Ad esempio, se un reparto riceve una nuova stampante, si desidera che la nuova stampante sia quella predefinita per i membri del gruppo di utenti del reparto. Oppure, quando sul sistema viene installata una nuova applicazione, i membri di un gruppo di utenti potrebbero desiderare un menu iniziale differente al momento del collegamento.

Il profilo di gruppo fornisce un modello che può essere copiato per creare singoli profili per i membri del gruppo. Tuttavia, i valori di personalizzazione nel profilo di gruppo non influenzano i singoli profili utente dopo la loro creazione. Ad esempio, la modifica di un campo, come l'*Unità di stampa* nel profilo di gruppo, non ha effetti sui membri del gruppo. E' necessario modificare il campo *Unità di stampa* in ogni singolo profilo utente.

E' possibile utilizzare il pannello Gestione profili utente per modificare un parametro per più utenti contemporaneamente. L'esempio mostra la modifica della coda di emissione per tutti i membri di un gruppo:

1. Immettere WRKUSRPRF *ALL e premere il tasto **Invio**.
2. Se viene visualizzato il pannello Gestione registrazione utente, utilizzare **F21** (Selezione livello assistenza) per passare al pannello Gestione profili utente.

```
                        Gestione profili utente

Immettere le opzioni e premere Invio.
  1=Creaz. 2=Modifica   3=Copia   4=Eliminaz. 5=Visualizzaz.
  12=Gestione oggetti per proprietario

          Profilo
Opz       utente        Testo

                HARRISOK         Harrison, Keith
2               HOGANR           Hogan, Richard
                JONESS           Jones, Sharon
2               WILLISR          Willis, Rose

   ⋮
                                                              Segue..
Parametri per le opzioni 1, 2, 3, 4 e 5 o comando
===> PRTDEV(PRT02)
F3=Fine   F5=Rivisual. F12=Annull.  F16=Rip. inizio elen. da F17=Inizio elenco da
F21=Selezione livello assistenza    F24=Altri tasti
```

3. Immettere **2** (Modifica) accanto ad ogni profilo che si desidera modificare.
4. Sulla riga parametro nella parte inferiore del pannello, immettere il nome del parametro e il nuovo valore. Se non si conosce il nome del parametro, premere **F4** (Richiesta).
5. Premere il tasto **Invio**. Si riceve un messaggio di conferma per ogni profilo modificato.

   Sebbene la modifica di un campo di personalizzazione nel profilo di gruppo non influenzi i membri del gruppo, potrebbe comunque essere di aiuto in futuro. Se si desidera aggiungere membri al gruppo successivamente, il profilo di gruppo fornisce un modello. E' anche un record dei valori standard del campo per il gruppo.

Fornire l'accesso di gruppo ad una nuova applicazione

Quando un gruppo di utenti richiede di accedere ad una nuova applicazione, è necessario analizzare le informazioni sul gruppo e sull'applicazione. Quello che segue è il metodo consigliato:

1. Consultare il modulo Descrizione dell'applicazione relativo alla nuova applicazione e il proprio diagramma di applicazioni, librerie e gruppi di utenti per individuare le librerie utilizzate dall'applicazione. Aggiungere quelle librerie al modulo Descrizione del gruppo di utenti.
2. Aggiornare il diagramma di applicazioni, librerie e gruppi di utenti in modo che visualizzi la nuova relazione tra il gruppo di utenti e l'applicazione.
3. Se la lista librerie iniziale del gruppo deve includere le librerie, modificare la descrizione lavoro del gruppo utilizzando il comando Modifica descrizione lavoro (CHGJOBD). Consultare "Creare una descrizione lavoro" a pagina 97 se si necessita di un aiuto per la gestione delle descrizioni lavoro.

   Nota: quando si aggiungono delle librerie alla lista librerie iniziale in una descrizione lavoro, non è necessario modificare i profili utente che utilizzano la descrizione lavoro. Quando l'utente effettua un nuovo collegamento, la lista librerie iniziale aggiunge automaticamente quelle librerie.
4. Valutare se è necessario modificare il programma iniziale o il menu iniziale del gruppo per fornire l'accesso alla nuova applicazione. E' necessario apportare una singola modifica al menu o al programma iniziale di ogni profilo utente utilizzando il comando CHGUSRPRF.
5. Esaminare nuovamente i moduli Descrizione della libreria relativi a tutte le librerie utilizzate dall'applicazione. Determinare se l'accesso pubblico disponibile per le librerie sia sufficiente per le necessità del gruppo. In caso contrario, potrebbe essere necessario fornire l'autorizzazione di gruppo alla libreria, agli oggetti specifici o alle liste di autorizzazioni. Utilizzare i comandi Editazione autorizzazione oggetto (EDTOBJAUT) e Editazione lista di autorizzazione (EDTAUTL) per effettuare questa operazione. (Consultare ″Impostare la sicurezza delle risorse″ se si necessita di ulteriori informazioni.)

Per aggiungere le applicazioni al sistema, consultare ″Aggiungere una nuova applicazione.″

Aggiungere una nuova applicazione

E’ necessario pianificare la sicurezza per ogni nuova applicazione con la stessa accuratezza con cui sono state pianificate le applicazioni di origine. Seguire le stesse procedure:

1. Preparare un modulo Descrizione dell’applicazione e i moduli Descrizione delle libreria relativi all’applicazione.
2. Aggiornare il proprio diagramma di applicazioni, librerie e gruppi di utenti.
3. Seguire le procedure in ″Pianificare la sicurezza delle risorse″ per decidere come proteggere la nuova applicazione.
4. Preparare un modulo Installazione dell’applicazione utilizzando il metodo descritto in ″Pianificare l’installazione dell’applicazione .″
5. Valutare se qualche emissione di stampa dall’applicazione è riservata e necessita di protezione. Se necessario, aggiornare il modulo Sicurezza della coda di emissione e della stazione di lavoro.
6. Seguire le istruzioni descritte in ″Impostare l’autorizzazione pubblica e la proprietà″ e ″Impostare la sicurezza delle risorse″ per installare e proteggere l’applicazione.

Per aggiungere una stazione di lavoro al proprio sistema, consultare ″Aggiungere una nuova stazione di lavoro.″

Aggiungere una nuova stazione di lavoro

Quando si aggiunge una nuova stazione di lavoro al proprio sistema, considerare i requisiti della sicurezza:

1. L’ubicazione fisica di una nuova stazione di lavoro pone dei rischi per la sicurezza? (Consultare ″Pianificare la sicurezza fisica″ per riferimenti all’argomento.)
2. Se la stazione di lavoro comporta rischi, aggiornare il modulo Sicurezza della coda di emissione e della stazione di lavoro.
3. Si dovrebbero creare normalmente nuove stazioni di lavoro con l’autorizzazione pubblica *CHANGE. Se in questo modo non vengono soddisfatti i requisiti della sicurezza per la stazione di lavoro, utilizzare il comando EDTOBJAUT per specificare un’autorizzazione differente.

Per modificare la responsabilità di un utente sul sistema, consultare ″Modificare le responsabilità di un utente.″

Modificare le responsabilità di un utente

Quando un utente di sistema riceve un nuovo incarico o una nuova serie di responsabilità all’interno dell’azienda, è necessario considerare il modo in cui ciò influenza il profilo utente.

1. L’utente dovrebbe appartenere ad un gruppo di utenti differente? E’ possibile utilizzare il comando CHGUSRPRF per modificare il gruppo di utenti.
2. E’ necessario modificare qualche valore di personalizzazione nel profilo, come ad esempio la stampante o il menu iniziale? E’ possibile utilizzare il comando CHGUSRPRF per modificare anche questi valori.
3. Le autorizzazioni all’applicazione del nuovo gruppo di utenti sono sufficienti per questa persona?
   - Utilizzare il comando Visualizzazione profilo utente (DSPUSRPRF) per visualizzare le autorizzazioni per i profili di gruppo nuovi e vecchi.
   - Visualizzare anche le autorizzazioni del singolo profilo utente.
   - Apportare le modifiche necessarie utilizzando il comando EDTOBJAUT.
4. L’utente possiede qualche oggetto? E’ necessario modificare la proprietà di quegli oggetti? Utilizzare il comando Gestione oggetti per proprietario (WRKOBJOWN).

5. L'utente esegue funzioni di sistema? L'utente deve eseguire funzioni di sistema per il nuovo incarico? Se necessario, aggiornare il modulo Responsabilità del sistema e modificare il profilo utente.

Per informazioni su come eliminare un utente dal sistema, consultare ″Eliminare un utente dal sistema.″

Eliminare un utente dal sistema

Se qualcuno lascia la società, è necessario eliminare immediatamente il profilo utente dal sistema. Prima di poter cancellare un profilo utente, è necessario cancellare o trasferire la proprietà di qualsiasi oggetto posseduto dal profilo. Per fare ciò è possibile utilizzare il comando WRKOBJOWN oppure è possibile utilizzare l'opzione **4** (Eliminazione) dal pannello Gestione registrazione utente.

Quando si seleziona l'opzione **4** (Eliminazione) per un profilo dal pannello Gestione registrazione utente, vengono visualizzati pannelli aggiuntivi che consentono di gestire tutti gli oggetti di proprietà dell'utente. E' possibile scegliere di assegnare tutti gli oggetti ad un nuovo proprietario o gestire gli oggetti singolarmente:

```
                              Eliminazione utente

Utente . . . . . . . . . . . :   HOGANR
Descrizione utente . . . . . :   Reparto vendite e marketing

Per eliminare questo utente immettere una delle seguenti opzioni, quindi premere Invio.

    1. Fornire tutti gli oggetti di proprietà di questo utente ad un nuovo proprietario
    2. Cancellare o modificare il proprietario di oggetti specifici di proprietà di questo utente.
```

Se si sceglie di gestire gli oggetti singolarmente (opzione **2**), lo schermo visualizza una lista di tutti gli oggetti di proprietà dell'utente:

```
                              Eliminazione utente

Utente . . . . . . . . . . . :   HOGANR
Descrizione utente . . . . . :   Reparto vendite e marketing

Nuovo proprietario  . . . . . . . . .     Nome, F4 per el.

Per eliminare questo utente, cancellare o modificare 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 Hogan, Richard
 4   QUERY1        DPTWH         Interrogazione inventario
```

Se si sceglie di cancellare gli oggetti, viene visualizzato il pannello Conferma cancellazione. Una volta che il sistema ha cancellato gli oggetti, è possibile eliminare il profilo utente. Viene visualizzato nuovamente il pannello Gestione registrazione utente con un messaggio che indica che il sistema ha eliminato l'utente.

Capitolo 10. Salvare le informazioni sulla sicurezza

Questo argomento presenta una panoramica delle modalità di salvataggio e di ripristino delle informazioni sulla sicurezza. Quando si pianifica l'esecuzione della copia di riserva e del ripristino del proprio sistema, è necessario tenere presente la sicurezza delle informazioni oltre alle informazioni stesse. Consultare l'argomento dell'Information Center, Copia di riserva, ripristino e disponibilità per assistenza nella predisposizione di un piano completo per la copia di riserva e il ripristino.

I seguenti argomenti descrivono come effettuare la copia di riserva e il ripristino delle informazioni sulla sicurezza create al momento dell'impostazione della sicurezza:

- Salvare i valori di sistema.
- Salvare i profili utente e di gruppo.
- Salvare le descrizioni lavoro.
- Salvare le informazioni sulla sicurezza delle risorse.
- Utilizzare il profilo proprietario predefinito (QDFTOWN).
- Ripristinare da una lista di autorizzazioni danneggiata.

Salvare i valori di sistema

I valori di sistema vengono memorizzati nella libreria di sistema, QSYS. La libreria QSYS viene salvata quando si effettuano le seguenti operazioni:

- Utilizzare il comando Salvataggio sistema (SAVSYS).
- Utilizzare l'opzione per salvare l'intero sistema dal menu Salvataggio.
- Utilizzare l'opzione per salvare le informazioni sul sistema dal menu Salvataggio.
- Utilizzare l'opzione per effettuare la copia di riserva dell'intero sistema dal menu Esecuzione copia di riserva (RUNBCKUP).

Se è necessario ripristinare l'intero sistema, nel momento in cui si ripristina il proprio sistema operativo vengono ripristinati automaticamente anche i valori di sistema.

Consultare il paragrafo successivo ″Salvare i profili utente e gruppo″.

Salvare i profili utente e gruppo

I profili utente e gruppo vengono memorizzati nella libreria QSYS. Vengono salvati quando si utilizza il comando Salvataggio sistema (SAVSYS) o se si seleziona l'opzione di menu per salvare l'intero sistema.

E' possibile inoltre salvare i profili utente e di gruppo utilizzando il comando Salvataggio dati di riservatezza (SAVSECDTA).

Ripristinare i profili utente utilizzando il comando Ripristino profilo utente (RSTUSRPRF). La sequenza normale è:

1. Ripristinare il sistema operativo, che ripristina la libreria QSYS.
2. Ripristinare i profili utente.
3. Ripristinare le librerie restanti.
4. Ripristinare l'autorizzazione agli oggetti utilizzando il comando Ripristino autorizzazione (RSTAUT).

Consultare il paragrafo successivo ″Salvare le descrizioni lavoro″.

Salvare le descrizioni lavoro

Quando si crea una descrizione lavoro, viene specificata una libreria nella quale dovrebbe risiedere tale descrizione. IBM consiglia la creazione di descrizioni lavoro nella libreria QGPL.

E' possibile salvare le descrizioni lavoro salvando la libreria che le contiene. Per fare ciò, utilizzare il comando Salvataggio libreria (SAVLIB). E' possibile salvare anche una descrizione lavoro utilizzando il comando Salvataggio oggetto (SAVOBJ).

E' possibile ripristinare il contenuto di una libreria utilizzando il comando Ripristino libreria (RSTLIB). E' possibile ripristinare una singola descrizione lavoro utilizzando il comando Ripristino oggetto (RSTOBJ).

Consultare il paragrafo successivo ″Salvare le informazioni sulla sicurezza delle risorse″.

Salvare le informazioni sulla sicurezza delle risorse

La sicurezza delle risorse, che definisce il modo in cui gli utenti possono gestire gli oggetti, consiste in diversi tipi di informazioni memorizzate in diverse ubicazioni:

Tabella 64. Salvare e ripristinare le informazioni sulla sicurezza delle risorse

Tipo di informazioni	Dove vengono memorizzate	Come vengono salvate	Come vengono ripristinate
Autorizzazione pubblica	Con l'oggetto	Comando SAVxxx [1]	Comando RSTxxx [2]
Valore di controllo oggetto	Con l'oggetto	Comando SAVxxx [1]	Comando RSTxxx [2]
Proprietà oggetto	Con l'oggetto	Comando SAVxxx [1]	Comando RSTxxx [2]
Gruppo primario	Con l'oggetto	Comando SAVxxx [1]	Comando RSTxxx [2]
Lista di autorizzazioni	Libreria QSYS	SAVSYS o SAVSECDTA	RSTUSRPRF USRPRF(*ALL)
Collegamento tra l'oggetto e la lista di autorizzazioni	Con l'oggetto	Comando SAVxxx [1]	Comando RSTxxx [2]
Autorizzazione privata	Con il profilo utente	SAVSYS o SAVSECDTA	RSTAUT

1. E' possibile salvare più tipi di oggetti utilizzando i comandi SAVOBJ o SAVLIB. Alcuni tipi di oggetti, come le configurazioni, hanno un comando di salvataggio speciale.
2. E' possibile ripristinare più tipi di oggetti utilizzando i comandi RSTOBJ o RSTLIB. Alcuni tipi di oggetti, ad esempio le configurazioni, hanno un comando di ripristino speciale.

Se si deve recuperare un'applicazione o l'intero sistema, è necessario pianificarne attentamente le fasi, incluso il ripristino dell'autorizzazione agli oggetti. Di seguito vengono riportate le fasi di base necessarie per ripristinare le informazioni sulla sicurezza delle risorse per un'applicazione:

1. Se necessario, ripristinare i profili utente, inclusi quelli che sono proprietari dell'applicazione. E' possibile ripristinare profili specifici o tutti i profili con il comando RSTUSRPRF.
2. Ripristinare tutte le liste di autorizzazioni utilizzate dall'applicazione. Vengono ripristinate le liste di autorizzazioni quando si utilizza RSTUSRPRF USRPRF(*ALL).

   Nota: questa operazione consente di ripristinare tutti i valori del profilo utente, incluse le parole d'ordine, dal supporto magnetico di riserva.
3. Ripristinare le librerie dell'applicazione utilizzando il comando RSTLIB o RSTOBJ. Questa operazione ripristina la proprietà dell'oggetto, l'autorizzazione pubblica e i collegamenti tra gli oggetti e le liste di autorizzazioni.
4. Ripristinare l'autorizzazione privata agli oggetti utilizzando il comando RSTAUT. Il comando RSTAUT ripristina anche le autorizzazioni utente in liste di autorizzazioni. E' possibile ripristinare l'autorizzazione per utenti specifici o per tutti gli utenti.

Consultare ″Utilizzare il profilo proprietario predefinito (QDFTOWN)″ per informazioni sul ripristino di un oggetto e di un profilo proprietario che non si trova nel proprio sistema.

Utilizzare il profilo proprietario predefinito (QDFTOWN)

Se si ripristina un oggetto e il profilo proprietario non si trova nel sistema, il sistema trasferisce la proprietà dell'oggetto ad un profilo predefinito denominato QDFTOWN. Una volta ripristinato o creato nuovamente il profilo proprietario, è possibile trasferire ancora la proprietà utilizzando il comando Gestione oggetto dal proprietario (WRKOBJOWN).

Per informazioni sul ripristino della lista di autorizzazioni, consultare ″Ripristinare da una lista di autorizzazioni danneggiata.″

Ripristinare da una lista di autorizzazioni danneggiata

Quando una lista di autorizzazioni protegge un oggetto e la lista di autorizzazioni risulta danneggiata, solo gli utenti con l'autorizzazione speciale a tutti gli oggetti (*ALLOBJ) hanno l'accesso all'oggetto.

Il ripristino da una lista di autorizzazioni danneggiata si effettua seguendo due fasi:

1. ripristinare gli utenti e le relative autorizzazioni sulla lista di autorizzazioni;
2. ripristinare l'associazione della lista di autorizzazioni agli oggetti.

Un utente che dispone dell'autorizzazione speciale *ALLOBJ può seguire queste fasi.

Fase 1: ripristinare la lista di autorizzazioni

Se si conosce l'autorizzazione utente alla lista di autorizzazioni, cancellare quella lista, crearla nuovamente e aggiungervi gli utenti.

Se non si conoscono tutte le autorizzazioni utente alla lista di autorizzazioni, ripristinarla dagli ultimi nastri SAVSYS o SAVSECDTA utilizzando le seguenti istruzioni:

1. Cancellare la lista di autorizzazioni danneggiata:
   ```
   DLTAUTL AUTL(nome-lista-autorizzazioni)
   ```
2. Ripristinare la lista di autorizzazioni:
   ```
   RSTUSRPRF USRPRF(*ALL)
   ```
3. Aggiungere gli utenti alla lista utilizzando il comando Ripristino autorizzazione (RSTAUT).

Fase 2: ripristinare l'associazione di oggetti alla lista di autorizzazioni

Una volta ripristinata o creata nuovamente la lista di autorizzazioni, è necessario stabilire il collegamento tra la lista e gli oggetti protetti dalla lista:

1. Utilizzare il comando Riacquisizione memoria (RCLSTG). RCLSTG assegna gli oggetti che sono protetti da liste di autorizzazioni danneggiate o mancanti ad una lista predefinita denominata QRCLAUTL.
2. Elencare gli oggetti protetti dalla lista di autorizzazioni QRCLAUTL:
   ```
   DSPAUTLOBJ AUTL(QRCLAUTL)
   ```
3. Utilizzare il comando GRTOBJAUT per proteggere gli oggetti tramite la lista di autorizzazioni corretta. Ad esempio, per proteggere il file ARWRK01 nella libreria CUSTLIB tramite la lista di autorizzazioni ARLST01, immettere
   ```
   GRTOBJAUT OBJ(CUSTLIB/ARWRK01) OBJTYPE(*FILE) +
             AUTL(ARLST01)
   ```

Capitolo 11. Monitorare la sicurezza

Questo argomento fornisce i suggerimenti di base per controllare l'efficacia della protezione nel proprio sistema.

Il monitoraggio regolare della sicurezza ha due scopi principali:

- verificare che le risorse della propria azienda vengano protette in maniera adeguata;
- rilevare i tentativi non autorizzati di accesso al sistema e alle informazioni dell'azienda.

Riesaminare la relazione sulla normativa di sicurezza e la memo sulla sicurezza per gli utenti nel momento in cui vengono stabilite le attività di monitoraggio che è necessario eseguire regolarmente.

Consultare i seguenti argomenti per ulteriori informazioni sul monitoraggio della sicurezza:

- Liste di controllo per il monitoraggio della sicurezza.
- Controllo della sicurezza.

Liste di controllo per il monitoraggio della sicurezza

Di seguito vengono riportate liste di controllo per esaminare nuovamente aspetti differenti della sicurezza nel proprio sistema. Utilizzarle per sviluppare il proprio piano.

Monitorare la sicurezza fisica

- Proteggere il supporto magnetico di riserva dal danneggiamento e dal furto.
- Limitare l'accesso alle stazioni di lavoro nelle aree pubbliche. Utilizzare il comando DSPOBJAUT per visualizzare chi dispone dell'autorizzazione *CHANGE alle stazioni di lavoro.

Monitorare i valori di sistema

- Verificare che le impostazioni corrispondano al modulo Selezione valori di sistema. Utilizzare il comando Stampa attributi riservatezza di sistema (PRTSYSSECA).
- Riesaminare le decisioni sui valori di sistema, in particolare quando si installano nuove applicazioni.

Monitorare i profili di gruppo

- Verificare che i profili di gruppo non dispongano di parola d'ordine. Utilizzare il comando DSPAUTUSR per verificare che tutti i profili di gruppo abbiano una parola d'ordine *NONE.
- Verificare che gli utenti corretti siano membri del gruppo. Utilizzare il comando DSPUSRPRF con l'opzione *GRPMBR per elencare i membri di un gruppo.
- Controllare le autorizzazioni speciali per ogni profilo di gruppo. Utilizzare il comando DSPUSRPRF. Se si sta effettuando l'esecuzione al livello di sicurezza 30, 40 o 50, i profili di gruppo non dovrebbero avere l'autorizzazione *ALLOBJ.

Monitorare i profili utente

- Verificare che i profili utente sul sistema appartengano ad una di queste categorie:
  - Profili utente per gli attuali dipendenti
  - Profili di gruppo
  - Profili proprietario dell'applicazione
  - Profili forniti da IBM (cominciano con la lettera Q)
- Eliminare il profilo utente quando l'azienda trasferisce un utente o quando un utente lascia l'azienda. Utilizzare il comando Modifica scadenza voce di pianificazione (CHGEXPSCDE) per cancellare o disabilitare automaticamente il profilo non appena il dipendente lascia l'azienda.

- Ricercare i profili inattivi e eliminarli. Utilizzare il comando Analisi attività profilo (ANZPRFACT) per disabilitare automaticamente i profili rimasti inattivi per un determinato periodo.
- Determinare quali utenti hanno una parola d'ordine uguale al loro nome profilo utente. Utilizzare il comando Analisi parole d'ordine predefinite (ANZDFTPWD). Utilizzare l'opzione di questo comando per forzare gli utenti a modificare le loro parole d'ordine al successivo collegamento al sistema.

  Attenzione: non eliminare dal sistema alcun profilo fornito dall'IBM. I profili forniti dall'IBM iniziano con la lettera Q.
- Prestare particolare attenzione agli utenti con una classe utente diversa da *USER e alle ragioni per cui questo avviene. Utilizzare il comando Stampa profilo utente (PRTUSRPRF) per ricevere una lista di tutti gli utenti, della relativa classe di utenti e delle autorizzazioni speciali. Mettere a confronto queste informazioni con il modulo Responsabilità del sistema.
- Controllare quali profili utente hanno il campo *Possibilità limitate* impostato su *NO.

Monitorare oggetti fondamentali

- Esaminare nuovamente gli utenti con accesso agli oggetti fondamentali. Utilizzare il comando Stampa autorizzazioni private (PRTPVTAUT) e Stampa oggetti autorizzati pubblicamente (PRTPUBAUT) per monitorare gli oggetti. Se un gruppo dispone dell'accesso, verificare i membri del gruppo con l'opzione *GRPMBR del comando DSPUSRPRF.
- Verificare chi può utilizzare i programmi dell'applicazione che forniscono l'accesso agli oggetti tramite un altro metodo di sicurezza, ad esempio l'autorizzazione adottata. Utilizzare il comando Stampa oggetti di adozione (PRTADPOBJ).

Monitorare accesso non autorizzato

- Istruire gli operatori di sistema in modo tale che siano vigili rispetto ai messaggi di sicurezza nella coda messaggi QSYSOPR. In particolare, essi devono informare il responsabile della riservatezza nel caso in cui si verificassero ripetuti tentativi di collegamento non riusciti. I messaggi di sicurezza sono compresi tra 2200 e 22FF e tra 4A00 e 4AFF. Essi hanno i prefissi CPF, CPI, CPC e CPD.
- Impostare il controllo della sicurezza per registrare i tentativi non autorizzati di accesso agli oggetti.

Consultare il paragrafo che segue Controllo della sicurezza.

Controllo della sicurezza

Durante il monitoraggio della sicurezza, il sistema operativo può registrare gli eventi di sicurezza che si verificano nel sistema. Tali eventi vengono registrati in speciali oggetti di sistema denominati **ricevitori di giornale**. E' possibile configurare i ricevitori di giornale in modo da registrare i diversi tipi di eventi di sicurezza, ad esempio la modifica di un valore di sistema o di un profilo utente o un tentativo di accesso non riuscito ad un oggetto. I seguenti valori controllano quali eventi vengono registrati:

- Valore di sistema QAUDCTL (controllo)
- Valore di sistema QAUDLVL (livello di controllo)
- Valore nei profili utente AUDLVL (livello di controllo)
- Valori nei profili utente OBJAUD (controllo dell'oggetto)
- Valore negli oggetti OBJAUD (controllo dell'oggetto).

Le informazioni contenute nei giornali di controllo vengono utilizzate per:

- Rilevare tentativi di violazione della sicurezza.
- Pianificare la migrazione ad un livello di sicurezza più alto.
- Monitorare l'utilizzo degli oggetti sensibili, ad esempio i file riservati.

Nei giornali di controllo sono disponibili dei comandi per visualizzare le informazioni in diversi modi.

Capitolo 12. Moduli di pianificazione della sicurezza di base del sistema

E' possibile copiare o stampare tali moduli da un browser.

Per stampare tutte le informazioni relative alla sicurezza di base, selezionare il pannello destro, quindi fare clic sull'icona PDF nell'intestazione dell'Information Center.

Per stampare un singolo modulo di pianificazione, fare clic sul collegamento corrispondente al modulo di pianificazione che si desidera stampare. Fare clic sul pannello destro, quindi fare clic sull'icona Stampa nel browser. In tal modo verrà stampato il modulo prescelto.

Qui di seguito è riportata una lista completa di tutti i moduli di pianificazione necessari pianificare e utilizzare la sicurezza di base del sistema con esito positivo:

- Modulo Pianificazione sicurezza fisica
- Modulo Descrizione dell'applicazione
- Modulo Convenzioni di denominazione
- Modulo Descrizione della libreria
- Modulo Selezione valori di sistema
- Modulo Responsabilità del sistema
- Modulo Identificazione gruppo di utenti
- Modulo Descrizione del gruppo di utenti
- Modulo Singolo profilo utente
- Modulo Lista di autorizzazioni
- Modulo Sicurezza della coda di emissione e della stazione di lavoro
- Modulo Installazione dell'applicazione

Modulo Pianificazione sicurezza fisica

Tabella 65. Modulo Pianificazione sicurezza fisica

Modulo Pianificazione sicurezza fisica	
Preparato da:	Data:
Istruzioni • Acquisire le informazioni su questo modulo in ″Pianificare la sicurezza delle risorse.″ • Utilizzare questo modulo per descrivere tutte le considerazioni sulla sicurezza relative all'ubicazione fisica della propria unità di sistema e delle unità collegate. • Non è necessario inserire le informazioni contenute in questo modulo nel sistema.	
Unità di sistema:	
Descrivere le misure di sicurezza per proteggere l'unità di sistema (ad esempio, una stanza chiusa a chiave):	
Quale posizione della chiave di blocco viene utilizzata generalmente?	
Dove si trova la chiave?	
Altri commenti relativi all'unità di sistema:	
Supporto magnetico di riserva e documentazione:	
Dove si trovano i nastri di riserva conservati nella propria azienda?	

Tabella 65. Modulo Pianificazione sicurezza fisica (Continua)

Dove si trovano i nastri di riserva conservati all'esterno della sede aziendale?	
Dove vengono conservate le parole d'ordine del responsabile della riservatezza, del servizio e DST?	
Dove si trova la documentazione importante di sistema, ad esempio il numero di serie e la configurazione?	

Modulo Pianificazione sicurezza fisica			Parte 2 di 2
Istruzioni aggiuntive per la Parte 2 • Elencare tutte le stazioni di lavoro o le stampanti la cui ubicazione potrebbe causare rischi per la sicurezza. Indicare quali misure di protezione saranno prese. Per una stampante, elencare gli esempi di prospetti riservati stampati nella colonna *Rischi per la sicurezza*. • Se si consente al sistema di configurare automaticamente le unità locali, non è possibile conoscere i nomi delle stazioni di lavoro e delle stampanti fino al termine dell'installazione del sistema. Se, nel momento in cui si prepara questo modulo, non si conoscono i nomi, completare le descrizioni (ad esempio l'ubicazione) e aggiungere i nomi in seguito.			
Sicurezza fisica delle stazioni di lavoro e delle stampanti			
Nome stazione di lavoro o stampante	Relativa ubicazione o descrizione	Rischi per la sicurezza	Misure di sicurezza da adottare

Modulo Descrizione dell'applicazione

Tabella 66. Modulo Descrizione dell'applicazione

Modulo Descrizione dell'applicazione	
Preparato da:	Data:
Istruzioni • Acquisire le informazioni su questo modulo in ″Descrivere l'applicazione″ e ″Pianificare la sicurezza delle risorse.″ • Preparare un modulo separato per ogni applicazione. • Non è necessario inserire le informazioni contenute in questo modulo nel sistema.	
Nome applicazione:	Abbreviazione:
Breve descrizione dell'applicazione:	
Nome menu primario:	Libreria:
Nome programma iniziale:	Libreria:
Elencare le librerie utilizzate dall'applicazione per i file e i programmi:	
Definire gli obiettivi della sicurezza per l'applicazione, ad esempio se alcune informazioni sono riservate:	

Modulo Convenzioni di denominazione

Tabella 67. Modulo Convenzioni di denominazione

Modulo Convenzioni di denominazione	
Preparato da:	Data:
Istruzioni • Acquisire le informazioni su questo modulo in ″Descrivere le applicazioni.″ • Non è necessario immettere informazioni da questo modulo direttamente nel sistema. • Utilizzare questo modulo per descrivere il modo in cui assegnare i nomi agli oggetti sul sistema. Fare esempi di ognuno.	
Tipo di oggetto	**Convenzione di denominazione**
Profili di gruppo	
Profili utente	
Liste di autorizzazioni	
Librerie	
File	
Calendari	
Unità	
Nastri	

Modulo Descrizione della libreria

Tabella 68. Modulo Descrizione della libreria

Modulo Descrizione della libreria	Parte 1 di 2
Preparato da:	Data:
Istruzioni: • Acquisire le informazioni su questo modulo in ″Pianificare la sicurezza dell'utente″ e ″Pianificare la sicurezza delle risorse.″ • Utilizzare questo modulo per descrivere le librerie principali e definire i requisiti della sicurezza delle risorse. • Completare un modulo per ogni libreria dell'applicazione principale sul sistema. • Accedere alle informazioni da questo modulo in ″Impostare la sicurezza delle risorse.″	
Nome libreria:	Nome descrittivo (testo):
Descrivere brevemente la funzione di questa libreria:	
Definire gli obiettivi della sicurezza per la libreria, ad esempio se le informazioni sono riservate:	
Autorizzazione pubblica alla libreria:	
Autorizzazione pubblica agli oggetti nella libreria:	
Autorizzazione pubblica per i nuovi oggetti (CRTAUT):	
Proprietario libreria:	

Modulo Descrizione della libreria		Parte 2 di 2
Preparato da:	Data:	
Nome libreria:		

Istruzioni aggiuntive per la Parte 2: • Nella tabella seguente, elencare individui oppure oggetti che necessitano dell'autorizzazione specifica. • Specificare il tipo di autorizzazione richiesto: *ALL, *CHANGE, *USE o *EXCLUDE.				
Elencare le autorizzazioni specifiche per gli oggetti della libreria				
Profilo di gruppo o profilo utente	Nome oggetto	Tipo oggetto	Autorizzazione necessaria	Lista di autorizzazioni

Modulo Selezione valori di sistema

Tabella 69. Modulo Selezione valori di sistema

Modulo Selezione valori di sistema		Parte 1 di 2
Preparato da:		Data:
Istruzioni • Acquisire le informazioni su questo modulo in ″Pianificare l'approccio generale .″ • Utilizzare questo modulo per registrare le scelte per i valori di sistema che influenzano la sicurezza e la personalizzazione. • Utilizzare l'opzione **1** dal Menu SETUP per accedere alla Parte 1 di questo modulo.		
Valori dal pannello Modifica opzioni di sistema		
Valore di sistema/attributo di rete	**Scelta consigliata**	**Scelta personale**
Nome sistema		
Separatore data (QDATSEP)		
Formato data (QDATFMT)		
Separatore ora (QTIMSEP)		
Formato di denominazione unità per nuove unità (QDEVNAMING)	1 (sistema iSeries)	
Stampante di sistema (QPRTDEV)		
Livello di sicurezza (QSECURITY)	40	
Consentire ai responsabili della riservatezza di collegarsi a qualsiasi stazione video (QLMTSECOFR)	N	
Salvare le informazioni relative all'account del lavoro sull'emissione completa della stampante (QACGLVL)	N (*NONE)	

Modulo Selezione valori di sistema	Parte 2 di 2

Istruzioni aggiuntive per la Parte 2 • Acquisire ulteriori informazioni sulla Parte 2 di questo modulo in ″Impostare i valori di sistema.″ • Utilizzare il comando Gestione valore di sistema (WRKSYSVAL) per accedere alla Parte 2.		
Valori di sistema della sicurezza		
Valore di sistema	**Scelta consigliata**	**Scelta personale**
Intervallo supero tempo lavoro inattivo (QINACTITV)	da 30 a 60	
Coda messaggi lavoro inattivo (QINACTMSGQ)	*DSCJOB	
Limite sessioni unità (QLMTDEVSSN)	1 (Sì)	
Azione da eseguire per i tentativi di collegamento non riusciti (QMAXSGNACN)	3 (Disabilitare entrambi)	
Numero massimo di tentativi di collegamento consentito (QMAXSIGN)	da 3 a 5	
Intervallo scadenza parola d'ordine (QPWDEXPITV)	da 30 a 60	
Lunghezza massima della parola d'ordine (QPWDMAXLEN)	8	
Lunghezza minima della parola d'ordine (QPWDMINLEN)	6	
Richiedere parole d'ordine differenti (QPWDRQDDIF)	7 (6 parole d'ordine univoche)	
Altri valori di sistema		
Valore di sistema	**Scelta consigliata**	**Scelta personale**
Intervallo supero tempo lavoro scollegato (QDSCJOBITV)	300	
Nota: è possibile che si desideri impostare altri valori di sistema correlati alla sicurezza. Consultare il Capitolo 3 di *Security-Reference* (SC41-5302-04) per una lista completa dei valori di sistema e i consigli relativi alla sicurezza.		

Modulo Responsabilità del sistema

Tabella 70. Modulo Responsabilità del sistema

Modulo Responsabilità del sistema			
Preparato da:			Data:
Istruzioni: • Acquisire le informazioni su questo modulo in ″Pianificare i singoli profili utente.″ • Utilizzare questo modulo per elencare tutti coloro che hanno una classe utente diversa da *USER. • Trasferire le informazioni da questo modulo alla colonna *Classe utente* del modulo Singolo profilo utente.			
Chi è il responsabile principale della riservatezza? Chi è il sostituto del responsabile della riservatezza?			
Nome profilo	Nome utente	Classe	Commenti

Modulo Identificazione gruppo di utenti

Tabella 71. Modulo Identificazione gruppo di utenti

Modulo Identificazione gruppo di utenti								
Preparato da:		Data:						
Istruzioni: • Acquisire le informazioni su questo modulo in ″Pianificare i gruppi di utenti.″ • Questo modulo consente di identificare i gruppi di utenti che necessitano di applicazioni simili. 1. Elencare le applicazioni principali dall'inizio del modulo. 2. Elencare gli utenti nella colonna a sinistra. 3. Contrassegnare le applicazioni necessarie per ogni utente. • Non è necessario inserire le informazioni contenute in questo modulo nel sistema.								
		Accesso necessario per le applicazioni						
Nome utente	Reparto	APP:	APP:	APP:	APP:	APP:	APP:	APP:
Nota: • Se l'ambiente della sicurezza è *non rigoroso*, utilizzare una **X** per contrassegnare le applicazioni necessarie per l'utente. • Se l'ambiente della sicurezza è *rigoroso*, potrebbe essere necessario utilizzare **C** (modifica) e **V** (visualizza) per specificare *come* vengono utilizzate le applicazioni.								

Modulo Descrizione del gruppo di utenti

Tabella 72. Modulo Descrizione del gruppo di utenti

Modulo Descrizione del gruppo di utenti	Parte 1 di 2
Preparato da:	Data:
Istruzioni per la Parte 1 • Acquisire le informazioni su questo modulo in ″Pianificare i gruppi di utenti.″ • Acquisire le informazioni su come compilare questo modulo in ″Impostare la sicurezza dell'utente.″ • Preparare un modulo separato per ogni gruppo che utilizzerà il sistema. • Utilizzare il comando Creazione descrizione lavoro (CRTJOBD) per creare una descrizione lavoro per il gruppo. La descrizione lavoro ha la lista iniziale delle librerie del gruppo.	
Nome profilo di gruppo: Descrizione del gruppo:	

Tabella 72. Modulo Descrizione del gruppo di utenti (Continua)

Applicazione principale per il gruppo: Elencare le altre applicazioni necessarie per il gruppo:
Elencare ogni libreria necessaria per il gruppo. Contrassegnare (✓) ogni libreria che dovrebbe trovarsi nella lista librerie iniziale del gruppo:
Nota: consultare il modulo Descrizione dell'applicazione per ogni applicazione elencata nella sezione precedente per individuare le librerie utilizzate dall'applicazione.

Modulo Descrizione del gruppo di utenti		Parte 2 di 2
Istruzioni aggiuntive per la Parte 2 • Le tabelle riportate di seguito elencano tutti i campi visualizzati sul pannello Creazione profilo utente. I campi sono divisi in due gruppi: quelli in cui è necessario effettuare una selezione e quelli in cui IBM consiglia il valore predefinito. • Utilizzare il pannello Gestione profili utente o il comando Creazione profilo utente (CRTUSRPRF) per immettere le informazioni contenute in questa parte del modulo nel proprio sistema.		
Scegliere i valori per questi campi nel profilo di gruppo:		
Nome campo	**Scelta consigliata**	**Scelta personale**
Nome profilo di gruppo (Utente)		
Parola d'ordine	*NONE	
Classe utente (Tipo utente)	*USER	
Libreria corrente (Libreria predefinita)	*uguale al nome profilo di gruppo*	
Programma iniziale da richiamare (Programma di collegamento)		
Libreria programma iniziale		
Menu iniziale (Primo menu)		
Libreria menu iniziale		
Possibilità limitate (Limitare utilizzo della riga comandi)	*YES	
Testo (Descrizione utente)		
Descrizione lavoro	*uguale al nome profilo di gruppo*	
Libreria descrizione lavoro		
Nome profilo di gruppo (Gruppo di utenti)	*NONE	
Unità di stampa (Stampante predefinita)		
Coda di emissione	*DEV	
Nota: questi campi si trovano nell'ordine in cui vengono visualizzati sul pannello Creazione profilo utente (utilizzando F4).		
Utilizzare i valori forniti dal sistema (predefiniti) per i campi riportati di seguito:		
Codice contabile	Buffer della tastiera	Autorizzazione pubblica
Livello assistenza	ID lingua	Impostare scadenza parola d'ordine
Programma di attenzione	Limite sessioni unità	Ordine di sequenza
CCSID	Memoria massima	Autorizzazione speciale
ID paese o regione	Coda messaggi	Ambiente speciale

Visualizzazione informazioni sul collegamento	Intervallo di scadenza della parola d'ordine	Stato
Parola d'ordine documento	Limite priorità	Opzioni utente
Nota: I campi in questa lista sono sistemati in ordine alfabetico.		

Modulo Singolo profilo utente

Tabella 73. Modulo Singolo profilo utente

Modulo Singolo profilo utente						
Preparato da:			Data:			
Istruzioni: • Acquisire le informazioni su come preparare questo modulo in ″Pianificare i singoli profili utente.″ • Utilizzare questo modulo per registrare le informazioni relative ai singoli utenti del sistema. Completare il modulo per ogni gruppo di utenti (profilo di gruppo) che si trova sul proprio sistema. • Utilizzare le colonne vuote a destra di ogni campo aggiuntivo che si desidera specificare per singoli utenti. • Acquisire le informazioni su come compilare questo modulo in ″Impostare i singoli utenti.						
Nomi profilo di gruppo:						
Proprietario degli oggetti creati:			Autorizzazione di gruppo agli oggetti creati:			
Tipo di autorizzazione di gruppo:						
Creare una voce per ogni membro del gruppo:						
Profilo utente	Testo (descrizione)	Classe utente	Possibilità limitate			

Modulo Lista di autorizzazioni

Tabella 74. Modulo Lista di autorizzazioni

Modulo Lista di autorizzazioni	
Preparato da:	Data:
Istruzioni • Acquisire le informazioni su questo modulo in ″Pianificare la sicurezza delle risorse.″ • Preparare un modulo per ogni lista di autorizzazioni. • Utilizzare questo modulo per elencare gli oggetti protetti dalla lista, dai gruppi e dagli individui che hanno accesso alla lista. • Acquisire le informazioni su come compilare questo modulo in ″Impostare la sicurezza delle risorse.″	
Nome lista di autorizzazioni:	

Tabella 74. Modulo Lista di autorizzazioni (Continua)

Descrizione:					
Elencare gli oggetti protetti dalla lista					
Nome oggetto	Tipo oggetto	Libreria oggetto	Nome oggetto	Tipo oggetto	Libreria oggetto
Elencare i gruppi e gli utenti che hanno accesso alla lista					
Gruppo o utente	Tipo di accesso consentito	Gestione liste?	Gruppo o utente	Tipo di accesso consentito	Gestione liste?

Modulo Sicurezza della coda di emissione di stampa e della stazione di lavoro

Tabella 75. Modulo Sicurezza della coda di emissione di stampa e della stazione di lavoro

Modulo Sicurezza della coda di emissione di stampa e della stazione di lavoro				
Preparato da:	Data:			
Istruzioni • Acquisire le informazioni su questo modulo in ″Proteggere l'emissione di stampa.″ • Creare una voce su questo modulo per ogni stazione di lavoro o emissione di stampa che richiede una protezione speciale. • Acquisire le informazioni su come compilare questo modulo in ″Proteggere le stazioni di lavoro.″				
Elencare i parametri per le code di emissione limitate:				
Nome coda emissione	Libreria coda emissione	Visualizzazione file (DSPDTA)	Autorizzazione da verificare (AUTCHK)	Controllo operatore (OPRCTL)

Tabella 75. Modulo Sicurezza della coda di emissione di stampa e della stazione di lavoro (Continua)

Stazioni di lavoro del responsabile della riservatezza: Se si limita il responsabile della riservatezza a stazioni di lavoro specifiche (il valore di sistema QLMTSECOFR è sì), elencare le stazioni di lavoro autorizzate per il responsabile della riservatezza e per chiunque disponga dell'autorizzazione *ALLOBJ:	
Elencare le autorizzazioni per le stazioni di lavoro limitate:	
Nome stazione di lavoro	Gruppi o utenti autorizzati (autorizzazione *CHANGE)
Nota: le stazioni di lavoro limitate devono avere l'autorizzazione pubblica impostata su *EXCLUDE.	

Modulo Installazione dell'applicazione

Tabella 76. Modulo Installazione dell'applicazione

Modulo Installazione dell'applicazione		Parte 1 di 2
Preparato da:		Data:
Istruzioni • Acquisire le informazioni su questo modulo in ″Pianificare l'installazione dell'applicazione.″ • Preparare un modulo per ogni applicazione che sarà installata. • Utilizzare il modulo per pianificare il modo in cui verrà stabilita l'autorizzazione pubblica e la proprietà per le applicazioni dopo averle caricate. • Acquisire le informazioni su come compilare questo modulo in ″Impostare la sicurezza delle risorse.″		
Nome applicazione:		
Descrizione:		
Elencare e spiegare i profili che devono essere creati per installare l'applicazione:		
Nome libreria:		
	Prima dell'installazione	Dopo l'installazione
Proprietario libreria		
Proprietario oggetto		
Autorizzazione pubblica alla libreria		
Autorizzazione pubblica all'oggetto		
Autorizzazione pubblica per i nuovi oggetti		
Nome libreria:		
	Prima dell'installazione	Dopo l'installazione
Proprietario libreria		
Proprietario oggetto		
Autorizzazione pubblica alla libreria		
Autorizzazione pubblica all'oggetto		
Autorizzazione pubblica per i nuovi oggetti		

Modulo Installazione dell'applicazione		Parte 2 di 2
Nome libreria:		
	Prima dell'installazione	Dopo l'installazione
Proprietario libreria		
Proprietario oggetto		
Autorizzazione pubblica alla libreria		
Autorizzazione pubblica all'oggetto		
Autorizzazione pubblica per i nuovi oggetti		
Nome libreria:		
	Prima dell'installazione	Dopo l'installazione
Proprietario libreria		
Proprietario oggetto		
Autorizzazione pubblica alla libreria		
Autorizzazione pubblica all'oggetto		
Autorizzazione pubblica per i nuovi oggetti		
Nome libreria:		
	Prima dell'installazione	Dopo l'installazione
Proprietario libreria		
Proprietario oggetto		
Autorizzazione pubblica alla libreria		
Autorizzazione pubblica all'oggetto		
Autorizzazione pubblica per i nuovi oggetti		

Printed in Denmark by IBM Danmark A/S