**SICUREZZA DATABASE**

Le autorizzazioni del Motore di database vengono gestite a livello di server tramite gli account di accesso e i ruoli del server e a livello di database tramite gli utenti e i ruoli del database. Il modello per il Database SQL espone lo stesso sistema all'interno di ogni database, ma le autorizzazioni a livello di server non saranno disponibili. Questo argomento illustra alcuni concetti di base sulla sicurezza e quindi descrive un'implementazione tipica delle autorizzazioni.

Entità di sicurezza

Con entità di sicurezza si definiscono le identità che usano SQL Server e a cui è possibile assegnare delle autorizzazioni per eseguire varie azioni. Si tratta in genere di utenti o gruppi di utenti, ma possono essere altre entità che fingono di essere utenti. Le entità di sicurezza possono essere create e gestite con il linguaggio Transact-SQL elencato o con SQL Server Management Studio.

Logins

Gli account di accesso sono account utente singoli per l'accesso al Motore di database di SQL Server. SQL Server e il Database SQL supportano account di accesso basati sull'autenticazione di Windows e account di accesso basati sull'autenticazione di SQL Server .

Ruoli predefiniti del server

In SQL Server i ruoli predefiniti del server sono costituiti da un set di ruoli preconfigurati che forniscono una serie appropriata di autorizzazioni a livello di server. Gli account di accesso possono essere aggiunti ai ruoli con l'istruzione ALTER SERVER ROLE ... ADD MEMBER . Per altre informazioni, vedere ALTER SERVER ROLE (Transact-SQL). Database SQL non supporta i ruoli predefiniti del server, ma ha due ruoli nel database master (dbmanager e loginmanager) che fungono da ruoli del server.

Ruoli del server definiti dall'utente

In SQL Serverè possibile creare ruoli del server personalizzati e assegnarvi autorizzazioni a livello di server. Gli account di accesso possono essere aggiunti ai ruoli del server con l'istruzione ALTER SERVER ROLE ... ADD MEMBER . Per altre informazioni, vedere ALTER SERVER ROLE (Transact-SQL). Database SQL non supporta i ruoli del server definiti dall'utente.

Utenti di database

Agli account di accesso viene concesso l'accesso a un database creando un utente in un database ed eseguendo il mapping di tale utente di database all'account di accesso. In genere, il nome utente di database è identico al nome dell'account di accesso, anche se non è necessario. Ogni utente di database esegue il mapping a un singolo account di accesso. Il mapping di un account di accesso può essere eseguito a un solo utente in un database, ma può essere eseguito come utente di database in diversi database.

Gli utenti di database possono anche essere creati senza avere un account di accesso corrispondente e vengono denominati utenti di database indipendente. Microsoft promuove l'uso di utenti di database indipendente perché semplifica lo spostamento di un database in un altro server. Analogamente agli account di accesso, gli utenti di database indipendente possono usare l'autenticazione di Windows o l'autenticazione di SQL Server . Per altre informazioni, vedere Utenti di database indipendente: rendere portabile un database.

Esistono 12 tipi di utenti con piccole differenze per la modalità di autenticazione e la relativa rappresentazione.

Ruoli predefiniti del database

I ruoli predefiniti del database sono costituiti da un set di ruoli preconfigurati che forniscono una serie appropriata di autorizzazioni a livello di database. Gli utenti del database e i ruoli del database definiti dall'utente possono essere aggiunti ai ruoli predefiniti del database con l'istruzione ALTER ROLE ... ADD MEMBER . Per altre informazioni, vedere ALTER ROLE (Transact-SQL).

Ruoli del database definiti dall'utente

Gli utenti con l'autorizzazione CREATE ROLE possono creare nuovi ruoli del database definiti dall'utente per rappresentare gruppi di utenti con autorizzazioni comuni. In genere, le autorizzazioni vengono concesse o negate per l'intero ruolo, semplificando la gestione e il monitoraggio delle autorizzazioni. Gli utenti di database possono essere aggiunti ai ruoli del database con l'istruzione ALTER ROLE ... ADD MEMBER .

Le autorizzazioni hanno una gerarchia padre/figlio, ovvero se si concede l'autorizzazione SELECT per un database, tale autorizzazione include l'autorizzazione SELECT per tutti gli schemi (figlio) presenti nel database. Se si concede l'autorizzazione SELECT per uno schema, tale autorizzazione include l'autorizzazione SELECT per tutte le tabelle e le viste (figlio) presenti nello schema. Le autorizzazioni sono transitive, ovvero se si concede l'autorizzazione SELECT per un database, tale autorizzazione include l'autorizzazione SELECT per tutti gli schemi (figlio) e tutte le tabelle e le viste (nipote).

Le autorizzazioni contengono anche le autorizzazioni implicite. L'autorizzazione CONTROL per un oggetto concede in genere tutte le altre autorizzazioni per l'oggetto.

Poiché sia la gerarchia padre/figlio che la gerarchia implicita possono agire sulla stessa autorizzazione, il sistema di autorizzazioni può diventare complicato. Prendiamo ad esempio una tabella (Region) di uno schema (Customers) in un database (SalesDB).

CONTROL per la tabella Region include tutte le altre autorizzazioni per la tabella Region, tra cui ALTER, SELECT, INSERT, UPDATE, DELETE e altre autorizzazioni.

SELECT per lo schema Customers a cui appartiene la tabella Region include l'autorizzazione SELECT per la tabella Region.

L'autorizzazione SELECT per la tabella Region può quindi essere ottenuta con una di queste sei istruzioni:

GRANT SELECT ON OBJECT::Region TO Ted;

GRANT CONTROL ON OBJECT::Region TO Ted;

GRANT SELECT ON SCHEMA::Customers TO Ted;

GRANT CONTROL ON SCHEMA::Customers TO Ted;

GRANT SELECT ON DATABASE::SalesDB TO Ted;

GRANT CONTROL ON DATABASE::SalesDB TO Ted;

Concedere l'autorizzazione minima

La prima autorizzazione elencata in precedenza (GRANT SELECT ON OBJECT::Region TO Ted;) è la più granulare, ovvero tale istruzione è l'autorizzazione minima possibile che concede l'autorizzazione SELECT. Non sono incluse autorizzazioni per gli oggetti subordinati. È una buona entità concedere sempre il minor numero possibile di autorizzazioni (è possibile leggere altre informazioni sul principio dei privilegi minimi),ma allo stesso tempo (contraddittorio) provare a concedere a livelli più elevati per semplificare il sistema di concessione. Se quindi Ted deve ottenere le autorizzazioni per l'intero schema, concedere SELECT una sola volta a livello di schema, anziché concedere SELECT molte volte a livello di tabella o di vista. La progettazione del database ha un notevole impatto sull'efficacia di questa strategia. Questa strategia funziona meglio quando il database viene progettato in modo tale che gli oggetti che devono ottenere autorizzazioni identiche vengano inclusi in un singolo schema.

Quando si progetta un database e i relativi oggetti, fin dall'inizio, pianificare chi o quali applicazioni accederanno a quali oggetti e in base a tale posizione, ovvero tabelle ma anche viste, funzioni e stored procedure negli schemi in base ai bucket di tipo di accesso per quanto possibile.

Autorizzazioni e ruoli predefiniti del server e ruoli predefiniti del database

Le autorizzazioni dei ruoli predefiniti del server e dei ruoli predefiniti del database sono simili ma non esattamente uguali alle autorizzazioni granulari. Ad esempio, i membri del ruolo predefinito del server sysadmin hanno tutte le autorizzazioni per l'istanza di SQL Server, come gli account di accesso con l'autorizzazione CONTROL SERVER . Ma concedere l'autorizzazione CONTROL SERVER non rende un account di accesso membro del ruolo predefinito del server sysadmin e aggiungere un account di accesso al ruolo predefinito del server sysadmin non concede in modo esplicito l'autorizzazione CONTROL SERVER all'account di accesso. Una stored procedure potrebbe talvolta verificare le autorizzazioni controllando il ruolo predefinito e non controllando l'autorizzazione granulare. Ad esempio, per scollegare un database è necessaria l'appartenenza al ruolo predefinito del database db\_owner . L'autorizzazione CONTROL DATABASE equivalente non è sufficiente. Questi due sistemi operano in parallelo ma raramente interagiscono tra loro. Se possibile, Microsoft consiglia di usare il sistema più recente di autorizzazioni granulari anziché i ruoli predefiniti.

sa Login

L'account SQL Server sa di accesso è un'entità a livello di server. Per impostazione predefinita, questo account viene creato durante l'installazione di un'istanza. A partire da SQL Server 2005 (9.x), il database predefinito di sa è il database master. diversamente da quanto consentito nelle versioni precedenti di SQL Server. L'account di accesso sa è un membro del ruolo predefinito a livello di server sysadmin. L'account di accesso sa dispone di tutte le autorizzazioni per il server e non può essere limitato. L'account di accesso sa non può essere eliminato, ma può essere disabilitato in modo da impedirne l'uso.

Utente dbo e schema dbo

L'utente dbo è un'entità utente speciale in ogni database. Tutti gli amministratori di SQL Server, i membri del ruolo predefinito del server sysadmin, l'account di accesso sa e i proprietari del database accedono al database come utenti dbo. L'utente dbo dispone di tutte le autorizzazioni nel database e non può essere limitato o eliminato. dbo rappresenta il proprietario del database, ma l'account utente dbo non equivale al ruolo predefinito del database db\_owner, mentre il ruolo predefinito del database db\_owner non equivale all'account utente registrato come proprietario del database.

L'utente dbo è proprietario dello schema dbo. Lo schema dbo è lo schema predefinito per tutti gli utenti, a meno che non venga specificato uno schema diverso. Lo schema dbo non può essere eliminato.

Ruolo del server public e ruolo del database

Ogni account di accesso appartiene al ruolo predefinito del server public e ogni utente del database appartiene al ruolo del database public. Quando a un account di accesso o a un utente non sono state concesse o negate autorizzazioni specifiche per un'entità a protezione diretta, l'account di accesso o l'utente eredita le autorizzazioni concesse al ruolo public su tale entità a protezione diretta. Il ruolo predefinito del server public e il ruolo predefinito del database public non possono essere eliminati. Tuttavia è possibile revocare le autorizzazioni dei ruoli public. Esistono numerose autorizzazioni assegnate per impostazione predefinita ai ruoli public. La maggior parte di queste autorizzazioni è necessaria per le operazioni di routine nel database, ovvero quelle operazioni che tutti gli utenti devono essere in grado di eseguire. Prestare attenzione durante la revoca delle autorizzazioni dell'account di accesso public o dell'utente perché questa operazione ha ripercussioni su tutti gli account di accesso e su tutti gli utenti. In genere non è consigliabile negare le autorizzazioni all'account di accesso public perché l'istruzione deny esegue l'override di qualsiasi istruzione grant che è possibile eseguire sui singoli utenti.

Per gestire facilmente le autorizzazioni nei database, SQL Server fornisce diversi ruoli che sono entità di sicurezza che raggruppano altre entità. I ruoli sono analoghi ai gruppi nel sistema operativo Microsoft Windows. L'ambito delle autorizzazioni dei ruoli a livello di database è l'intero database.

Per aggiungere e rimuovere utenti a un ruolo del database, usare le opzioni ADD MEMBER e DROP MEMBER dell'istruzione ALTER ROLE

Esistono due tipi di ruoli a livello di database: i ruoli predefiniti del database , che sono predefiniti nel database, e i ruoli del database definiti dall'utente , che possono essere creati.

I ruoli predefiniti del database vengono definiti a livello di database e sono presenti in ogni database. I membri del ruolo del database db\_owner possono gestire l'appartenenza ai ruoli predefiniti del database. Nel database msdb sono presenti anche alcuni ruoli predefiniti del database per scopi specifici.

È possibile aggiungere qualsiasi account del database e altri ruoli ai ruoli a livello di database.

Le autorizzazioni dei ruoli del database definiti dall'utente possono essere personalizzate usando le istruzioni GRANT, DENY e REVOKE . Ruoli predefiniti del database

La tabella seguente contiene i ruoli predefiniti del database e le rispettive caratteristiche. Questi ruoli esistono in tutti i database. Fatta eccezione per il ruolo del database pubblico, non è possibile modificare le autorizzazioni concesse ai ruoli predefiniti del database.

**Nome del ruolo predefinito del database** Descrizione

**db\_owner** I membri del db\_owner ruolo predefinito del database possono eseguire tutte le attività di configurazione e manutenzione nel database drop e anche il database in SQL Server. In Database SQL e Azure Synapse alcune attività di manutenzione richiedono autorizzazioni a livello di server e non possono essere eseguite da ruoli db\_owners.

**db\_securityadmin** I membri del ruolo predefinito del database db\_securityadmin possono modificare le appartenenze al ruolo solo per i ruoli personalizzati e gestire le autorizzazioni. I membri di questo ruolo possono potenzialmente elevare i propri privilegi ed è consigliabile monitorarne le azioni.

**db\_accessadmin** I membri del ruolo predefinito del database db\_accessadmin possono aggiungere o rimuovere le autorizzazioni di accesso al database per gli account di accesso di Windows, i gruppi di Windows e gli account di accesso di SQL Server .

**db\_backupoperator** I membri del ruolo predefinito del database db\_backupoperator possono eseguire il backup del database.

**db\_ddladmin** I membri del ruolo predefinito del database db\_ddladmin possono eseguire qualsiasi comando DDL (Data Definition Language) in un database.

**db\_datawriter** I membri del ruolo predefinito del database db\_datawriter possono aggiungere, eliminare o modificare i dati di tutte le tabelle utente.

**db\_datareader** I membri del db\_datareader ruolo predefinito del database possono leggere tutti i dati da tutte le tabelle e viste utente. Gli oggetti utente possono esistere in qualsiasi schema, ad eccezione di sys e INFORMATION\_SCHEMA.

**db\_denydatawriter** I membri del ruolo predefinito del database db\_denydatawriter non possono aggiungere, modificare o eliminare dati delle tabelle utente contenute in un database.

**db\_denydatareader** I membri del db\_denydatareader ruolo predefinito del database non possono leggere dati dalle tabelle utente e dalle viste all'interno di un database.

Non è possibile modificare le autorizzazioni concesse ai ruoli predefiniti del database. La figura seguente mostra le autorizzazioni assegnate ai ruoli predefiniti del database:

