**SICUREZZA DATABASE (2° parte)**

Ruoli applicazione

Un ruolo applicazione è un'entità di database che consente a un'applicazione di funzionare con proprie autorizzazioni simili a quelle per utenti. I ruoli applicazione possono essere utilizzati per consentire l'accesso a dati specifici solo agli utenti che si collegano attraverso un'applicazione particolare. A differenza dei ruoli di database, i ruoli applicazione non contengono membri e sono inattivi per impostazione predefinita. I ruoli applicazione vengono abilitati usando sp\_setapprole, che richiede una password. Poiché si tratta di entità a livello di database, i ruoli applicazione possono accedere ad altri database solo tramite le autorizzazioni concesse in questi database all'account utente guest. Ogni database in cui l'account utente guest è stato disabilitato non sarà quindi accessibile ai ruoli applicazione di altri database.

Connessione attraverso un ruolo applicazione

Il passaggio da un contesto di sicurezza all'altro da parte di un ruolo applicazione si svolge nel modo seguente:

Un utente esegue un'applicazione client.

L'applicazione client si collega a un'istanza di SQL Server come utente.

L'applicazione esegue quindi la stored procedure sp\_setapprole con una password nota solo all'applicazione.

Se il nome del ruolo applicazione e la password sono validi, il ruolo applicazione viene abilitato.

A questo punto la connessione perde le autorizzazioni dell'utente e assume le autorizzazioni del ruolo applicazione.

Le autorizzazioni acquisite attraverso il ruolo applicazione rimangono valide per tutta la durata della connessione.

Nelle versioni precedenti di SQL Server, l'unico modo per un utente di ritornare al contesto di sicurezza originale dopo l'avvio di un ruolo applicazione consiste nel disconnettersi e riconnettersi a SQL Server. A partire da SQL Server 2005 (9.x), sp\_setapprole dispone di un'opzione che crea un cookie. Il cookie contiene informazioni di contesto precedenti all'abilitazione del ruolo applicazione. Questo cookie può essere usato da sp\_unsetapprole per riportare la sessione al contesto originale

Utenti di database indipendente: rendere portabile un database

Usare gli utenti di database indipendente per autenticare le connessioni SQL Server e Database SQL a livello di database. Un database indipendente è un database isolato dagli altri database e dall'istanza di SQL Server/ Database SQL (e del database master) che ospita il database. SQL Server supporta gli utenti di database indipendente per l'autenticazione di Windows e SQL Server . Quando si usa Database SQL, combinare gli utenti di del database indipendente con le regole firewall a livello di database. Questo argomento illustra le differenze e i vantaggi correlati all'uso del modello di database indipendente rispetto al modello tradizionale basato su account di accesso/utente e alle regole firewall a livello di server o Windows. L'uso del modello tradizionale basato su account di accesso/utente e delle regole firewall a livello di server può essere ancora necessario in scenari specifici, per la gestibilità o per la logica di business dell'applicazione.

Modello tradizionale basato su account di accesso e utente

Nel modello di connessione tradizionale gli utenti di Windows o i membri di gruppi di Windows si connettono al Motore di database fornendo le credenziali utente o di gruppo autenticate da Windows. In alternativa si può specificare un nome e una password e connettersi usando l'autenticazione di SQL Server . In entrambi i casi, il database master deve disporre di un account di accesso corrispondente alle credenziali di connessione. Dopo che il Motore di database ha verificato le credenziali di autenticazione di Windows o ha autenticato le credenziali di autenticazione di SQL Server , la connessione in genere tenta di connettersi a un database utente. Per connettersi a un database utente, l'account di accesso deve poter essere sottoposto a mapping (ovvero associato) a un utente del database nel database utente. La stringa di connessione può inoltre specificare la connessione a un database specifico. Questo è facoltativo in SQL Server , ma obbligatorio nel Database SQL.

L'aspetto importante è che sia l'account di accesso (nel database master) che l'utente (nel database utente) devono esistere ed essere correlati tra loro. Ciò significa che la connessione al database utente presenta una dipendenza dall'account di accesso nel database master e questo limita la capacità del database di essere spostato in un server SQL Server o database SQL di Azure di hosting diverso. Se inoltre per qualsiasi motivo non è disponibile una connessione al database master (ad esempio è in corso un failover), aumenterà il tempo complessivo di connessione oppure potrà verificarsi un timeout della connessione. Questo potrebbe quindi ridurre la scalabilità della connessione.

Modello di utente di database indipendente

Nel modello di utente di database indipendente l'account di accesso nel database master non è presente. Al contrario, il processo di autenticazione si verifica nel database utente e l'utente del database nel database utente non dispone di un account di accesso associato nel database master. Il modello di utente di database indipendente supporta sia l'autenticazione di Windows che l'autenticazione di SQL Server e può essere usato sia in SQL Server che nel Database SQL. Per connettersi come utente di database indipendente, la stringa di connessione deve sempre contenere un parametro per il database utente in modo che il Motore di database sappia quale database è responsabile della gestione del processo di autenticazione. L'attività dell'utente di database indipendente è limitata al database di autenticazione, pertanto durante la connessione come utente di database indipendente, l'account utente del database deve essere creato in modo indipendente in ogni database richiesto dall'utente. Per modificare i database, gli utenti del Database SQL devono creare una nuova connessione. Gli utenti di database indipendente in SQL Server possono modificare i database se è presente un utente identico in un altro database.

Per Database SQL e Azure Synapse Analytics, dal momento che il nome del database è sempre richiesto nella stringa di connessione, non sono necessarie modifiche della stringa di connessione quando si passa dal modello tradizionale al modello di utente di database indipendente. Per le connessioni a SQL Server , il nome del database deve essere aggiunto alla stringa di connessione, se non è già presente.

Importante

Quando si usa il modello tradizionale, i ruoli e le autorizzazioni a livello di server possono limitare l'accesso a tutti i database. Quando si usa il modello di database indipendente, i proprietari del database e gli utenti del database con autorizzazione ALTER ANY USER possono concedere l'accesso al database. In questo modo si riduce il controllo di accesso di account di accesso server con privilegi elevati e si espande il controllo di accesso per includere utenti di database con privilegi elevati.

Firewall

SQL Server

Le regole di Windows Firewall si applicano a tutte le connessioni e producono gli stessi effetti sugli account di accesso (connessioni con modello tradizionale) e sugli utenti di database indipendente.

Database SQL Firewall

Database SQL consente regole del firewall separate per connessioni a livello di server (account di accesso) e per connessioni a livello di database (utenti di database indipendente). Durante la connessione a un database utente vengono verificate per prime le regole del firewall a livello di database. Se non esistono regole che consentono l'accesso al database, vengono verificate le regole del firewall a livello di server, operazione che richiede l'accesso al database master del server di database SQL. L'uso combinato di regole del firewall a livello di database e utenti di database indipendente consente di non dover accedere al database master del server durante la connessione e implica di conseguenza un miglioramento della scalabilità della connessione.

Differenze di sintassi

| **Modello tradizionale** | **Modello di utente di database indipendente** |
| --- | --- |
| **Quando connesso al database master:**  CREATE LOGIN login\_name WITH PASSWORD = 'strong\_password';  Quindi, quando connesso a un database utente:  CREATE USER 'user\_name' FOR LOGIN 'login\_name'; | **Quando connesso a un database utente:**  CREATE USER user\_name WITH PASSWORD = 'strong\_password'; |
| **Modello tradizionale** | **Modello di utente di database indipendente** |
| Per cambiare la password, nel contesto del database master:  ALTER LOGIN login\_name WITH PASSWORD = 'strong\_password'; | Per cambiare la password, nel contesto del database utente:  ALTER USER user\_name WITH PASSWORD = 'strong\_password'; |

database SQL

Istanza gestita di SQL di Azure si comporta come SQL Server in locale nel contesto dei database indipendenti. Assicurarsi di modificare il contesto del database dal database master al database utente durante la creazione dell'utente indipendente. Quando si imposta l'opzione di indipendenza, inoltre, non devono essere presenti connessioni attive al database utente.

Osservazioni

In SQL Server gli utenti di database indipendente devono essere abilitati per l'istanza di SQL Server.

Gli account di accesso e gli utenti di database indipendente con nomi diversi possono coesistere nelle applicazioni.

Se nel database master è presente un account di accesso denominato nome1 e si crea un utente di database indipendente denominato nome1, quando viene specificato un nome di database nella stringa di connessione il contesto dell'utente del database verrà preferito a quello dell'account di accesso durante la connessione al database, ovvero gli utenti di database indipendente avranno la precedenza rispetto agli account di accesso con lo stesso nome.

Nel Database SQL il nome dell'utente di database indipendente non può essere uguale a quello dell'account dell'amministratore del server.

L'account dell'amministratore del server Database SQL non può mai essere un utente di database indipendente. L'amministratore del server dispone di autorizzazioni sufficienti per creare e gestire utenti del database indipendente. L'amministratore del server può concedere a utenti di database indipendente autorizzazioni per i database utente.

Dal momento che gli utenti del database indipendente sono entità a livello di database, è necessario creare utenti del database indipendente in ogni database in cui verranno usati. L'identità è confinata al database ed è da ogni punto di vista indipendente rispetto a un utente con lo stesso nome e la stessa password in un altro database nello stesso server.

Usare le stesse password complesse usate in genere per gli account di accesso.