Лабораторная работа № 12

Тема «Авторизация доступа к объектам и операциям (службы Analysis Services)»

Доступ неадминистративных пользователей к кубам, измерениям и моделям интеллектуального анализа данных внутри базы данных Службы Analysis Services предоставляется посредством включения пользователя в одну или несколько ролей базы данных.Администраторы служб Службы Analysis Services создают указанные роли базы данных, предоставляют разрешения на чтение или чтение и запись объектов служб Службы Analysis Services, а затем добавляют к каждой роли пользователей и группы Windows Корпорация Майкрософт.
Службы Службы Analysis Services определяют действительные разрешения для конкретного пользователя или группы Windows, объединяя разрешения, связанные с ролью базы данных, к которой пользователь или группа принадлежит.Как следствие, если одна роль базы данных не предоставляет пользователю или группе разрешения на просмотр измерения, меры или атрибута, но при этом другая роль базы данных предоставляет пользователю или группе такое разрешение, то у пользователя или группы будет разрешение на просмотр объекта.

Важно

Участники роли администратора сервера и участники роли базы данных Службы Analysis Services, обладающие разрешениями «Полный доступ» (администратор), имеют доступ ко всем данным и метаданным в базе данных, и не нуждаются в дополнительных разрешениях на просмотр конкретных объектов.Более того, членам роли сервера служб Службы Analysis Services не может быть отказано в доступе к любому объекту любой базы данных, а членам роли базы данных служб Службы Analysis Services, обладающей разрешениями «Полный доступ» (администратор) в рамках базы данных, не может быть отказано в доступе к любому объекту в рамках такой базы данных. Специальные административные операции, такие как обработка, можно авторизовать с помощью отдельных ролей с меньшими разрешениями.Дополнительные сведения см. в разделе Предоставление разрешений доступа (службы Analysis Services).

Список ролей, заданных для базы данных

Чтобы получить список ролей, заданных на сервере, администраторы могут выполнить простой запрос динамических административных представлений (DMV) в SQL Server Management Studio.

1. В SSMS щелкните правой кнопкой мыши базу данных и выберите команду **Создать запрос** | **Многомерное выражение**.
2. Введите следующий запрос и нажмите клавишу F5, чтобы выполнить его:
3. ```
   Select * from $SYSTEM.DBSCHEMA_CATALOGS
   ```

   В результате запроса будет показано имя базы данных, описание, имя роли и дата последнего изменения.Используя эти сведения в качестве отправной точки, можно переходить к отдельным базам данных и проверять членство и разрешения конкретной роли.
   ```

Организованный сверху вниз обзор авторизации Analysis Services

Этот раздел охватывает базовый рабочий процесс для настройки разрешений.

Шаг 1. Администрирование сервера

В качестве первого шага решите, кто будет обладать правами администратора на уровне сервера.Во время установки локальному администратору, установившему SQL Server, необходимо указать одну или несколько учетных записей Windows от имени администратора сервера служб Analysis Services.Администраторы сервера обладают всеми возможными разрешениями на сервере, включая разрешение на просмотр, изменение и удаление любого объекта на сервере или просмотр связанных данных.После завершения установки администратор сервера может добавить или удалить учетные записи, чтобы изменить членство этой роли.Сведения об этом уровне разрешений см. в разделе Предоставление разрешений администратора сервера (службы Analysis Services).

Шаг 2. Администрирование базы данных

Далее, после создания табличного или многомерного решения оно развертывается на сервере как база данных.Администратор сервера может делегировать задачи администрирования базы данных, определив роль с разрешениями "Полный доступ" для соответствующей базы данных.Участники этой роли могут обработать или запросить объекты в базе данных, а также создать дополнительные роли для доступа к кубам, измерениям и другим объектам в самой базе данных.Подробнее см. в разделе Предоставление разрешений базы данных (службы Analysis Services).

Шаг 3. Разрешение доступа к кубу или модели для запроса и обработки рабочих нагрузок

По умолчанию только администраторы сервера и базы данных имеют доступ к кубам или табличным моделям.Для предоставления этих структур данных другим пользователям организации требуются назначения дополнительных ролей, которые сопоставляют учетные записи пользователя и группы Windows с кубами или моделями, а также с разрешениями, определяющими привилегии **Read**.Дополнительные сведения см. в разделе Предоставление разрешений кубу или модели (службы Analysis Services).

Обработку задач можно изолировать от других административных функций, позволив администраторам сервера и базы данных делегировать эту задачу другим пользователям или настроить автоматическую обработку, указав учетные записи службы, запускающие планирование программного обеспечения.Дополнительные сведения см. в разделе Предоставление разрешений доступа (службы Analysis Services).

> **Примечание**
>
> Пользователям не требуется ни разрешений для реляционных таблиц в базовой реляционной базе данных, из которой службы Службы Analysis Services загружают свои данные, ни разрешений на уровне файла на компьютере, на котором запущен экземпляр служб Службы Analysis Services.

Шаг 4 (необязательно). Разрешение или отклонение доступа к внутренним объектам кубов

Службы Analysis Services предоставляет параметры безопасности для разрешений безопасности на индивидуальных объектах, включая элементы измерения и ячейки в модели данных.Дополнительные сведения см. в разделахПредоставление настраиваемого доступа к данным

измерения (службы Analysis Services) и Предоставление настраиваемого доступа к данным ячейки (службы Analysis Services) .
Также можно изменять разрешения на базе удостоверения пользователя.Это часто называется динамической безопасностью и реализуется с помощью функции UserName (многомерные выражения)

Рекомендации

Для лучшего управления разрешениями рекомендуется использовать подход, аналогичный следующему.

1. Создание ролей по названию функции (например, dbadmin, cubedeveloper, processadmin), чтобы пользователь, управляющий ролями мог сразу понять, что разрешает роль.Как указано ранее, роли можно определить в определении модели, сохранив их в последующих развертываниях решения.
2. Создайте соответствующую группу безопасности Windows в Active Directory и сохраните ее в Active Directory, чтобы гарантировать, что она содержит соответствующие индивидуальные учетные записи.Таким образом, ответственность за членство группы безопасности ляжет на специалистов по безопасности, которые уже имеют опыт в работе со средствами и процессами, использующимися для обслуживания учетной записи в организации.
3. Создайте скрипты в Среда SQL Server Management Studio, чтобы можно было быстро реплицировать назначения ролей при каждом повторном реплицировании модели из файлов источника на сервер.Сведения о быстром создании скрипта см. в разделе Предоставление разрешений кубу или модели (службы Analysis Services).
4. Заключите соглашение об именовании, которое отражает область и членство роли.Имена ролей видны только в средствах конструирования и администрирования, поэтому следует использовать соглашение об именовании, знакомое специалистам по безопасности.Например, **processadmin-windowsgroup1** указывает доступ на чтение и права на обработку для пользователей организации, чьи индивидуальные учетные записи Windows являются членами группы безопасности **windowsgroup1**.
   Включение сведений об учетной записи может помочь отслеживать, какие учетные записи используются в разных ролях.Поскольку роли аддитивны, объединенные роли, связанные с **windowsgroup1**, составляют набор действующих разрешений для пользователей, входящих в эту группу безопасности.
5. Разработчикам кубов потребуются разрешения "Полный доступ" для разрабатываемых моделей и баз данных, но после передачи базы данных на рабочий сервер нужны только разрешения на чтение.Не забывайте разрабатывать определения ролей и назначения для всех сценариев, включая разработку, тестирование и рабочие развертывания.

Использование подобного подхода снижает время обработки определений ролей и членства ролей в модели, а также предоставляет видимость назначений ролей, что упрощает реализацию и поддержание разрешений кубов.

См. также

Предоставление разрешений администратора сервера (службы Analysis Services)
Роли и разрешения (службы Analysis Services)
Методики проверки подлинности, поддерживаемые службами Analysis Services