

Лабораторная работа № 11

Тема «Роли и разрешения (службы Analysis Services)»

В службах Службы Analysis Services действует ролевая модель авторизации, которая предоставляет доступ к операциям, объектам и данным. Все пользователи получают доступ к экземпляру служб Службы Analysis Services или базе данных в контексте некоторой роли.

В качестве системного администратора службы Службы Analysis Services, вы отвечаете за предоставление членства **роли администратора сервера**, которая передает неограниченный доступ к операциям на сервере. Эта роль имеет фиксированные разрешения, и ее нельзя настраивать. По умолчанию члены локальной группы администраторов автоматически являются системными администраторами служб Analysis Services.

Пользователи без прав администратора, которые запрашивают или обрабатывают данные, получают доступ через **роли базы данных**. И системные администраторы и администраторы баз данных могут создавать роли, которые описывают разные уровни доступа в рамках заданной базы данных, а затем назначают членство каждому пользователю, которому необходим доступ. Каждая роль обладает настраиваемым набором разрешений для доступа к объектам и операциям в рамках отдельной базы данных. Разрешения назначаются на уровне базы данных, на уровне внутренних объектов (кубов и измерений, но не перспектив) и на уровне строк.

Распространенной практикой является разделение операций по созданию ролей и назначению членства. Часто разработчик моделей добавляет роли на этапе проектирования. Таким образом, все определения ролей отражаются в файлах проекта, определяющих модели. Членство в ролях обычно определяется позднее, когда база данных переносится в рабочую среду. Обычно членство назначают администраторы базы данных, которые создают скрипты для разработки, тестирования и выполнения в качестве независимой операции.

Вся авторизация выполняется по допустимому удостоверению пользователя Windows. Службы Службы Analysis Services используют для проверки подлинности удостоверений пользователей исключительно проверку подлинности Windows. Службы Analysis Services не предоставляет собственный способ проверки подлинности. Обратитесь к разделу [Методики проверки подлинности, поддерживаемые службами Analysis Services](#).

Важно

Разрешения являются аддитивными для каждого пользователя или группы Windows, по всем ролям базы данных. Если одна роль запрещает пользователю или группе выполнять определенные задачи или просматривать определенные данные, а другая роль предоставляет такое разрешение указанному пользователю или группе, то этому пользователю или группе будет разрешено выполнять упомянутые задачи или просматривать упомянутые данные.

В этом разделе

- [Авторизация доступа к объектам и операциям \(службы Analysis Services\)](#)
- [Предоставление разрешений базы данных \(службы Analysis Services\)](#)
- [Предоставление разрешений кубу или модели \(службы Analysis Services\)](#)
- [Предоставление разрешений доступа \(службы Analysis Services\)](#)

- [Предоставление разрешений на чтение описания метаданным объекта \(службы Analysis Services\)](#)
- [Предоставление разрешений объекту источника данных \(службы Analysis Services\)](#)
- [Предоставление разрешений структурам интеллектуального анализа данных и моделям интеллектуального анализа данных \(службы Analysis Services\)](#)
- [Предоставление разрешений измерению \(службы Analysis Services\)](#)
- [Предоставление настраиваемого доступа к данным измерения \(службы Analysis Services\)](#)
- [Предоставление настраиваемого доступа к данным ячейки \(службы Analysis Services\)](#)

См. также

[Создание ролей и управление ими \(табличные службы SSAS\)](#)