Архитектура системы безопасности SQL Server. Режимы аутентификации. Типы учетных записей, пользователи, роли сервера, роли баз данных.

Система безопасности

Система безопасности SQL Server 2000 базируется на пользователях и учетных записях. Пользователи проходят следующие два этапа проверки системой безопасности. На первом этапе пользователь идентифицируется по имени учетной записи и паролю, то есть проходит аутентификацию. Если данные введены правильно, пользователь подключается к SQL Server. Подключение к SQL Server, или регистрация, не дает автоматического доступа к базам данных. Для каждой базы данных сервера регистрационное имя (или учетная запись — login) должно отображаться в имя пользователя базы данных (user). На втором этапе, на основе прав, выданных пользователю как пользователю базы данных (user), его регистрационное имя (login) получает доступ к соответствующей базе данных. В разных базах данных login одного и того же пользователя может иметь одинаковые или разные имена user с разными правами доступа.

Для доступа приложений к базам данных им также понадобятся права. Чаще всего приложениям выдаются те же права, которые предоставлены пользователям, запускающим эти приложения. Однако для работы некоторых приложений необходимо иметь фиксированный набор прав доступа, не зависящих от прав доступа пользователя. SQL Server 2000 позволяет предоставить такие с применением специальных ролей приложения.

Итак, на уровне сервера система безопасности оперирует следующими понятиями:

1) аутентификация (authentication);

2) учетная запись (login);

3) встроенные роли сервера (fixed server roles).

На уровне базы данных используются следующие понятия: пользователь базы данных (database user); фиксированная роль базы данных (fixed database role); пользовательская роль базы данных (users database role); роль приложения (application role).[11]

Режимы аутентификации

SQL Server 2000 может использовать два режима аутентификации пользователей: режим аутентификации средствами Windows NT/2000 (Windows NT Authentication); смешанный режим аутентификации (Windows NT Authentication and SQL Server Authentication).

Смешанный режим позволяет пользователям регистрироваться как средствами Windows NT, так и средствами SQL Server. Кроме того, этот режим предлагает некоторые удобства по сравнению с первым. В частности, при аутентификации только средствами домена Windows NT, если пользователь не имеет учетной записи в домене Windows NT, то он не сможет получить доступа к серверу баз данных. Смешанный режим аутентификации позволяет избежать этой проблемы.[12]

При выборе режима аутентификации следует исходить как из требований обеспечения наибольшей безопасности, так и из соображений простоты администрирования. Если ваша организация небольшая и должности администратора сети и администратора баз данных совмещает один человек, то удобнее использовать аутентификацию Windows NT. Если же в организации сотни пользователей и функции системного администратора и администратора баз данных выполняют различные люди, то может оказаться, что аутентификация средствами SQL Server удобнее. В противном случае человеку, занимающемуся администрированием сервера баз данных, придется постоянно обращаться к системному администратору для создания нового пользователя, смены пароля или для перевода пользователя из одной группы в другую. К тому же системный администратор будет иметь возможность назначать права доступа по своему усмотрению, а это совсем ни к чему.

С другой стороны, каждый пользователь организации, скорее всего, имеет в домене учетную запись, администрированием которой занимается системный администратор. Благодаря аутентификации Windows NT администратор баз данных может использовать уже готовые учетные записи, а не отвлекаться на создание новых.

Режим аутентификации SQL Server

Для установки соединения с сервером SQL Server 2000, находящемся в домене, с которым не установлены доверительные отношения, можно использовать аутентификацию SQL Server. Аутентификация SQL Server также используется, когда вообще нет возможности зарегистрироваться в домене. Например, при подключении к SQL Server 2000 по Интернету.

При работе с аутентификацией SQL Server доступ также предоставляется на основе учетных записей. Но в этом случае используются учетные записи SQL Server, а не Windows NT.

Для аутентификации средствами SQL Server Server член стандартной роли сервера sysadmin или securityadmin должен создать и сконфигурировать для пользователя учетную запись, в которую входит имя учетной записи, уникальный идентификатор SQL Server и пароль. Вся эта информация будет храниться в системной базе master. Создаваемая учетная запись не имеет отношения к учетным записям Windows NT.

В этом режиме при попытке пользователя получить доступ к SQL Server сервер сам проверяет правильность имени пользователя и пароль, сравнивая их с данными в системных таблицах. Если данные, введенные пользователем, совпадают с данными SQL Server, пользователю разрешается доступ к серверу. В противном случае попытка доступа отклоняется и выдается сообщение об ошибке.

Аутентификация SQL Server может применяться в следующих случаях: для пользователей Novell NetWare, Unix и т. д.; при подключении к SQL Server 2000 через Интернет, когда регистрация в домене не выполняется; под управлением операционной системы Windows 98.

В большинстве случаев учетная запись в SQL Server создается с целью предоставления доступа. Но бывают ситуации, когда необходимо запретить доступ пользователю или группе. Например, при наличии сложной системы безопасности Windows NT доступ обычно предоставляется группе пользователей. Однако если в группе имеется человек, которому нельзя разрешать доступ к SQL Server, его необходимо убрать из этой группы. Но такой подход неудовлетворителен, если группа предназначена не только для объединения пользователей, имеющих доступ к SQL Server, но имеет еще и какие-то

дополнительные функции. SQL Server разрешает создать учетную запись с целью запрещения доступа. Это гарантирует, что пользователь никаким образом не сможет установить соединение с сервером. Создав группу Windows NT и запретив ей доступ к SQL Server, вы можете включать в нее пользователей, которым необходимо отказать в доступе.[13]

Компоненты структуры безопасности

Фундаментом системы безопасности SQL Server 2000 являются учетные записи (login), пользователи (user), роли (role) и группы (group).

Пользователь, подключающийся к SQL Server, должен идентифицировать себя, используя учетную запись. После того как клиент успешно прошел аутентификацию, он получает доступ к SQL Server. Для получения доступа к любой базе данных учетная запись пользователя (login) отображается в пользователя данной базы данных (user). Объект «пользователь базы данных» применяется для предоставления доступа ко всем объектам базы данных: таблицам, представлениям, хранимым процедурам и т. д. В пользователя базы данных может отображаться: учетная запись Windows NT; группа Windows NT; учетная запись SQL Server.

Подобное отображение учетной записи необходимо для каждой базы данных, доступ к которой хочет получить пользователь. Отображения сохраняются в системной таблице sysusers, которая имеется в любой базе данных. Такой подход обеспечивает высокую степень безопасности, предохраняя от предоставления пользователям, получившим доступ к SQL Server, автоматического доступа ко всем базам данных и их объектам. Пользователи баз данных, в свою очередь, могут объединяться в группы и роли для упрощения управлением системой безопасности.

В ситуации, когда учетная запись не отображается в пользователя базы данных, клиент все же может получить доступ к базе данных под гостевым именем guest, если оно, разумеется, имеется в базе данных. Обычно пользователю guest предоставляется минимальный доступ только в режиме чтения. Но в некоторых ситуациях и этот доступ необходимо предотвратить.

Если в сети имеется небольшое количество пользователей, то достаточно легко предоставить доступ каждому пользователю персонально. Однако в больших сетях с сотнями пользователей подобный подход займет много времени. Гораздо более удобным и эффективным является подход, когда доступ к SQL Server 2000 предоставляется целым группам пользователей. Как раз такой подход возможен при аутентификации средствами Windows NT/2000, когда на уровне домена создается несколько групп, каждая из которых предназначена для решения специфических задач. На уровне SQL Server 2000 такой группе разрешается доступ к серверу, предоставляются необходимые права доступа к базам данных и их объектам. Достаточно включить учетную запись Windows NT в одну из групп, и пользователь получит все права доступа, предоставленные этой группе. Более того, одна и та же учетная запись может быть включена во множество групп Windows NT, что даст этой учетной записи возможность пользоваться правами доступа, предоставленными всем этим группам. Администратор SQL Server 2000 должен сам решить, как удобнее предоставлять доступ к серверу: персонально каждой учетной записи или группе в целом.[14]

Пользователи

После того как пользователь прошел аутентификацию и получил идентификатор учетной записи (login ID), он считается зарегистрированным и ему предоставляется доступ к серверу. Для каждой базы данных, к объектам которой пользователю необходимо получить доступ, учетная запись пользователя (login) ассоциируется с пользователем (user) конкретной базы данных. Пользователи выступают в качестве специальных объектов SQL Server, при помощи которых определяются все разрешения доступа и владения объектами в базе данных.

Имя пользователя может использоваться для предоставления доступа как конкретному человеку, так и целой группе людей (в зависимости от типа учетной записи).

При создании базы данных определяются два стандартных пользователя: dbo и guest.Если учетная запись (login) не связывается явно с пользователем (user), последнему предоставляется неявный доступ с использованием гостевого имени guest. То есть все учетные записи, получившие доступ к SQL Server 2000,
автоматически отображаются в пользователей guest во всех базах данных. Если вы удалите из базы данных пользователя guest, то учетные записи, не имеющие явного отображения учетной записи в имя пользователя, не смогут получить доступа к базе данных. Тем не менее, guest не имеет автоматического доступа к объектам. Владелец объекта должен сам решать, разрешать пользователю guest этот доступ или нет. Обычно пользователю guest предоставляется минимальный доступ в режиме «только чтение».

Для обеспечения максимальной безопасности можно удалить пользователя guest из любой базы данных, кроме системных баз данных master и Tempdb. В первой из них guest используется для выполнения системных хранимых процедур обычными пользователями, тогда как во второй позволяет создавать любым пользователям временные объекты.

Владелец базы данных (DataBase Owner, DBO) — специальный пользователь, обладающий максимальными правами в базе данных. Любой член роли sysadmin автоматически отображается в пользователя dbo. Если пользователь, являющийся членом роли sys admin, создает какой-нибудь объект, то владельцем этого объекта назначается не данный пользователь, а dbo. Пользователь, который создает объект в базе данных, например таблицу, хранимую процедуру или представление, становится владельцем объекта. Владелец объекта (database object owner) имеет все права доступа к созданному им объекту. Чтобы пользователь мог создать объект, владелец базы данных (dbo) должен предоставить пользователю соответствующие права. Полное имя создаваемого объекта включает в себя имя создавшего его пользователя

SQL Server позволяет передавать права владения от одного пользователя другому. Чтобы удалить владельца объекта из базы данных, сначала необходимо удалить все объекты, которые он создал, или передать права на их владение другому пользователю.