2011

ЦЕНТРИНФОРМ

CRLS

(Система управления доступом к данным)

Система CRLS предназначена для осуществления политики разграничения доступа к информации на уровне записей и ячеек защищаемых таблиц, хранящихся в базе данных под управлением MS SQL сервера и предоставления удобных средств администрирования настройки доступа

Общее описание системы

Содержание

1 АННОТАЦИЯ

Документ содержит описание требований, предъявляемых к системе разграничения доступа к данным на уровне записей / ячеек и подхода к реализации такой системы.

2 ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

Аутентификация – процедура проверки подлинности данных и субъектов информационного взаимодействия исключительно на основе внутренней структуры самих данных.

БД – база данных.

Доступ – возможность / совершение субъектом операций над объектом.

Защищаемая таблица – таблица, доступ к записям и ячейкам которой разграничивается системой CRLS.

Объект – контейнер информации в системе (в контексте CRLS: таблица, записи таблицы, ячейки таблицы базы данных).

Операция – действие по извлечению, добавлению, изменению, удалению объекта, также возможные / побочные результаты в контексте SQL сервера: блокировки, изоляция и т.д.

ОС – операционная система.

Права доступа – совокупность правил, регламентирующих порядок и условия доступа субъекта к объекту.

Правило – предикат CRLS системы, классифицирующий контекст доступа: объект, субъект, операция.

Предикат – это высказывание, в которое можно подставлять аргументы. Предикат позволяет специфицировать условие, результатом вычисления которого может быть ИСТИНА или ЛОЖЬ.

Представление таблицы – это пустая именованная таблица, определяемая перечнем тех столбцов таблиц и признаками тех их строк, которые хотелось бы в нем увидеть.

Роль – набор привилегий, определяющий право пользователя на то или иное действие по отношению к объекту (понятие из ролевой модели контроля доступа).

СУБД – система управления базами данных.

Субъект – пользователь при работе в системе (далее: пользователь).

Таблица – таблица базы данных СУБД SQL.

ХП – хранимая процедура.

Шифрование данных – процесс преобразования открытых данных в закрытые по определенному алгоритму с использованием секретного ключевого элемента – ключа шифрования.

T-SQL (Transact-SQL) – расширение языка SQL компаний Microsoft (для Microsort SQL Server).

3 ОСНОВНЫЕ СВЕДЕНИЯ

Полное наименование системы: Система управления доступом к данным.

Условное обозначение: CRLS.

Год реализации проекта: 2009 год.

Организация-исполнитель: Федеральное государственное унитарное предприятие «ЦентрИнформ» Федеральной службы по регулированию алкогольного рынка.

4 ВВЕДЕНИЕ

Современные автоматизированные системы обработки данных имеют дело с большими объемами разнообразной информации и рассчитаны на одновременную работу с ними множества пользователей. В связи с этим часто встает проблема управления доступом: предоставление необходимых (разрешенных) данных отдельным пользователям или их группам.

Как правило, это необходимо в тех случаях, когда пользователи какой-либо системы неравноценны по своему статусу или выполняемым функциям и/или хранимая информация является коммерческой тайной и корпоративной политикой безопасности фирмы предусмотрен ряд ограничений на доступ к ней со стороны сотрудников.

Цель управления доступом это ограничение операций, которые может проводить пользователь системы. Управление доступом указывает, что конкретно пользователь имеет право делать с данными, а также поддерживает требуемый уровень конфиденциальности и доступности данных.

5 ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

5.1 Классы решаемых задач

Контроль доступа к информации, базирующийся на правах доступа пользователя, является фундаментальной частью большинства информационных систем и осуществляется на определенном уровне. Например, ОС Windows контролирует доступ к файлам пользователей, но не к их частям. Microsoft SQL, как и большинство реляционных

СУБД, контролирует доступ к таблице в целом, и не предоставляет возможность разграничить доступ на уровне записей таблицы или ячеек.

Часто возникает необходимость осуществлять контроль доступа на достаточно низком (мелком) уровне. Например, список пациентов и их диагнозов может храниться в одном файле или таблице. Каждый врач должен иметь доступ к информации только своих пациентов (разграничение на уровне записей). Сотрудники регистратуры должны иметь доступ к определенной части информации о пациенте (разграничение на уровне ячеек записи).

Похожие требования предъявляются к системам из многих областей, включая финансы, юриспруденцию, государственные и военные системы. Для государственных учреждений и всех российских предприятий, в ведении которых находится обработка персональных данных, выполнение требований такого рода продиктовано принятием Федерального закона «О защите персональных данных».

Типичным подходом реализации таких требований в приложениях, использующих БД, является реализация необходимой логики в коде приложения:

- в n – уровневых системах за реализацию таких требований может, к примеру, отвечать уровень бизнес логики; в двух уровневой системе клиент-серверного приложения за это может отвечать клиентская часть.

Данный подход может быть эффективен в рамках приложения, но сами данные остаются незащищенными.

Другим общеизвестным подходом, устраняющим вышеуказанную проблему, является подход, при котором весь доступ к данным БД осуществляется через хранимые процедуры. Пользователям не предоставляется доступ к таблицам с информацией, а предоставляется доступ на выполнение хранимых процедур, реализующих необходимую логику фильтрации. Данный подход также имеет недостатки. Например, добавление нового пользователя, влекущее за собой изменение логики фильтрации, становится трудновыполнимой задачей.

Необходима система, предоставляющая механизм, автоматически применяющий логику фильтрации на требуемых пользователю данных из таблиц (или представлений). Логика фильтрации должна основываться на контексте (пользователь, данные ….) и позволять управлять доступом к предоставляемым пользователю данным на уровне записей и уровне ячеек таблиц данных.

5.2 Назначение системы

Назначением системы является осуществление любой разумной политики разграничения доступа к информации на уровне записей и ячеек защищаемых таблиц,

хранящихся в базе данных под управлением MS SQL сервера и предоставления удобных средств администрирования настройки доступа.

5.3 Существующие и разрабатываемые аналогичные решения

В версиях СУБД Microsoft SQL Server версий: 2008, 2005, 2000, 7 и ниже, не предоставляется никаких встроенных решений для разграничения доступа к данным на уровнях ниже уровня объектов БД, таких как таблицы/представления.

Для СУБД семейства Oracle, начиная с версии 8.1, появилось расширение FGAC (Fine Grained Access Control – детальный контроль доступа), предоставляющее возможность разграничения доступа и работающее в связке с Secure Application Contexts (контексты защищенных приложений).

В различных изданиях детальный контроль доступа может быть назван по-разному. Ниже перечислены его синонимы:

- детальный контроль доступа (Fine Grained Access Control – техническое наименование);
- виртуальная частная база данных (Virtual Private Database - маркетинговое наименование);
- безопасность на уровне строк (Row Level Security – техническое наименование, базирующееся на PL/SQL-пакетах).

Дальнейшей эволюцией расширения FGAC является Oracle Label Security.

Существует ряд коммерческих продуктов, в той или иной степени удовлетворяющих заявленным выше требованиям. К таким решениям можно отнести Data Security for SQL Server NetLib Encryptionizer for SQL Server и SQL Server 2005 Label Security Toolkit.

Разработанная система управления доступом (CRLS) позволяет реализовывать разграничения доступа к данным на уровнях ниже уровня объектов баз данных (таблицы, представления) для MS SQL Server с помощью специального средства администрирования, независимого от специфики приложений, взаимодействующих с СУБД.

5.4 Основные потребители

Потребителями результатов разработки системы управления доступом к данным являются юридические (физические) лица, использующие в своей деятельности информационные бизнес системы, где хранение и обработка данных реализованы средствами СУБД MS SQL и нуждающиеся в разграничении доступа к информации на уровне ниже уровня таблиц баз данных и ее защите.

Необходимость защиты информации в информационных системах жестко регламентируется законодательством Российской Федерации. В частности, подлежит защите любая информация, служащая для идентификации личности (ФИО, адрес, телефон и т.д.). Кроме того, любая коммерческая информация, разглашение которой нежелательно для нормальной работы организации, тоже должна быть защищена по закону.

6 ОПИСАНИЕ СИСТЕМЫ

6.1 Ограничения предметной области

Подход к реализации механизма контроля доступа на уровне записи и ячейки таблицы, описываемый в данном документе, подразумевает, что приложения, использующие БД, будут осуществлять подключения к БД с помощью соединений, позволяющих однозначно идентифицировать пользователя, от лица которого осуществляется доступ к данным. Это может быть как встроенная Windows аутентификация, так и SQL серверная аутентификация.

Данное допущение нивелирует пользу от работы пула соединений, используемого средними уровнями в многоуровневых архитектурах. Пул позволяет улучшить масштабируемость и повысить производительность. Тем не менее, для систем, требующих разграничения доступа на уровне записей и ячеек, скорее всего, актуально наличие подсистемы аудита, других подсистем безопасности, одним из требований которых является то, что пользователь однозначно идентифицировался на всех уровнях системы, в том числе и на уровне БД. Отказ от использования пула соединений для подобных систем, таким образом, оказывается вынужденной необходимостью.

Реализация подхода подразумевает разграничение доступа на самом нижнем уровне – на уровне БД. На данном уровне это возможно средствами Microsoft SQL Server.

Разграничение доступа к данным производится в рамках таблицы. Разграничение возможно на уровне записи таблицы: RLS – row level security, и на уровне ячейки: CLS – cell level security.

Для интеграции описываемого подхода в n – уровневые системы, а также системы, построенные на основе WEB, где за разграничение доступа к данным отвечает уровень бизнес логики (WEB сервер), а работа с БД ведется с использованием фиксированного соединения (соединение, ведущееся от встроенной учетной записи, представляющей один из уровней архитектуры, в частности для WEB-ориентированных приложений это будет WEB сервер IIS, Apache…), реализован механизм идентификации и последующей имперсонализации (возможность уже аутентифицированного пользователя работать от

имени другого лица) пользователя на уровне БД при использовании фиксированного соединения.

6.2 Требования к системе

Реализованная система управления доступом к данным должна удовлетворять следующим требованиям:

1) Позволять реализовывать любую разумную политику разграничения доступа к данным (записи/ячейки), оставаясь при этом максимально удобной в администрировании;

2) Предоставлять возможность ручного управления доступом на уровне строк (записей) и ячеек таблицы;

3) Иметь возможность автоматически разграничивать доступ к данным в соответствии с предопределяемыми настройками;

4) Поддерживать модель безопасности Microsoft SQL Server;

5) Интегрироваться в приложения, архитектура которых предполагает работу с БД через фиксированное соединение;

6) Удовлетворять требованиям по производительности;

7) Обеспечивать прозрачный доступ средствами, предоставляемыми Microsoft SQL Server, к данным защищенным системой разграничения;

8) Иметь средства администрирования, независимые от специфики приложений, взаимодействующих с БД.

6.3 Принципы функционирования

6.3.1 Уровень разграничения доступа

Минимальным разумным уровнем, на котором необходимо разграничение доступа к данным БД, является ячейка таблицы. Отталкиваясь от этого, можно относительно реляционных СУБД выделить следующие уровни, на которых ведется разграничение доступа:

- сервер СУБД;
- база данных сервера;
- таблица базы;
- запись таблицы;
- ячейка записи.

За разграничение доступа на первых трех уровнях отвечают системы, встроенные в СУБД, и системы разграничения, относящиеся к ОС. Разграничение доступа на

оставшихся уровнях берет на себя система управления доступом к данным (CRLS). Из сказанного следует, что основная работа системы ведется в рамках таблицы.

Разграничение доступа осуществляется на двух уровнях – на уровне записи защищаемой таблицы и на уровне ячейки. На уровне записи разграничение доступа представляет собой разрешение или запрещение выполнения операции. На уровне ячейки определяется доступность данных – содержимого ячейки: доступно / недоступно. Уровень записи и уровень ячейки в контексте разграничения доступа состоят в отношениях вложенности. Разрешения уровня ячейки умножаются (логически) на разрешения записи, в которой находится ячейка.

6.3.2 Место CRLS – системы в инфраструктуре SQL сервера

Основой описываемого решения является изолирование субъекта (пользователя) от прямого доступа к объекту (таблице). Реализуется это посредством установки запрета на прямой доступ субъекта к объекту (полный запрет доступа) и созданием отображения (представления, полностью повторяющего структуру таблицы, в том числе значения по умолчанию, вычисляемые поля и т.д.), через которое субъект может осуществить доступ к объектам. Таким образом, объект – таблица становится таблицей, защищаемой системой CRLS.

За разграничение доступа, посредством созданного представления, отвечает инфраструктура системы CRLS, основная часть которой располагается на уровне базы данных. Инфраструктура, располагающаяся на уровне сервера, отвечает за создание контекста безопасности и поддержку архитектур с фиксированным подключением [выполнение треб. 5]. Схематично, взаимодействие CRLS – системы с MS SQL представлено на рис. 1.

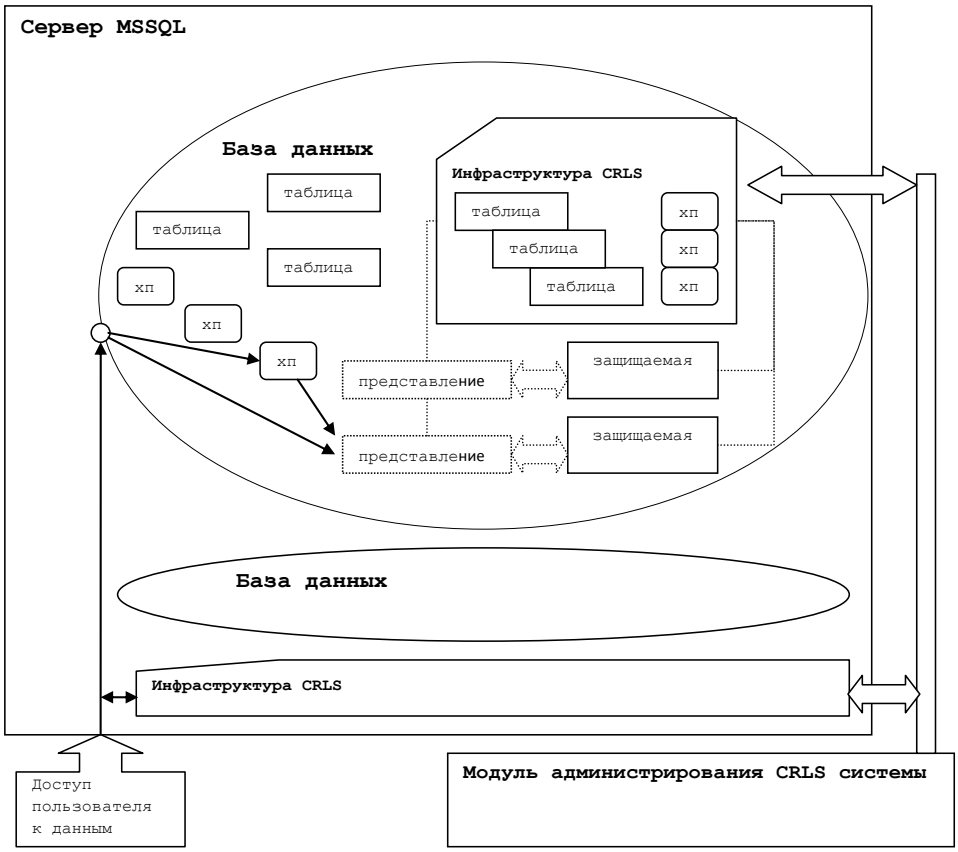

Рисунок 1 - Взаимодействие CRLS – системы с MS SQL

Работа с представлением, созданным системой CRLS для отображения данных защищаемой таблицы, ничем не отличается от работы со стандартным представлением. Из сказанного следует, что все ограничения, накладываемые системой CRLS в противовес прямому доступу, соответствуют ограничениям, накладываемым при работе со стандартным представлением. В частности, таким ограничением является отсутствие поддержки некоторых конструкций запросов проприетарного языка T-SQL. Стандарт ANSI SQL, по заявлениям разработчиков поддерживается полностью.

В целом, работа CRLS системы по разграничению до ступа (запросы, выполнение ХП и т.д.) к данным защищаемых таблиц прозрачна для потребителя (пользователя или приложения) [выполнение треб. 7].

6.3.3 Доступ к конкретному объекту (ручной режим).

Система CRLS, как и большинство систем разграничения доступа, позволяет ответственному лицу (далее администратору безопасности) вручную задать разрешения на доступ к конкретному объекту: запись, ячейка. Осуществляется это посредством назначения для конкретных субъектов (пользователь, роль, представляющая группу входящих в нее пользователей) разрешений на выполнение операций над конкретным объектом (запись, ячейка) [выполнение треб. 2].

Данный режим работы системы не является основным. Обуславливается это спецификой БД: большое количество объектов разграничения доступа в рамках одной таблицы, отсутствие какой-либо иерархии объектов разграничения (например, иерархия каталогов файловой системы). В виду этого не представляется разумным осуществление разграничения доступа посредством ручного назначения разрешений для конкретных объектов.

6.3.4 Доступ к группе объектов (автоматический режим). Классификация контекста доступа при помощи правил

Основным режимом работы системы является режим, при котором разграничение доступа производится системой CRLS автоматически [выполнение треб. 3]. Достигается данная возможность благодаря использованию системы правил. Правила представляют собой условие, формируемое, ответственным за разграничение доступа лицом, с помощью модуля администрирования системы CRLS. Основная задача правил классифицировать контекст, при котором осуществляется доступ.

С помощью правил можно классифицировать:

- операцию: выборка, добавление, удаление, изменение;
- объект: запись, ячейку, удовлетворяющую необходимым условиям;
- субъект: пользователь, пользователь входящий в роль, и т.д;
- и их комбинации.

Правила позволяют увеличить масштаб, при котором администратору необходимо осуществить настройку разграничения доступа. Разграничение доступа сводится не к ручной привязке разрешений к конкретным объектам, а к привязке разрешений к правилам, классифицирующим контекст доступа, согласно требованиям безопасности. Система CRLS автоматически применяет правила и вычисляет разрешения в момент работы (доступа) с данными защищаемой таблицы.

Также реализована возможность настройки автоматического задания разрешений для ситуаций доступа, неклассифицированных правилами, так называемая политика по умолчанию.

Разрешение, привязываемое к правилам для разграничения на уровне записи, представляет собой сочетание трех величин:

- роль (пользователь);
- операция;
- разрешено/запрещено.

Для уровня ячейки соответственно сочетание:

- роль (польз.);

- разрешено/запрещено.

6.3.5 Ролевая политика

Относительно ролей, в системе CRLS поддерживается построение иерархии и включение в нее пользователей. Также реализована поддержка пользователей, ролей и иерархии ролей, определенных в рамках БД SQL сервера [выполнение треб. 4]. Далее, как оговаривалось ранее, система CRLS имеет возможность однозначно идентифицировать пользователя, от лица которого осуществляется доступ к данным. На основании идентифицированного пользователя, система вычисляет набор ролей (эффективные роли), в которые прямо или косвенно (через наследование ролей в иерархии) входит пользователь.

Учитывая необходимые для решения конкретной прикладной бизнес задачи требования, можно построить иерархию ролей, на основании которой станет возможно произвести требуемое разграничение доступа.

6.3.6 Средство администрирования системы CRLS

Для настройки механизмов системы CRLS и окружения, при осуществлении требуемой политики разграничения доступа, важным является наличие удобного средства администрирования. Разработанный для системы CRLS модуль администрирования позволяет провести необходимые действия для реализации целостной защиты данных [выполнение треб. 8]. К таким действиям относятся:

- создание, редактирование правил, в том числе правил с неограниченной вложенностью условий;
- назначение разрешений, привязываемых к правилам;
- создание ролей, иерархии, пользователей;
- интеграция существующей на SQL сервере модели безопасности в систему CRLS;
- перевод предметных таблиц БД в состояние защищаемых и обратно;
- настройка политик, применяемых по умолчанию;
- поддержка инфраструктуры шифрования данных;
- применение шаблонов настроек безопасности к объектам БД сервера задействованных в разграничении доступа.

7 ВЫВОДЫ

В настоящее время организации большую часть своих информационных ресурсов хранят в базах данных (БД), доступ к которым, как правило, имеют различные категории пользователей. Количество и роли пользователей постоянно меняются, и все более актуальной становится проблема обеспечения информационной безопасности многопользовательских БД.

Взаимодействие пользователей и приложений с БД осуществляется под контролем системы управления базами данных (СУБД). СУБД стали доминирующим инструментом хранения больших массивов разнообразной информации. Большинство известных корпоративных СУБД соответствуют классу безопасности, который требует управления доступом именованных пользователей к именованным объектам. Это требование частично обеспечивает стандарт SQL, который эти СУБД поддерживают.

Язык SQL включает средства управления доступом к данным, но в рамках этого стандарта, разграничение доступа к поименованным информационным объектам БД (таблицам, представлениям, процедурам и т. п.) ограничивается полным набором данных, предоставляемым тем или иным объектом, тогда как существуют задачи, требующие более детального управления доступом.

Разработанная система управления доступом к данным (CRLS) решает проблему детального доступа до уровня записей / ячеек и разработана для работы совместно с MS SQL Server. Модуль администрирования, предоставляет удобные средства по управлению доступом к информации. Настроив окружение и систему CRLS, можно получить целостное решение, удовлетворяющее политике доступа согласно любым правилам корпорации и учитывающее сложные взаимосвязи между объектами и субъектами системы.

Данные полей, содержащих конфиденциальную информацию, шифруются, что позволяет избежать компрометации данных путем создания резервной копии БД.

Система CRLS, в момент осуществления доступа, получает все необходимые знания для выполнения разграничения. Такими знаниями являются:

- разрешения, вычисленные в результате применения правил;
- текущая операция;
- субъект, осуществляющий доступ (пользователь и его эффективные роли).

На основании этих знаний система однозначно определяет: разрешено ли субъекту осуществить запрашиваемую операцию над объектом.

Данный механизм позволяет администратору осуществить любую разумную политику разграничения доступа к данным (записи/ячейки) [выполнение треб. 1].

8 МЕТОДЫ И СРЕДСТВА РАЗРАБОТКИ

Система состоит из двух частей:

- серверной, которая отвечает за разграничение доступа;
- клиентской, предназначенной для настройки и администрирования серверной части.

Серверная часть системы реализована средствами MS SQL Server с использованием языка Transact-SQL.

Основным средством реализации клиентской части системы CRLS является продукт MS Visual Studio, который представляет собой интегрированную среду разработки, программного обеспечения.

К основным технологиям, используемым в процессе разработки системы, относятся следующие:

- ASP.net 2.0 – единая модель для разработки веб-приложений с применением минимума кода, которая содержит службы, необходимые для построения WEB-приложений. ASP.NET является частью платформы .NET Framework;
- WCSF – структурированный набор программных артефактов для разработки WEB – приложений, устанавливаемый в среду разработки.

При создании клиентской части был использован язык программирования C#.