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

Описание контрольного примера

Содержание

1 АННОТАЦИЯ

В настоящем документе представлено описание контрольного примера для системы разграничения доступа к данным на уровне записей / ячеек (CRLS).

В документе описаны исходные требования, которым должно удовлетворять разграничение доступа для выбранной предметной области, построенная для реализации примера иерархия ролей и система правил.

Документ включает одно приложение: «Список терминов и сокращенных наименований».

2 НАЗНАЧЕНИЕ

Назначением системы является осуществление 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. Как было указано в документе «Общее описание системы» реализованная система управления доступом к данным должна удовлетворять следующим требованиям:

- позволять реализовывать любую разумную политику разграничения доступа к данным (записи/ячейки), оставаясь при этом максимально удобной в администрировании;
- предоставлять возможность ручного управления доступом на уровне строк (записей) и ячеек таблицы;
- иметь возможность автоматически разграничивать доступ к данным в соответствии с предопределяемыми настройками;
- поддерживать модель безопасности Microsoft SQL Server;
- интегрироваться в приложения, архитектура которых предполагает работу с БД через фиксированное соединение;
- удовлетворять требованиям по производительности;
- обеспечивать прозрачный доступ средствами, предоставляемыми Microsoft SQL Server, к данным защищенным системой разграничения;

иметь средства администрирования, независимые от специфики приложений, взаимодействующих с БД.

3 ИСХОДНЫЕ ДАННЫЕ

3.1 Предметная область

Одной из областей применения системы CRLS является защита персональных данных граждан. Типичным примером информационной системы, нуждающейся в разграничении доступа к персональным данным, может стать система, обеспечивающая учет и регистрацию граждан в рамках территориального объединения.

В рассматриваемом примере общую организационную структуру можно представить двумя уровнями:

1) Район.

2) Город.

На уровне района действует организация (подобие паспортного стола) занимающаяся учетом населения. Основными задачами организации является первичный учет (ввод данных, присвоение идентификаторов) и выдача справок по запросу.

На уровне города оперируют субъекты, контролирующие организации уровня района, а также субъекты, имеющие доступ к банку данных (военкомат, МВД).

Данные для всех субъектов доступны в единой БД, расположенной на городском сервере.

За основу учета, для упрощения примера, можно взять банк данных, представленный таблицами БД, приведенных на рис. 1, где:

- таблица regions хранит справочную информацию о районах города;
- таблица citizens хранит информацию о гражданах, прошедших первичный учет в районных организациях.

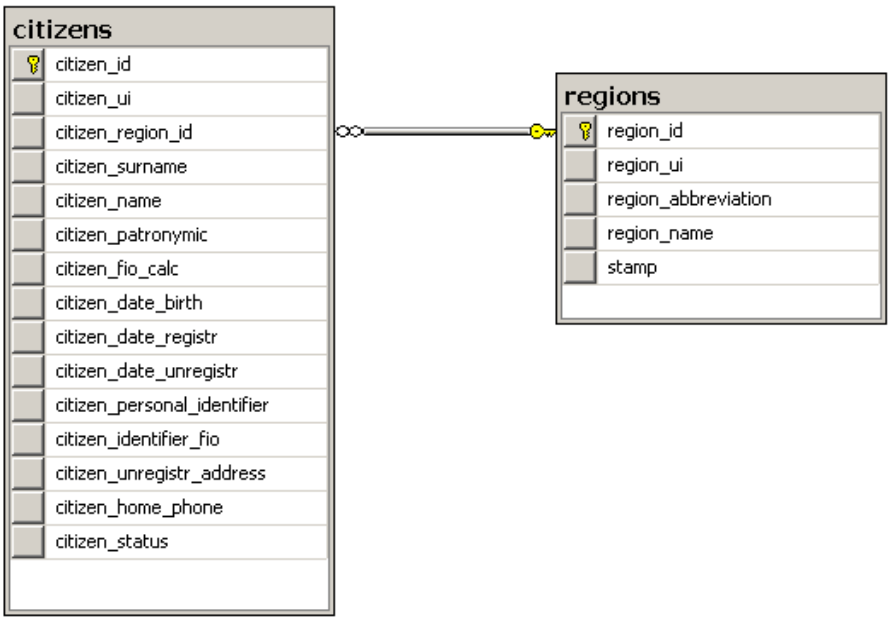

Рисунок 1 - Таблицы БД рассматриваемого примера

Поля таблицы citizens приведены в Таблице 1.

Поле	Описание	Примечание
citizen_id	первичный ключ	identity
citizen_ui	идентификатор	guid
citizen_region_id	район	foreign key
citizen_surname	фамилия	
citizen_name	имя	
citizen_patronymic	отчество	
citizen_fio_calc	ФИО	калькулируемое
citizen_date_birth	дата рождения	
citizen_date_registr	дата регистрации	
citizen_date_unregistr	дата выписки	
citizen_personal_identifier	персональный идентификатор	*
citizen_identifier_fio	ФИО в привязке к ид	*
citizen_unregistr_address	адрес выписки	*
citizen_home_phone	телефон	*
citizen_status	статус	default(1)

Таблица 1

Поля, помеченные звездочкой (далее CLS поля), содержат конфиденциальную информацию, либо информацию, изменение которой доступно только ответственным лицам.

Данные таблицы citizens подлежат разграничению доступа.

3.2 Постановка задачи

Описав предметную область, сформулируем требования, которым должно удовлетворять разграничение доступа нашего примера.

3.2.1 **Уровень района:**

1) Прием документов от населения и ввод первичной информации производят *операторы* (1..N). Разграничение доступа по операциям к записям защищаемой таблицы можно представить следующим списком:
   - выбор (select) только записей введенных пользователем;
   - добавление (insert) только записей района, находящегося в ведении организации;
   - обновление (update) только записей введенных пользователем;

   удаление (delete) запрещено.

Разграничение доступа на уровне ячеек определяется доступностью полей: CLS поля не доступны.

2) Обработка введенных операторами данных (присвоение уникального идентификатора) и выдача справок населению ведется *регистраторами* (1..N). Разграничение доступа на уровне записей:
   - выбор (select) записей района, находящегося в ведении организации;
   - добавление (insert) не предполагается;
   - обновление (update) записей района, находящегося в ведении организации;
   - удаление (delete) запрещено.

   Разграничение доступа на уровне ячеек: доступны CLS поля:
   - citizen_identifier_fio;
   - citizen_personal_identifier;
   - citizen_home_phone.

   В момент присвоения citizen_personal_identifier заполняется защищенное поле citizen_identifier_fio.
3) Контроль работы организации и выписку граждан осуществляет *начальник* (1..1). Разграничение доступа на уровне записей:
   - выбор (select) записей района;
   - добавление (insert) не предполагается;
   - обновление (update) записей района, находящегося в ведении организации;
   - удаление (delete) записей района, находящегося в ведении организации.

   Разграничение доступа на уровне ячеек: доступны CLS поля:
   - citizen_unregistr_address;
   - citizen_home_phone.

3.2.2 **Уровень города:**

1) За контроль работы районных организаций и организацию межрайонного взаимодействия отвечают сотрудники контролирующей организации (1..N). Разграничение доступа определяется наследованием прав всех районных начальников.
2) Сотрудники других ведомств, таких как МВД, Военкоматы и пр., также должны иметь ограниченный доступ к банку данных.

   Разграничение доступа на уровне записей:
   - выбор (select) всех записей банка с присвоенным citizen_personal_identifier;

   добавление (insert) запрещено;
   - обновление (update) запрещено;

- удаление (delete) запрещено.

3) удаление (delete) записей района, находящегося в ведении организации.

Разграничение доступа на уровне ячеек: доступны CLS поля:

- citizen_personal_identifier.

4 РЕАЛИЗАЦИЯ ТРЕБОВАНИЙ РАЗГРАНИЧЕНИЯ ДОСТУПА

4.1 Ограничения контрольного примера

Для упрощения примера будем считать, что:

1) Город разделен на три района. Районы будем обозначать цифрами 1, 2, 3;
2) В каждом районе действует по организации, в ведении которой находится первичный учет граждан соответствующего района;
3) Управление каждой районной организацией поручено начальнику, первичным учетом занимаются операторы, обработкой занимаются регистраторы;
4) На уровне города работают сотрудники контролирующей организации и сотрудники организаций, допущенных к банку данных.

4.2 Построение иерархии ролей

Учитывая сформулированные в постановке задачи требования, можно построить иерархию ролей, на основании которой станет возможно произвести требуемое разграничение доступа. Роли и отношения между ними представлены схемой, изображенной на рис. 2:

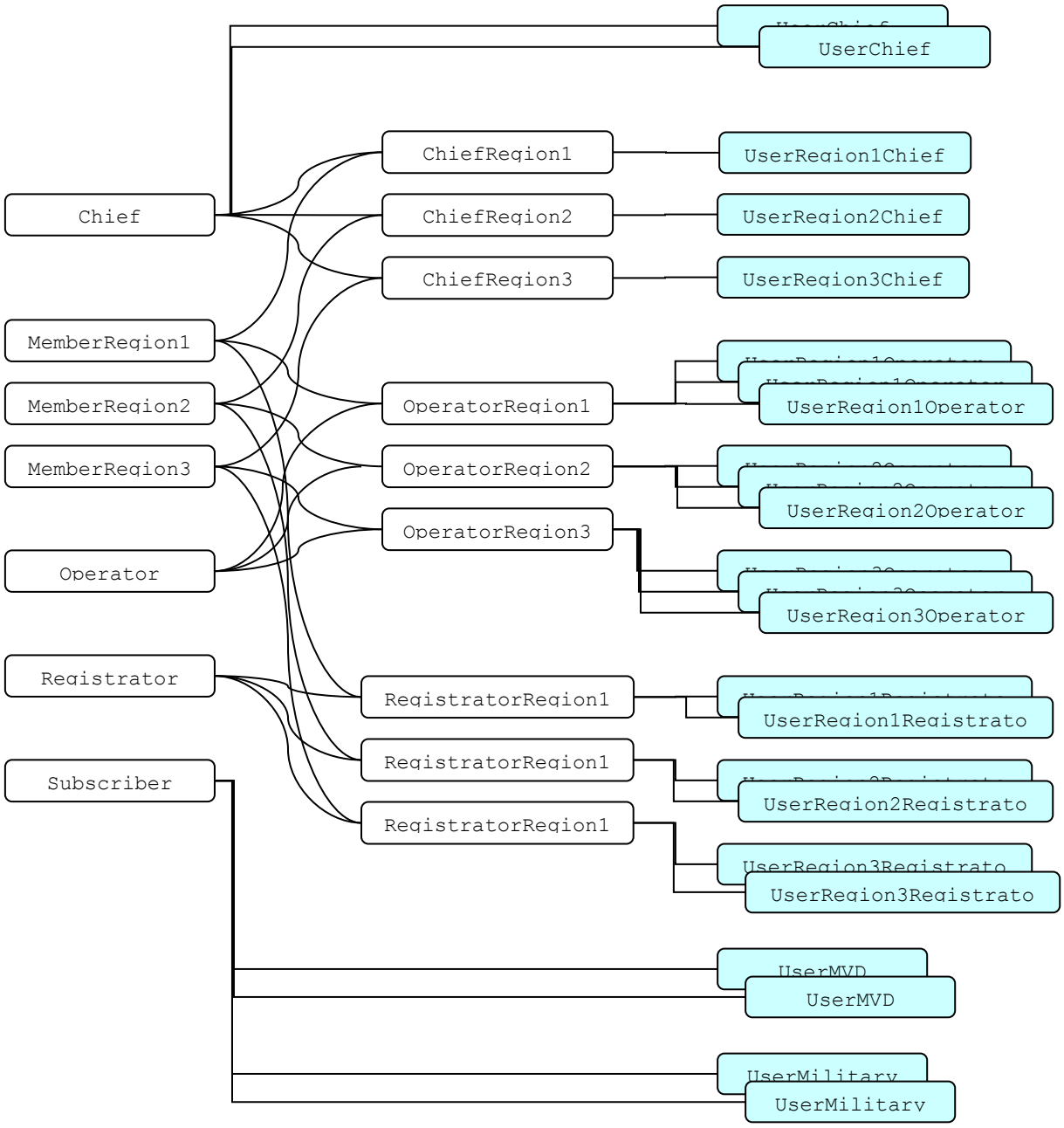

Рисунок 2 - Ролевая модель задачи контрольного примера

На представленной схеме, в двух колонках слева располагаются условные обозначения ролей, правый столбец содержит условные обозначения пользователей.

Иерархия на схеме организована таким образом, что сущности находящиеся правее, являются членами сущностей (входят, наследуют разрешения), расположенных левее, с которыми они на схеме соединены линиями.

Среди ролей верхнего уровня (столбец слева) можно выделить две группы: по выполняемым функциям (Chief, Operator, Registator, Subscriber) и по принадлежности к конкретному району (MemberRegion 1, 2, 3).

4.3 Правила и разрешения

Учитывая построенную иерархию ролей и требования, описанные в постановке задачи, формулируем правила, к которым привязываем соответствующие разрешения для осуществления необходимого разграничения доступа. Полученный результат приведен в Таблице 2.

№ п/п	Тип правила	CLS поле	Условие	Привязываемые разрешения							
				Chief	MemberRegion1	MemberRegion2	MemberRegion3	Operator	Registrator	Subscriber	OWNER *
1	RLS		(isNotRoleMember(Subscriber))	D-p, U-p				S-d, D-d	D-d, U-p	S-p,	D-d
2			(citizen_region_id <> 1)		I-d, D-d, U-d						
3			(citizen_region_id <> 2)			I-d, D-d, U-d					
4			(citizen_region_id <> 3)				I-d, D-d, U-d				
5			(citizen_personal_identifier is null)							S-d	
6			(isRoleMember(Subscriber))							I-d	
7			(citizen_region_id = 1		S-p						
8			citizen_region_id = 2			S-p					
9			citizen_region_id = 3				S-p				
10			((citizen_region_id = 1) or (citizen_region_id = 2) or (citizen_region_id = 3))	S-p							
11	CLS	citizen_unregistr_address	(isRoleMember(Chief) or isRoleMember(Registrator) or isRoleMember(Operator))	p				d	d	d	
12		citizen_identifier_fio	(isRoleMember(Chief) or isRoleMember(Registrator) or isRoleMember(Operator))					d	p	d	
13		citizen_home_phone	(isRoleMember(Chief) or isRoleMember(Registrator))	p				d	p	d	
14		citizen_personal_identifier	(isRoleMember(Chief) or isRoleMember(Registrator) or isRoleMember(Operator))					d	p	d	

S - Select; I - Insert; U - Update; D - Delete; p - permit; d - deny.

Таблица 2

* Роль OWNER - встроенная роль системы CRLS. Назначая разрешения на эту роль, можно управлять политикой разграничения доступа субъектов к объектам, владельцами которых они являются. Понятие владельца в рамках системы CRLS несет тот же смысл, что и понятие владельца в системах разграничения доступа к файлам и каталогам. Разрешения, назначенные на роль OWNER, имеют более низкий приоритет по отношению к разрешениям, назначенным на эффективные роли.

5 ИТОГИ

Пример был полностью реализован на тестовой БД.

Для функционирования системы был использован следующий состав технических средств:

- сервер, где был установлен SQL-сервер и база данных;
- WEB-сервер (может быть совмещен с SQL-сервером);
- браузер Internet Explorer.

Была проведена проверка системы на предмет удовлетворения заявленным требованиям разграничения данных, целостности, возможности внесения изменений в политику разграничения данных, удовлетворения условиям прозрачности и совместимости.

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

Также производилось тестирование производительности на больших объемах данных (более 1000000 записей). Все проверки и тесты система прошла успешно.

Как видно из рассматриваемого примера, система управления доступа к данным оперирует тремя группами объектов: ролями, правилами и разрешениями.

Внутри каждой группы можно настраивать объекты под требования предметной области, в зависимости от бизнес-логики, реализуемых функций и требований к безопасности информации.

Рассмотренный в документе пример может быть реализован другим набором правил, интерпретацией ролей и назначенными разрешениями.

Такая система значительно расширяет возможности по управлению доступом к данным, обеспечивая гибкость настройки прав для разных пользователей к хранимым данным.

6 СПИСОК ТЕРМИНОВ И СОКРАЩЁННЫХ НАИМЕНОВАНИЙ

Сокращение, термин	Полное наименование, определение
СУБД	Система управления базами данных
БД	База данных
MS SQL Server	СУБД, разработанная корпорацией Microsoft
Таблица	Таблица базы данных СУБД SQL
Субъект	Пользователь при работе в системе (далее: пользователь)
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.
Доступ	Возможность / совершение субъектом операций над объектом
Права доступа	Совокупность правил, регламентирующих порядок и условия доступа субъекта к объекту
Роль	Набор привилегий, определяющий право пользователя на то или иное действие по отношению к объекту (понятие из ролевой модели контроля доступа)
Предикат	Высказывание, в которое можно подставлять аргументы. Предикат позволяет специфицировать условие, результатом вычисления которого может быть ИСТИНА или ЛОЖЬ
Правило	Предикат CRLS системы, классифицирующий контекст доступа: объект, субъект, операция
Шифрование данных	процесс преобразования открытых данных в закрытые по определенному алгоритму с использованием секретного ключевого элемента – ключа шифрования