Политика доступа на основе RLS. Мандатный доступ.

Мандатное управление доступом (англ. *Mandatory access control, MAC*) — разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности. Также иногда переводится как **Принудительный контроль доступа**. Это способ, сочетающий защиту и ограничение прав, применяемый по отношению к компьютерным процессам, данным и системным устройствам и предназначенный для предотвращения их нежелательного использования. Контроль доступа осуществляется в зависимости от уровней безопасности взаимодействующих сторон на основании двух правил:

1. No read up (NRU) – нет чтения вверх: субъект имеет право читать только те документы, уровень безопасности которых не превышает его собственный уровень безопасности.

2. No write down (NWD) – нет записи вниз: субъект имеет право заносить информацию только в те документы, уровень безопасности которых не ниже его собственного уровня безопасности.

Первое правило обеспечивает защиту информации, обрабатываемой более доверенными (высокоуровневыми) лицами, от доступа со стороны менее доверенных (низкоуровневых). Второе правило предотвращает утечку информации (сознательную или несознательную) от высокоуровневых участников процесса обработки информации к низкоуровневым.

Безопасность на уровне строк (RLS) позволяет использовать членство в группе или контекст выполнения для управления доступом к строкам в таблице базы данных.

Система базы данных применяет ограничения доступа каждый раз при попытке доступа к данным с любого уровня.

RLS реализуется с помощью инструкции Transact-SQL CREATE SECURITY POLICY и предикатов, созданных как встроенные функции с табличным значением

Уровень А

Для пользователя, который регистрируется в MS SQL Server указывается уровень допуска. Каждая строка таблицы имеет метку безопасности.

Под меткой безопасности, понимается та часть информации, которая описывает «чувствительность» элемента данных (строки). Строка маркируется меткой, описывающей уровни допуска, классифицируемые по одному или нескольким признакам. Пользователи (субъекты) имеют разрешения, описанные с теми же метками. Разрешения каждого субъекта могут рассматриваться в качестве собственных меток. Метка субъекта сравнивается с меткой строки для определения возможности доступа к этой строке.

Привязка метки безопасности к пользователю определяет, к каким строкам таблицы он может получить доступ.

Таблица 1

ID	Name	Classification
1	Ivan Ivanov	SECRET
2	Peter Petrov	TOP SECRET
3	Michael Sidorov	UNCLASSIFIED

Также в базе данных может храниться информация о пользователях (табл. 2):

Таблица 2

User	Clearance
Anna	SECRET
Alex	UNCLASSIFIED (no clearance)

Оба пользователя, Anna и Alex, могут выполнить запрос на выборку вида SELECT * FROM <tablename> к таблице данных (табл. 1), но результаты данного запроса выглядят неодинаково. Пользователь Anna получает набор данных, представленный в табл. 3, пользователь Alex - представленный в табл. 4.

Таблица 3

ID	Name	Classification
1	Ivan Ivanov	SECRET
3	Michael Sidorov	UNCLASSIFIED

Таблица 4

ID	Name	Classification
3	Michael Sidorov	UNCLASSIFIED

Для настройки безопасности необходимо завести вспомогательные таблицы для хранения информации о метках доступа и их приоритетах.

Реализовать данную политику в MS SQL Server.

Уровень B

В дополнении к заданию уровня A реализовать следующие ограничения:

1. Если субъекту требуется внести информацию в объект с более низким, чем у субъекта, уровнем безопасности (что запрещено правилом NWD), то субъект может подать команду это сделать, но в результате

выполнения этой операции уровень безопасности объекта автоматически повышается до уровня безопасности субъекта в системе.
2. Субъекты могут являться членами групп (одна или несколько) (роль в MS SQL Server) И уровни доступа назначаются ролям. Уровень доступа субъекта – максимум из возможных

Уровень С

Реализовать доступ согласно заданию из файла Домашнее задание.pdf