АДМИНИСТРИРОВАНИЕ И МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ SQL AZURE

Скляренко С.Е., Быков П.И.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина 14, каф. Телекоммуникационных систем, тел. (057) 702-55-92
E-mail: discoveryid@gmail.com ; тел. +38(093) 8 121 77 5

Every day we have to increasingly deal with concepts such as cloud technology, computing power, as well as data centers.SQL Azure is a powerful storage infrastructure, data management and analysis. The work is based on SQL Azure component Cloud Fabric, which in turn controls the database instance and ensures their deployment, administration, updating, monitoring and supporting the entire lifecycle of the data. Users are provided with only such tasks as creating a scheme and its maintenance, query optimization, and security management. Understanding of administration and security arrangements SQL Server, is one of the most important and pressing issues in information technology. In this regard, this report focuses on the study of these issues.

С каждым днем нам приходиться все чаще сталкиваться с такими понятиями как облачные технологии, вычислительные мощности, а так же центры хранения данных. SQL Azure является мощной инфраструктурой хранения, управления и анализа данных. Работа SQL Azure базируется на компоненте Cloud Fabric, который в свою очередь управляет экземплярами базы данных и обеспечивает их развертывание, администрирование, обновление, мониторинг и поддерживает весь жизненный цикл работы с данными. Пользователям предоставляется лишь выполнение таких задач, как создание схемы и ее поддержание, оптимизация запросов и управление безопасностью. Понимание вопросов администрирования и механизмов обеспечения безопасности SQL Server, является одним из важнейших и актуальных вопросов в информационных технологиях. В связи с этим, данный доклад посвящен изучению этих вопросов.

SQL Azure является службой реляционных баз данных на платформе Windows Azure. Преимущества использования базы данных SQL Azure включают управляемость, высокий уровень доступности, масштабируемости, хранения, а так же управления и анализа данных.

База данных SQL Azure размещается на серверах, реализующих технологии SQL Server в центрах обработки данных Microsoft. С точки зрения архитектуры существует четыре разных уровня абстракции, которые работают совместно и обеспечивают реляционную базу данных, которой пользуются создаваемые приложения: уровень клиента, уровень служб, уровень платформы и уровень инфраструктуры.

В ходе анализа SQL Azure было показано, что при обеспечении безопасности баз данных SQL Azure необходимо рассматривать следующие вопросы:

- Брандмауэр;
- Шифрование и проверка сертификатов;
- Проверка подлинности;
- Имена входа и пользователи.

Первоначально весь доступ к серверам SQL Azure блокирован брандмауэром SQL Azure, попытки соединения с сервером SQL Azure, исходящие из Интернета или Windows Azure, будут неудачными. Чтобы начать использование сервера SQL Azure, необходимо подключиться к порталу управления и указать один или несколько параметров брандмауэра, разрешающих доступ к серверу SQL Azure. С помощью параметров брандмауэра указать область разрешенных IP-адресов из Интернета, а также то, разрешаются ли приложениям Windows Azure попытки подключения к серверу SQL Azure. Это можно осуществить с использованием портала управления платформой Windows Azure или программным путем с использованием средств «Операции с правилами брандмауэра», до-

ступ к которым предоставляет API REST управления базами данных API сервера SQL Azure. Кроме того, после организации доступа можно использовать базу данных **master** для просмотра и изменения настроек брандмауэра программным путем. Также, стоит отметить, что доступ к службе баз данных SQL Azure предоставляется только через порт 1433 протокола TCP. Для обеспечения доступа к базе данных SQL Azure следует убедиться в том, что применяемый брандмауэр разрешает исходящие соединения через порт 1433 протокола TCP.

Когда компьютер пытается подключиться к серверу SQL Azure из Интернета, брандмауэр SQL Azure проверяет исходный IP-адрес запроса, сравнивая его с полным набором параметров брандмауэра. Если IP-адрес запроса не принадлежит ни к одному из указанных диапазонов, попытка соединения блокируется и не достигает сервера SQL Azure.

Если приложение пытается выполнить подключение к серверу SQL Azure из Windows Azure, брандмауэр SQL Azure отыскивает определенный параметр брандмауэра, указывающий, разрешены ли соединения с Windows Azure.

Параметр брандмауэра с начальным и конечным адресом, равным 0.0.0.0, указывает, что соединения с Windows Azure разрешены. Если IP-адрес запроса не находится в пределах одного из указанных диапазонов, попытка соединения блокируется и не достигает сервера SQL Azure.

База данных SQL Azure обеспечивает полноценное многопользовательское обслуживание баз данных на основе общих источников.

Чтобы обеспечивались хорошие условия работы для всех клиентов базы данных SQL Azure, предложено соединение клиента со службой закрыть при возникновении следующих условий:

- Чрезмерное использование ресурсов;
- Соединения, неактивные в течение 30 минут и более;
- Отработка отказа в результате сбоя сервера.

Весь обмен данными между База данных SQL Azure и конкретным приложением (SSL) требует постоянного шифрования. SQL Azure не поддерживает незашифрованные подключения и имеет подписанный сертификат, выпущенный центром сертификации. Эти факторы также помогают обеспечить защиту передачи данных и предотвратить сетевые атаки с посредником (man-in-the-middle attacks).

Подтверждение шифрования происходит в потоке PRELOGIN протокола TDS. Это требуется для всей клиентский связи с SQL Azure, включая SQL Server Management Studio и приложения через ADO.NET.

Для обеспечения проверки сертификатов с помощью прикладного кода или специальных инструментов следует запрашивать зашифрованное соединение и не доверять сертификатам сервера. Если прикладной код или специальные инструменты не запрашивают зашифрованное соединение, то все равно получают зашифрованные соединения. Но эти программные средства могут не проверять сертификаты сервера, поэтому становятся восприимчивыми к атакам путем перехвата сообщений.

При соединении с базой данных в SQL Azure с помощью приложения ADO.NET следует учитывать следующие аспекты:

- Предотвращать атаки по принципу внедрения кода с применением класса Sql Connection String Builder. Он предоставляется в составе платформы .NET Framework в целях упрощения создания строки подключения;
- Тщательно защищать применяемую строку подключения. Строка подключения становится источником потенциальной уязвимости, если она не защищена;
- В целях полной защиты применяемого соединения, особенно при подключении к SQL Azure по Интернету, обязательно задать параметры соединения Encrypt и TrustServerCertificate платформы ADO.NET. Задать значение свойства соединения Encrypt, равное True (Encrypt = True), и значение свойства соединения

TrustServerCertificate, равное False (TrustServerCertificate = False). Это позволяет создать зашифрованное соединение и сделать невозможными какие-либо атаки путем перехвата сообщений.

Среда SQL Server Management Studio также поддерживает проверку сертификатов. В диалоговом окне «**Подключение к серверу**» следует выбрать параметр «**Шифровать соединение**» во вкладке «**Свойства**».

База данных SQL Azure поддерживает только проверку подлинности SQL Server. Проверка подлинности Windows (с помощью встроенных средств защиты) не поддерживается. Пользователи должны предоставлять учетные данные (имя входа и пароль) при каждом своем подключении к базе данных SQL Azure.

Для предотвращения снижения производительности повторная проверка подлинности в соединении не проводится сразу же после переустановки пароля базы данных SQL Azure, даже если это соединение переустанавливается в результате выполнения операций с пулом соединений. В этом состоит отличие от поведения локального экземпляра SQL Server. Вместо этого база данных SQL Azure прибегает к использованию механизма повторной проверки подлинности при разъединении просроченных сеансов. После того как в любом соединении по прошествии более 60 минут после последней повторной проверки подлинности выдается новый запрос, выполняется повторная проверка подлинности. Если пароль был изменен, попытка выполнения запроса окончится неудачей и произойдет разрыв соединения.

Администрирование безопасности в базе данных SQL Azure аналогично администрированию безопасности в локальном экземпляре SQL Server. Управление безопасностью на уровне базы данных практически полностью идентично, если не рассматривать различия в применимости нескольких параметров. Ключевой проблемой в администрирование баз данных SQL Azure является разграничение прав пользователей, это тот аспект, на который следует обратить особое внимание.

Сервер SQL Azure задает дополнительный уровень абстракции, на котором определяется группирование баз данных. Базы данных, связанные с конкретным сервером SQL Azure, могут размещаться на разных физических компьютерах в центре обработки данных Microsoft. Для администрирования на уровне сервера всеми этими базами данных используется отдельная база данных с именем **master.**

База данных **master** содержит имена входа и сведения о том, какие имена входа имеют разрешения на создание баз данных или других имен входа. Для выполнения операций CREATE, ALTER или DROP с именами входа или базами данных необходимо подключение к базе данных **master**. База данных **master** также содержит представления sys.sql_logins и sys.databases, которые можно использовать для просмотра соответственно имен входа и баз данных.

Для подключения к базе данных SQL Azure с использованием созданных имен входа сначала необходимо предоставить каждому из таких имен входа разрешения уровня базы данных, используя команду CREATE USER. В некоторых средствах поток табличных данных (TDS) реализован иначе, поэтому может потребоваться добавить имя сервера SQL Azure к имени входа в строке подключения с помощью нотации <login>@<server>.

Чтобы имена входа, которые не являются именем входа субъекта серверного уровня, могли управлять безопасностью уровня сервера, в базе данных SQL Azure реализованы две роли безопасности: loginmanager - для создания имен входа и dbmanager - для создания баз данных. Эти роли могут назначаться только пользователям в базе данных **master**.

Аналогично роли securityadmin в локальном экземпляре SQL Server, роль loginmanager в базе данных SQL Azure необходима для создания имен входа. Создавать другие имена входа могут только имена входа субъекта серверного уровня и имена входа, относящиеся к роли loginmanager.

Таким образом, в ходе анализа работы SQL Azure можно предложить ряд дополнений, которые будут повышать безопасность и стойкость работы с данными в облаках:

1. Ограничение количества передаваемых и принимаемых пакетов в определенный промежуток времени, после чего будет выполняться запрос на повторную аутентификацию;

2. Реализация алгоритма проверки подлинности Windows-Server-SQL Server$

3. Внедрение программ и алгоритмов генерации хэш-функций отправляемых данных аутентификации и сравнение полученных значений; проверка значений хэша полученных данных маркера доступа с хэшем отправленных данных;

4. Повышение безопасности передачи данных при работе клиента с севером Azure (дополнительный процесс шифрования данных передачи клиент-сервер);

5. Разграничение прав пользователей при работе с облаками (администраторы, пользователи, продвинутые пользователи – одни имеют право чтения и изменения любых данных и любых настроек, в том числе и политик доступа; вторые имеют право лишь чтения и записи данных, без возможности удаления; а последние чтения, изменения и удаления данных).

Литература:

1. http://msdn.microsoft.com/ru-ru/library/ee872418.aspx

2. http://msdn.microsoft.com/ru-ru/library/ee336243.aspx

3. http://msdn.microsoft.com/practices

4. Кейт Браун. Руководство по Microsoft .NET Access Control Service для разработчиков. 2009.