Швейкин Владислав Витальевич
студент
ФГАОУ ВО «Самарский национальный исследовательский университет им. академика С.П. Королева»
г. Самара, Самарская область

АУТЕНТИФИКАЦИЯ С ПОМОЩЬЮ СЕРТИФИКАТОВ В СУБД ORACLE

Аннотация: *в данной работе рассматриваются механизмы и технологии проверки подлинности пользователей баз данных, в основе которых лежит инфраструктура сертификатов.*

Ключевые слова: *базы данных, сертификат, информационная безопасности, аутентификация, сервер.*

Основные определения

1. СУБД (система управления базами данных) – программно-аппаратный комплекс, позволяющий управлять и манипулировать базами данных.

Инфраструктура сертификатов

Одним из средств обеспечения высокого уровня управления разграничением доступа в СУБД Oracle является сервер безопасности. Он предоставляет единый механизм для аутентификации пользователей и ролей в распределённой среде и управления паролями. В основе механизма аутентификации находятся сертификаты стандарта X.509. Сервер обеспечивает поддержку данного стандарта и выполняет функции сертификационного центра.

Администратор базы данных или администратор режима безопасности с помощью утилиты Oracle Security Server осуществляет поддержку режима безопасности в глобальной среде. Этот программный инструмент позволяет администратору создавать учётные записи для новых пользователей с их идентификацией на основании персонального сертификата, а не пароля. Для регистрации на некоторых узлах пользователю необходимо иметь персональный сертификат, в кото-

ром указывается уникальная информация, согласно которой можно точно идентифицировать обладателя. Сертификат оформляется только один раз в Oracle Security Server в соответствии с международными стандартами X.509 и вся содержащаяся в нём информация должна быть надёжно защищена. Для того чтобы проверить правильность идентификации пользователей, которые имеют доступ к базе данных, в Oracle предусмотрена двухуровневая система безопасности. Сначала администратор базы данных должен создать для пользователя персональный сертификат с помощью Oracle Security Server, а затем отдельно создать для него учётную запись глобального пользователя. В случае отсутствия сертификата или учётной записи доступ к базе данных будет невозможен.

Аутентификация пользователя или машины осуществляется с помощью цифрового сертификата. Сертификат содержит имена пользователя и центра сертификации, номер сертификата, срок действия сертификата, предназначение открытого ключа и другую информацию. Так же он используется протоколом Secure Sockets Layer(SSL), обеспечивающим шифрование и проверку целостности данных при передаче по каналам связи.

На сегодняшний день Oracle позволяет реализовать аутентификацию на основе протокола Remote Authentication in Dial-In User Service (RADIUS). В качестве клиента выступает сервер Oracle и проходит аутентификацию на сервере RADIUS. Когда пользователь выполняет предусмотренную процедуру регистрации на сервере базы данных Oracle, последний в свою очередь для аутентификации этого запроса обращается на сервер RADIUS, который принимает или отклоняет запрос. Полученный результат передаётся на сервер Oracle, который предпринимает дальнейшие действия. Таким образом, выполняется прозрачная и защищённая процедура аутентификации.

Протокол RADIUS дополнительно можно использовать в качестве схемы аутентификации и учёта, выполняемых как последовательно действий:

1. Сервер RADIUS отправляет пароль серверу приложения.
2. Сервер приложения передаёт пароль машине клиента.
3. Пароль предоставляется конечному пользователю.

4. Пользователь отправляет отзыв на полученный пароль.

5. Значение отзыва возвращается на сервер RADIUS.

6. Сервер RADIUS проверяет полученное значение и отправляет серверу приложения ответ с указанием принять или отклонить соединение с данным пользователем.

Следует добавить, что с помощью сводных отчётов учётной службы RADIUS можно контролировать попытки нарушения защиты и доступа к ресурсам.

Список литературы

1. Смирнов С.Н. Безопасность систем баз данных. – М.: Гелиос АРВ, 2007. – 352 с.