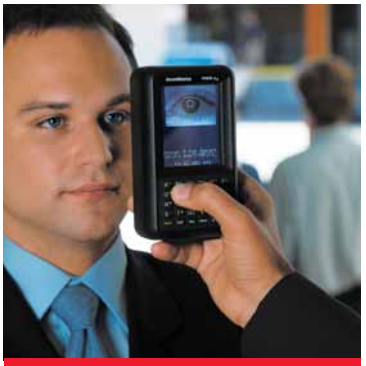
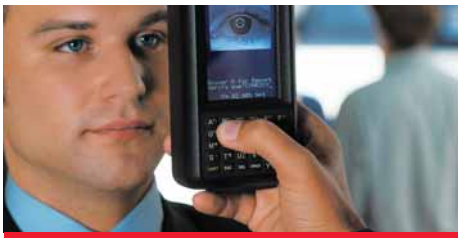
Oracle Advanced Security



ORACLE

ORACLE IS THE INFORMATION COMPANY



СОДЕРЖАНИЕ

Введение

Любая деятельность в современном мире бизнеса включает в себя множество задач по обеспечению безопасности и соблюдению законодательных норм. Экономические выгоды от передачи стороннему подрядчику некоторых бизнес-функций или частей бизнес-процесса предприятия с целью повысить производительность труда и снизить себестоимость продукции должны быть тесно взаимосвязаны с адекватной защитой сохранности интеллектуальной собственности и информации, касающейся частной жизни. В последние годы было множество случаев хищения персональных данных и мошеннических операций с использованием информации кредитных карт, приведших к убыткам в размере десятков миллионов долларов. Защита от таких видов угроз требует эффективных решений по безопасности. Университеты и медицинские организации повысили уровень безопасности данных, используемых для идентификации личности (PII), таких как номера социального страхования. Компании розничной торговли в настоящее время работают над обеспечением соответствия своих информационных систем требованиям PCI-DSS. Опции Oracle Advanced Security позволяют обеспечивать безопасность в строгом соответствии со стандартами, защищать данные в сети, на дисках и в резервных копиях, оставаясь «прозрачными» для приложений, т.к. их применение не требует внесения изменений в приложения.

Краткий обзор средств шифрования Oracle Database

Шифрование данных является ключевым компонентом при реализации принципа глубокой многоуровневой защиты, а также важным элементом защиты данных во время передачи и хранения. Впервые Oracle представил базу данных с программным интерфейсом (API) для шифрования данных в Oracle8i. На данный момент многие клиенты использую интерфейсы шифрования в базе данных Oracle для повышения безопасности конфиденциальных данных приложений. Достижение прозрачности чтения/записи зашифрованных данных посредством использования крипто-API, требует внедрения функции вызовов внутри самого приложения или использования предустановленного триггера БД. Представления данных приложения также могут нуждаться в расшифровывании, прежде чем они будут переданы в приложение. Кроме того, управление ключами шифрования должно производиться программным путем.

Oracle Advanced Security Transparent Data Encryption (TDE), впервые представленная в Oracle Database 10g Release 2, является самым передовым решением в области шифрования. TDE обеспечивает встроенное управление ключами шифрования и полную прозрачность шифрования конфиденциальных данных. Используемый при этом механизм шифрования баз данных основан на использовании команд DDL, полностью исключающих необходимость в изменении приложений, создании программных средств управления ключами шифрования, триггеров и представлений в базах данных.

Таблица 1. Краткое описание Oracle Database Encryption

Комплекс функций	НАБОР ПРОГРАММ DBMS OBFUSCATION (Oracle 8i и выше) SE & EE	DBMS CRYPTO (Oracle Database 10g R1 и выше) SE & EE	Oracle Advanced Security Transparent Data Encryption EE Only Option
Алгоритмы шифрования	DES, 3DES	DES, DES, AES, RC4, 3DES_2KEY(1)	3DES, AES (128, 192, и 256 бит)
Дополнительные формы	Не поддерживается	PKCS5, нули	PKCS5(2)
Режимы соединения на основе блочного шифра	CBC	CBC, CFB, ECB, OFB	CBC(2)
Шифровальные хэш-алгоритмы	MD5	SHA-1, MD4(1), MD5(1)	SHA-1(2)
Хэш-алгоритмы по ключу (MAC)	none supported	HMAC_MD5, HMAC_SH1	Не применяются
Шифровальный псевдо-случайный генератор чисел	RAW, VARCHAR2	RAW, NUMBER, BINARY_ INTEGER	Не применяется
Типы баз данных	RAW, VARCHAR2	RAW, CLOB, BLOB	Все кроме: OBJ., ADT, LOB

1) Предусматривает совместимость с предыдущими версиями

2) Для внутреннего использования, недоступно для разработчиков

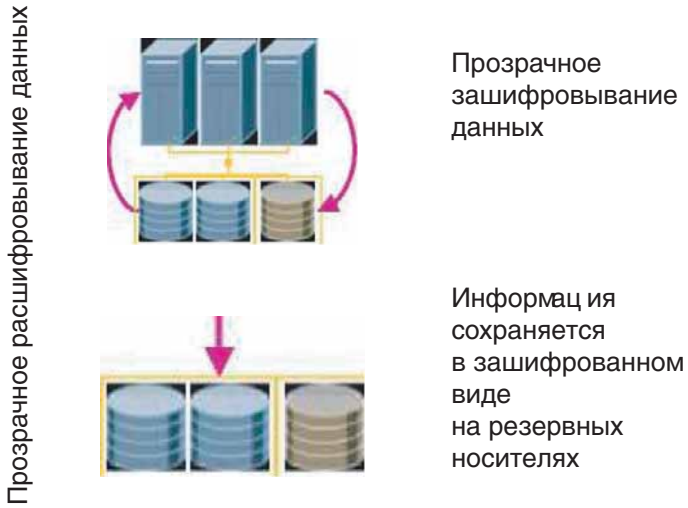


Рис 1. Краткое описание прозрачного шифрования данных

Прозрачное шифрование данных

Средствами TDE обеспечивается шифрование данных перед записью на диск и расшифровывание данных, прежде чем они возвращаются в приложение. Процесс зашифровывания и расшифровывания выполняется на уровне SQL и полностью прозрачен для прикладных программ и пользователей. Резервные копии баз данных, записанные на диск или магнитную ленту, будут содержать эти данные в зашифрованном виде. TDE, при необходимости, может быть использовано в сочетании с Oracle RMAN для зашифровывания всей СУБД Oracle в ходе резервирования на диски.

Преимущества прозрачного шифрования данных

1. Встроенное управление ключами шифрования
2. Прозрачное шифрование защищаемых данных (по столбцам) в прикладных программах
3. Прозрачное шифрование табличных пространств (Впервые в 11g)
4. Прозрачное шифрование файлов/LOBS (Впервые в 11g)
5. Интеграция аппаратного модуля безопасности (HSM) (Впервые в 11g)

Рис 2. Архитектура управления распределения ключами TDE

Краткое описание управления ключами шифрования

TDE автоматически создает ключ шифрования, когда проводится зашифровывание данных столбца в таблице базы данных. Ключ шифрования – уникальный для каждой таблицы. Если в таблице зашифровывается более одного столбца, то для каждого из столбцов используется один и тот же ключ шифрования. Ключи шифрования для таблиц сохраняются в справочнике Oracle и зашифровываются при помощи первичного ключа (мастер-ключа) шифрования TDE. Первичный ключ шифрования сохраняется вне базы данных в «тубусе для ключей» Oracle Wallet (файл формата PKCS#12), который зашифрован с помощью пароля, определяемого администратором безопасности или DBA в процессе создания. Новым в Oracle Database 11g Advanced Security является возможность сохранять первичный ключ в устройстве HSM, используя PKCS#11 интерфейс.

Этапы внедрения

В связи с тем, что TDE прозрачно для существующих приложений (не требуются создавать триггеры и представления баз данных), процесс шифрования стал проще по сравнению с традиционными решениями на основе использования API. Следующие шаги могут быть использованы для применения TDE:

1. Инициализация мастер-ключа
2. Определение данных для зашифровывания (PII данные, кредитные карты)
3. Проверка: поддерживает ли TDE выбранный тип данных, а также, не используются ли данные колонки в качестве внешних ключей.
4. Зашифровывание конфиденциальных данных, используя TDE

Инициализация мастер-ключа

Мастер-ключ для каждой базы данных свой. Несмотря на это, любой мастер-ключ может быть скопирован во вторичную базу данных, если ранее он не был там использован. Прежде чем, зашифровывать данные таблицы, необходимо создать мастер-ключ. Для этого существует следующая команда:

```
SQL> alter system set key identified by "password";
```

Эта команда создает «тубус для ключей» (Oracle Wallet) и использует указанный в команде пароль для зашифровывания в соответствии со стандартом PKCS#5. Oracle Wallet сохраняет историю уже использованных мастер-ключей и делает их доступными, когда данные, зашифрованные старым ключом, считываются с резервных носителей.

Как открыть «тубус для ключей» Oracle Wallet

До того как база данных сможет расшифровать табличные ключи для зашифровывания и расшифровывания прикладных данных, необходимо открыть «тубус для ключей» Wallet, который содержит первичный ключ шифрования. Конечно, можно запустить базу данных и работать в ней без открытия Wallet, но при попытке получить доступ к зашифрованным данным база данных выдаст сообщение об ошибке. Закрывать Wallet (и ограничивать тем самым доступ к данным) целесообразно только в ходе работ по техническому обслуживанию, когда доступ к базе данных разрешен специалисту, занимающемуся поддержкой.

Как изменить Мастер-ключ

Мастер-ключ может быть изменен при повторном запуске команды “alter system”.

```
SQL> alter system set key identified by "password";
```

При изменении мастер-ключа все табличные ключи в справочнике Oracle будут обновлены (расшифрованы и зашифрованы вновь). Стандарт безопасности данных PCI (DSS) 1.1 требует «обновлять ключи шифрования, не реже одного раза в год». Изменение мастер-ключа приведет к обновлению зашифрованных ключей столбцов, используя новый мастер-ключ, а зашифрованные данные в таблицах останутся без изменений.

Как изменить пароль Wallet

Пароль Wallet может быть изменен независимо от мастер-ключа шифрования, он используется исключительно для зашифровывания данных файла Wallet на диске. Для этого можно воспользоваться программой Oracle Wallet Manager (введите в командной строке 'owm') или утилитой 'orapki'.

Определение конфиденциальных данных

Процесс поиска конфиденциальных данных, таких как номера социального страхования и кредитных карт, может оказаться затруднительным, особенно в комплексных приложениях. Единственный метод, которым можно воспользоваться, – это поиск в справочнике Oracle по названию столбца и типу данных, которые часто используются для хранения подобной информации.

```
SQL> select column_name, table_name, data_type from
dba_tab_cols where column_name like '%SOCIAL%' or
column_name like '%SSN%' or column_name like
'%SECNUM%' or column_name like "%SOC%' and
owner='<owner>';
```

Типы данных, поддерживаемых TDE

TDE поддерживает наиболее распространенные типы данных. К ним относятся:

VARCHAR2	CHAR	DATE
NUMBER	NVARCHAR2	NCHAR
RAW	RAW	SECUREFILES (LOBS)
BINARY_DOUBLE	BINARY_FLOAT	

TDE и внешние ключи

TDE не может быть использован для зашифровывания столбцов, которые используются во внешнем ключе. Для того чтобы проверить, является ли колонка частью внешнего ключа, изучаются данные из справочника Oracle.

```
select A.owner, A.table_name, A.column_name, A.constraint_name

from dba_cons_columns A, dba_constraints B

where

A.table_name = B.table_name and

A.column_name = 'YOURCOLNAME' and

B.constraint_type = 'R';
```

Зашифровывание данных с помощью TDE

Чтобы зашифровать существующие столбцы в таблице:

```
SQL> alter table customers modify (credit_card encrypt);
```

В ходе выполнения транзакции по зашифровыванию поддерживается последовательное чтение данных. Транзакции DML (вставить, обновить, удалить), выполняемые в течение транзакции зашифровывания, будут запрашивать 'изменения online '.

Создавать новую таблицу с зашифрованными колонками просто. Например, с помощью стандартного алгоритма шифрования AES192.

```
SQL> create table billing_information (

first_name varchar2(40)

,last_name varchar2(40)

,card_number varchar2(19) encrypt using 'AES256');
```

Transparent Data Encryption поддерживает работу с индексами, минимизируя дополнительный поиск в зашифрованном столбце.

```
SQL> create index cust_idx on customers (credit_card);
```

Когда столбец с индексами готов к зашифровыванию, сначала рекомендуется удалить существующие индексы, зашифровать столбец, а затем заново создать индексы.

Смена ключа таблицы/столбца

При выполнении команды "alter table" ключ таблицы или столбца, размер ключа и алгоритм могут быть независимо изменены:

```
SQL> ALTER TABLE employee REKEY;

SQL> ALTER TABLE employee REKEY USING 'AES256';

SQL> ALTER TABLE employee ENCRYPT USING 'AES128';
```

Изменение ключа таблицы или столбца приведет к повторению шифрования данных в таблице.

Практические рекомендации по проведению начального шифрования данных

За время существования таблицы, ее данные могут фрагментироваться, расположиться в ином порядке, разделяться по категориям, увеличиваться в количестве и перемещаться внутри табличного пространства; это может привести к возникновению неиспользуемых блоков со старыми, недоступными копиями данных внутри файла базы данных. Когда шифруется существующий столбец, шифруется только его самая последняя "действующая" копия, при этом могут оставаться данные в незашифрованном виде в «старых» копиях данных столбца.

Для минимизации риска оставить конфиденциальные данные в незашифрованном виде при шифровании Oracle рекомендует создавать новое табличное пространство, перемещать таблицы приложений в него, и удалять старое табличное пространство.

1. Подготовьте полную резервную копию вашей базы данных
2. Создайте новое табличное пространство, точно определяющее новый массив данных
3. Зашифруйте столбцы с конфиденциальными данными в исходной таблице
4. Повторите шаг 3 для всех таблиц, содержащих конфиденциальные данные
5. Переместите таблицы из исходного табличного пространства в новое табличное пространство.
6. Удалите исходное табличное пространство. Внимание: не используйте опцию '... and datafile' вместе с командой 'drop tablespace' , применяйте утилиту 'shred' или другие зависящие от платформы утилиты для безопасного удаления содержания старых файлов данных в операционной системе.

Использование команд операционной системы, таких как 'shred' , уменьшает вероятность обнаружить побочные копии файлов баз данных, сгенерированные либо операционной системой, либо программным обеспечением хранения данных.

Шифрование при резервном копировании с помощью rman

Для повышения уровня безопасности резервные копии, созданные с помощью RMAN, могут быть зашифрованы посредством Oracle Advanced Security. И в случае, если даже неавторизированные пользователи получат доступ к зашифрованным резервным копиям данных, они не смогут их прочитать. Зашифрованы могут быть любые копии, создаваемые RMAN, за исключением образов данных (image copy backups).

Зашифрованные резервные копии расшифровываются автоматически во время операций восстановления только, если доступны необходимые для их расшиф-

ровывания ключи, – вводимые пользователями пароли или с помощью Oracle Encryption Wallet.

Для использования шифрования с RMAN, параметр инициализации COMPATIBLE в целевой базе данных должен быть установлен как минимум на 10.2.0.

Когда используется команда “backup backupset” с зашифрованными резервными наборами, резервные наборы копируются в зашифрованном виде. Так как “backup backupset” просто копирует уже зашифрованную резервную программу на диск или магнитную ленту, то в ходе операции “backup backupset” не нужен никакой ключ расшифровывания, и данные никогда не расшифровываются в ходе какой-либо части процесса. Команда “backup backupset” не может ни зашифровать, ни расшифровать резервные наборы.

Если некоторые столбцы базы данных зашифрованы при использовании Transparent Data Encryption и скопированы с помощью резервного шифрования, то эти столбцы будут вторично зашифрованы во время копирования. Когда резервные программы расшифровываются во время восстановления, зашифрованные столбцы возвращаются к своему исходному виду. Если не установлен определенный алгоритм шифрования, то по умолчанию применяется 128-битный алгоритм шифрования AES.

Методы шифрования RMAN

RMAN предлагает три метода шифрования: прозрачный метод, метод паролей, и комбинированный метод. Оба метода, прозрачный и комбинированный, предусматривают использование Oracle Encryption Wallet.

Прозрачное шифрование резервных копий

Прозрачное шифрование способно создать и восстановить зашифрованные резервные копии без вмешательства DBA, если доступна инфраструктура систем управления ключами. Прозрачное шифрование лучше всего подходит для ежедневных операций резервирования, где резервные копии восстанавливаются в той же базе данных, из которой они были скопированы. Прозрачное шифрование – метод, используемый по умолчанию, для шифрования в RMAN.

При использовании прозрачного шифрования предварительно необходимо установить и настроить Oracle Encryption Wallet, так как описано в документации для Oracle Transparent Data Encryption. После того как Oracle Encryption Wallet установлен, зашифрованные резервные копии могут быть созданы и восстановлены без дальнейшего вмешательства DBA.

Резервные копии, зашифрованные при помощи пароля

Шифрование при помощи пароля требует, чтобы DBA вводил пароль при создании и восстановлении зашифрованных резервных копий. Восстановление резервных копий, зашифрованных при помощи пароля, требует тот же пароль, который использовался для создания резервной копии. Шифрование с паролем полезно для резервных копий, которые будут восстановлены в удаленном месте, но которые должны оставаться защищенными во время передачи. Шифрование с использованием паролей не стоит использовать постоянно. Oracle Encryption Wallet не требует настройки в случае, если парольное шифрование применяется однократно.

Если вы забыли, или утратили пароль, который вы использовали для шифрования резервной копии, зашифрованной при помощи пароля, восстановить резервную копию вы не сможете.

Для применения парольного шифрования, воспользуйтесь командой "SET ENCRYPTION ON IDENTIFIED BY password ONLY” находящейся в командных файлах RMAN.

Резервные копии, зашифрованные комбинированным методом

Резервные копии, зашифрованные при помощи комбинированного метода шифрования, могут быть восстановлены либо с помощью прозрачного метода, либо при помощи ввода пароля. Резервные копии, зашифрованные при помощи метода комбинированного шифрования, полезны, когда вы создаете резервные копии, которые обычно восстанавливаются на месте, используя Oracle Encryption Wallet, но которые периодически необходимо восстанавливать дистанционно, там, где Oracle Encryption Wallet не доступен.

Когда восстанавливается резервная копия, зашифрованная при помощи комбинированного метода шифрования, вы можете использовать либо Oracle Encryption Wallet, либо пароль.

Если вы забыли или потеряли пароль, который вы использовали для шифрования резервной копии комбинированным методом, и Oracle Encryption Wallet также утрачен, то вы не сможете восстановить данные из зашифрованной резервной копии.

Для создания резервных копий комбинированным методом, укажите команду SET ENCRYPTION ON IDENTIFIED BY в RMAN-скриптах.

Расширение функциональных возможностей прозрачного шифрования данных

Oracle Database 11g Advanced Security Transparent Data Encryption включает в себя несколько важных доработок.

Поддержка дополнительных типов данных

Oracle Database 11g Advanced Security Transparent Data Encryption поддерживает шифрование нового типа данных Oracle Database 11g SecureFiles. Это дает возможность прозрачного шифрования, для отсканированных медицинских снимков, договоров и других важных документов, сохраненных в базе данных.

Шифрование табличного пространства

В Oracle Database 11g для опции Advanced Security/ Transparent Data Encryption появилась поддержка шифрования табличных пространств баз данных. Шифрование табличного пространства означает, что все его объекты могут быть прозрачно зашифрованы на уровне блоков. Блоки данных будут прозрачно расшифрованы при чтении.

Могут быть зашифрованы только новые (вновь создаваемые) табличные пространства.

```
SQL> CREATE TABLESPACE securespace DATAFILE '/
home/user/oradata/secure01.dbf' SIZE 150M ENCRYPTION
USING 'AES192' DEFAULT STORAGE(ENCRYPT);
```

Все объекты базы данных, создаваемые в новом табличном пространстве (перемещаемые в него) будут зашифрованы. При использовании шифрования табличного пространства снимаются ограничения по внешнему ключу, характерные для шифрования по столбцам.

Аппаратные модули безопасности (HSM) защиты мастер-ключа

Для обеспечения соответствия еще более строгим мерами безопасности мастер-ключ может быть сохранен в соответствующем стандарту PKCS#11 HSM-устройстве, которое позволяет множеству баз данных или копиям базы данных в среде RAC с одинаковыми зашифрованными данными, обмениваться одинаковыми мастер-ключами шифрования. С введением компанией Oracle поддержки устройств стандарта PKCS#11, клиенты могут выбирать из огромного множества поставщиков HSM-устройств.

Когда необходимо обеспечить переход от шифрования на уровне столбцов (при помощи TDE в Oracle 10g R2) к шифрованию табличного пространства (Oracle11g R1), следует выполнить операцию смены ключа, которая генерирует новый мастер-ключ для зашифрованных столбцов и создает новый мастер-ключ для шифрования табличного пространства.

При изменении способа хранения мастер-ключа шифрования в файле, на способ хранение его в устройстве HSM, выполните следующие шаги:

1) Заново создайте мастер-ключ для генерации ключа шифрования табличного пространства, на случай, если позже он вам понадобится

2) Измените файл sqlnet.ora:

```
ENCRYPTION_WALLET_LOCATION=
SOURCE=(METHOD=HSM)
```

3) SQL> alter set key identified by "<user_id:password>" migrate from <wallet password>

<user_id:password> is the authentication information for the HSM device.

Шифрование DataPump

Прозрачное шифрование данных может быть применено с помощью утилиты Oracle Datapump. Это новая функция в Oracle Database 11g. Для дополнительной информации см. документацию Oracle Datapump.

Поддержка для Oracle Streams и логического резервирования

Oracle Database 11g Advanced Security TDE поддерживает технологию Oracle Streams и логическое резервирование баз данных (logical standby), в то время, как Oracle Database 10g Release 2 Advanced Security TDE обеспечивает поддержку только физического (physical standby) резервирования.

Шифрование данных при передаче по сети

Oracle Advanced Security обеспечивает безопасность и конфиденциальность данных в сети, устраняя утечку данных, потерю данных, противодействуя атакам по подмене информации или атакам типа «person-in-the-middle». Все каналы связи в Oracle Database могут быть зашифрованы с помощью Oracle Advanced Security. Для баз данных, содержащих наиболее важную информацию ограничение доступа за счет строгой аутентифи-

кации является первым рубежом многоуровневой защиты. Oracle Advanced Security обеспечивает ряд решений для строгой аутентификации, включая Kerberos, инфраструктуру открытых ключей, RADIUS и DCE для Oracle Database 10g.

Промышленный стандарт шифрования и контроля целостности данных

Oracle Advanced Security защищает все входящие и исходящие каналы связи в СУБД Oracle. Предприятия имеет выбор между использованием родных алгоритмов шифрования/обеспечения целостности в Oracle Advanced Security и SSL для защиты данных в сети. Некоторые типичные сценарии, требующие сетевое шифрование:

- Сервер базы данных должен находиться за межсетевым экраном, и пользователи получают доступ к серверу посредством клиент-серверного приложения
- Передача данных между серверными приложениями в DMZ и базой данных, которая находится за вторым межсетевым экраном, должна быть зашифрована.

Алгоритмы родного шифрования и обеспечения целостности в Oracle Advanced Security не требуют внедрения PKI. С каждой последующей версией БД добавляются новые алгоритмы шифрования, по мере того как они улучшают промышленные свойства. Последнее добавление – это Advanced Encryption Standard (AES), усовершенствованный в плане безопасности алгоритм и выполняемый вместо DES. Полный список алгоритмов Encryption и Data integrity:

- AES (128,192 и 256 бит)
- RC4 (40, 56,128,256 бит)
- 3DES (2 и 3 ключа; 168 бит)
- MD5
- SHA1

Шифрование на основе SSL доступно для предприятий, которые выбрали для использования инфраструктуру открытых ключей. В версии Oracle Advanced Security 10g появилась поддержка протокола TLS 1.0 Oracle Advanced Security предоставляет набор шифров AES вместе с запуском протокола TLS 1.0 в Oracle Database 10g.

SSL

Oracle внедряет протокол SSL для шифрования данных, которые передаются из баз данных клиентов в СУБД и обратно. Он охватывает данные Oracle Net Services (он же в прошлом Net8), LDAP, толстого JDBC, и IIOP формата. SSL предоставляет пользователям альтернативный исходному протоколу Oracle Net Services способ шифрования, который поддерживается в Oracle Advanced Security (ранее известный как Advanced Networking Option), начиная с версии Oracle7. Преимущество SSL в том, что это действующий стандарт Интернета, и может использоваться клиентами, которые не работают с протоколами Oracle Net Services.

В трехуровневой системе, поддержка SSL в базе данных означает, что обмен данными между средним уровнем и базой данных может быть зашифрован при использовании SSL. Протокол SSL завоевал доверие пользователей, и это, возможно, наиболее широко применяемый и хорошо понимаемый в использовании протокол на сегодняшний день. Программная реализация SSL в Oracle поддерживает три стандартных метода аутентификации, включая анонимный метод (Диффи – Хеллман), только серверную аутентификацию, используя протоколы X.509 certificates, и взаимную (клиент-серверную) аутентификацию с X.509.

Oracle Application Server также поддерживает SSL шифрование между тонкими клиентами и Oracle Application Server, так же как между Oracle Application Server и Oracle Data Server. Как и в Oracle, анонимная, только серверная и клиент-серверная аутентификация поддерживается X.509 .

Безопасность JDBC

JDBC, интерфейс Java, который обеспечивает соединение с реляционной базой данных из программ Java. Sun Microsystems и компания Oracle совместно определили стандарт JDBC, а Oracle, как индивидуальный провайдер, дополняет и расширяет стандарт при помощи собственных JDBC-драйверов. Oracle использует два типа JDBC драйверов: толстые JDBC-драйвера, надстроенные поверх клиента C-based Oracle Net Services, и тонкие (чистая Java) JDBC-драйвера для поддержки загружаемых приложений.

В связи с тем, что толстый JDBC использует полный стек передачи данных Oracle Net Services для клиента и сервера, он может использовать преимущества шифрования Oracle Advanced Security и механизмов аутентификации. Так как тонкие JDBC драйверы предназначены для использования с загружаемыми приложениями в Интернете, Oracle включает 100% реализацию Java в шифровании Oracle Advanced Security и алгоритмах

обеспечения целостности, для использования с тонкими клиентами.

Простая конфигурация, без изменений приложений

Настройка параметров сети для сервера и/или клиента дает возможность применения функций шифрования/целостности. Большинство предприятий, могут легко применять эту технологию, поскольку она не требует изменений в приложении.

Средства строгой аутентификации Oracle Database 10

Несанкционированный доступ к информации – это очень старая проблема. Сегодня деловые решения принимаются на основе информации, собранной из терабайтов добытых данных. Защита важной информации – это важнейший фактор способности бизнеса оставаться конкурентоспособным. Доступ к ключевым хранилищам данных, таким как Oracle Database 10g, которые могут содержать ценную информацию, должен быть предоставлен только тогда, когда пользователи идентифицированы и прошли аутентификацию. Проверка пользовательской идентификационной информации подразумевает сбор большего количества информации, нежели стандартные имя пользователя и пароль. Oracle Advanced Security предоставляет фирмам возможность усилить их существующие инфраструктуры безопасности, такие как технология Kerberos, Инфраструктура Открытых Ключей (PKI) и RADIUS для средств строгой аутентификации Oracle Database 11g. Списки аннулированных сертификатов могут быть сохранены в файловой системе, Oracle Internet Directory или используя Пункты Распределения CRL (CRL Distribution Points).

Способность серверов Oracle Database или клиентов/пользователей использовать реквизиты доступа PKI, сохраненные в смарт-карте или другом аппаратном модуле памяти, используя отраслевой стандарт PKCS#11. Это особенно полезно для пользователей, так как это предоставляет мобильный доступ к базе данных через приложения типа клент-сервер или веб-интерфейс.

Сохранение реквизитов доступа сервера в аппаратных модулях обеспечивает дополнительный уровень безопасности, который требуют некоторые внедренные системы.

Аутентификация Kerberos

Oracle Advanced Security включает клиент Kerberos, совместимый с мандатом технологии Kerberos v5, которая издана Массачусетским технологическим институтом (MIT). Версия 5 совместима с любым сервером Kerberos или Microsoft KDC. Предприятия могут продолжать работать в гетерогенной среде, используя решение Oracle Advanced Security. Как только база данных Oracle зарегистрирована на сервере технологии Kerberos и сконфигурирована для поддержки сервиса Kerberos Service, пользователи предприятия могут произвести аутентификацию в базу данных без каких-либо дополнительных сложностей. Организации, которые уже используют сервер технологии Kerberos и его адаптер, могут переместить своих внешних пользователей базы данных в каталог, чтобы извлечь выгоду от централизованного управления пользователями.

Расширения функциональных возможностей технологии Kerberos

Расширение функциональных возможностей Oracle Database 11g Advanced Security Kerberos включают поддержку для основных имен до 2000 символов в длину. Кроме того, Oracle Database 11g Advanced Security предоставляет поддержку областей пересечения технологии Kerberos, разрешающую администраторам доступа Kerberos в одной области подтвердить подлинность администраторам Kerberos в другой области.

Вот пример создания пользователя Oracle с внешней аутентификацией. Имя пользователя должно соответствовать пользователю Kerberos.

```
SQL> CONNECT / AS SYSDBA;

SQL> CREATE USER "KRBUSER@SOMECO.COM"
IDENTIFIED

EXTERNALLY; SQL> GRANT CREATE SESSION TO
"KRBUSER@SOMECO.COM";
```

Пожалуйста, обратитесь к руководству администратора Oracle Advanced Security для дополнительной информации по настройке базы данных Oracle и клиента для аутентификации Kerberos.

Поддержка PKI

Клиент SSL в Oracle Advanced Security может использоваться в любом PKI, который является совместимым с отраслевыми стандартам и соответствует стандарту запросов сертификата PKCS7 и выпуску сертификатов X509v3. Oracle Advanced Security предусматривает адаптер Entrust, который позволяет бизнес-приложениям использовать Entrust PKI совместно с базой данных Oracle 11 (с Oracle Database 11g).

Oracle Wallet Manager продолжает быть инструментом для использования запросов сертификатов и других задач управления сертификатом для конечных пользователей. Дополнительные утилиты командной строки, которые помогают в управлении Списком Аннулированных Сертификатов (CRLs) и других операций Oracle Wallet также доступно в этом выпуске.

Список Аннулированных Сертификатов, размещенный на LDAP сервере, файловая система или URL, поддерживаются инфраструктурой Oracle SSL.

Поддержка PKCS#12

Oracle Advanced Security поддерживает сертификаты X.509 сохраненные в контейнере PKCS#12, обеспечивая накопителю Oracle поддержку приложений 3-х фирм, таких как Netscape Communicator 4.x и Microsoft Internet Explorer 5.x, и предоставляя накопителю мобильность в рамках операционных систем. Пользователи, которые имеют существующие учетные данные PKI, могут их экспортировать в формате PKCS#12 и многократно использовать в Oracle Wallet Manager, и наоборот. Таким образом PKCS#12 увеличивает функциональную совместимость и уменьшает стоимость развертывания PKI для организаций.

Поддержка PKCS#11, Смарт–карты/ Аппаратные Модули Безопасности

Oracle Wallet – это программный контейнер, который содержит в себе секретный ключ и другие доверительные пункты сертификата. Oracle Advanced Security 10g обеспечивает поддержку отраслевого стандарта PKCS#11. Это позволяет создавать и хранить секретные ключи, которые ранее хранились в файловой системе, в безопасных устройствах, таких как аппаратный модуль безопасности или смарт-карта, которые доступны на рынке.

Аутентификация с использованием PKI для Oracle Database 10g Enterprise Users

Начиная с Oracle8i, Oracle Advanced Security поддерживает аутентификацию для пользователей каталога к базе данных Oracle, используя цифровые сертификаты, хранящиеся в каталоге.

Oracle расширяет интеграцию PKI и функциональную совместимость при помощи:

- Поддержки PKCS#11
- Хранение накопителя в Oracle Internet Directory
- Множественных сертификатов на основе накопителя
- Устойчивого шифрования накопителя
- Сервера сертификатов OracleAS

Хранение ключей пользователя в Oracle Internet Directory

Создание пользовательских «тубусов» для хранения ключей в Oracle Enterprise Security Manager – часть процесса регистрации пользователя. Хранение ключей осуществляется в справочнике Oracle Internet Directory или другом совместимом с LDAP каталоге. Oracle Wallet Manager может загружать «тубусы» в LDAP и извлекать их из LDAP. Сохранение «тубуса» для ключей в централизованном LDAP-каталоге поддерживает передвижение пользователей, позволяя получать доступ из любой точки местоположения или с любого устройства устройств. Это обеспечивает непротиворечивую и надежную аутентификацию пользователя, предоставляя централизованное управление «тубусом» для хранения ключей на протяжении всего жизненного цикла накопителя.

Поддержка множества сертификатов

Oracle Wallets поддерживает множество сертификатов на накопителе, включая:

• Сертификат подписи протокола S/MIME;

• Сертификат кодирования протокола S/MIME;

• Сертификат, подписывающий код;

Oracle Wallet Manager версии 3.0 поддерживает множественные сертификаты отдельной цифровой единицы в маске – с множественными парами секретного ключа в маске (каждый секретный ключ может соответствовать только одному сертификату). Это допускает объединение и более безопасное управление PKI полномочиями пользователей.

Устойчивое шифрование данных в Wallet

Секретные ключи, связанные с сертификатом X.509, требуют устойчивого шифрования по безопасным каналам. Oracle заменяет DES-шифрование тройным DES, который является существенно более устойчивым алгоритмом шифрования и обеспечивает мощную защиту для хранения ключей в Oracle.

Поддержка протокола аутентификации (RADIUS)

Oracle Advanced Security снабжен протоколом RADIUS, который позволяет Oracle DataBase 11 соблюдать аутентификацию и полномочия, утвержденные на сервере RADIUS. Эта функция особенно полезна для фирм, которые заинтересованы в двухфакторной аутентификации, которая устанавливает Вашу личность на основе того, что Вы знаете (пароль или ПИН – код) и том, чем Вы владеете (карту с переменным паролем), предоставленную неким производителем карт с переменным паролем. RADIUS (RFC #2138) это распространенная система, которая обеспечивает удаленный доступ к сетевым службам и давно признанна как отраслевой стандарт для удаленного и контролируемого доступа к сети. Полномочия пользователя в RADIUS и информация доступа определены на сервере RADIUS для того, чтобы дать возможность этому внешнему серверу выполнить аутентификацию, авторизацию и учет, когда это требуется.

Поддержка RADIUS в Oracle – это реализация протоколов клиента RADIUS (RADIUS Client), которые дают возможность базе данных предоставить пользователям RADIUS аутентификацию, авторизацию и службы учета. Они посылают запрос аутентификации на сервер RADIUS и действуют в соответствии с откликами сервера. Аутентификация может произойти в синхронном или асинхронном режиме аутентификации и является частью конфигурации Oracle для поддержки RADIUS.

Oracle Advanced Security предоставляет пользователям RADIUS аутентификацию, разрешения авторизации, сохраненные в RADIUS и основные службы учета при обращении к базе данных Oracle .

Заключение

Шифрование – это ключевой компонент концепции глубокой защиты. Oracle продолжает разрабатывать инновационные решения, чтобы помочь клиентам соответствовать все более и более строгим требованиям безопасности по охране данных РП.

Компании розничной торговли могут использовать Oracle Advanced Security TDE, чтобы соответствовать требованиям PCI-DSS, в то время как учебные и здравоохранительные организации могут использовать TDE для защиты номеров социального страхования и прочей важной информации. Шифрование играет особенно важную роль в защите данных при пересылке. Oracle Advanced Security Network защищает данные при пересылке по внутрикорпоративной сети от сетевого прослушивания и модификации. Oracle Advanced Security TDE защищает важную информацию на дисковых и резервных носителях от несанкционированного доступа, помогая уменьшить ущерб от утерянных или похищенных носителей.

Oracle Россия

123317, г. Москва,
Пресненская наб., 10,
Москва-Сити,
БЦ «Башня на набережной», блок С
Тел.: +7 (495) 6411400
Факс: +7 (495) 6411414
E-mail: oracle_ru@oracle.com
Internet: www.oracle.com/ru/

191186, г. Санкт-Петербург,
Невский пр., 25
Тел.: +7 (812) 363 3257
Факс: +7 (812) 363 3258

Oracle Украина
01601, г. Киев,
Бизнес-центр «Парус»,
ул. Мечникова, 2-а, 16 эт.
Тел.: + 380 (44) 490-90-50/51
Факс: + 380 (44) 490-90-52

Oracle Казахстан
480099, г. Алматы,
микрорайон Самал-2, Самал Тауэрс,
оф. 97, блок А-2, 6-й этаж
Тел.: +7 (3272) 58 47 48/40
Факс: +7 (3272) 58 47 44

Oracle Республика Беларусь
220004, г. Минск,
ул. Немига, д. 40,
БЦ «Немига-Сити», к. 511
Тел.: +375296193426
+79152147406

Oracle Азербайджан
AZ1065, г. Баку,
ул. Джафар Джаббарли, 14,
БЦ «Каспиан Плаза III», 11 этаж

ORACLE®