ЧАСТЬ II

ПРАКТИКА

ВВЕДЕНИЕ

Практическая роль аутентификации в современном компьютеризированном мире весьма велика. Пользователи компьютеров используют механизмы аутентификации для того, чтобы быть авторизованными в своем компьютере, в корпоративной сети, для доступа к различным приложениям. С точки зрения защиты информации аутентификация является обязательной составляющей практически всех систем защиты информации, а для защиты от несанкционированного доступа аутентификация является одним из важнейших механизмов защиты наряду с шифрованием информации. С точки зрения бизнес-ориентированных информационных систем роль аутентификации особенно велика для организации таких сервисов, как:

- доступ к корпоративной сети;
- удаленный доступ к корпоративной сети и приложениям, в том числе беспроводной доступ;
- применение ЭЦП в документообороте, а также для подписи и шифрования сообщений;
- доступ к системам дистанционного банковского обслуживания;
- доступ к системам планирования ресурсов предприятия (ERP), управления взаимоотношениями с клиентами (CRM), управления цепочками поставок (SCM), биллинговым системам и т.д.;
- организация защищенных каналов взаимодействия (VPN);
- защита данных на серверах и рабочих станциях.

Безусловно, для организации доступа к различным информационным системам требуется использовать те или иные механизмы и средства аутентификации (рассмотренные в первой части данной книги) в зависимости от уровня защищенности систем и информационных ресурсов.

Практические решения ряда типовых задач по организации систем аутентификации на различных платформах приводятся в следующих главах.

Глава I
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДОСТУПА К ДАННЫМ И ПРИЛОЖЕНИЯМ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНИЗАЦИИ НА ОСНОВЕ РЕКОМЕНДАЦИЙ И ПРОДУКТОВ MICROSOFT. ТИПОВЫЕ РЕШЕНИЯ

1.1. Основные сервисы для обеспечения надежной аутентификации и управления доступом

Корпорация Microsoft выделяет пять основных сервисов (областей), связанных с обеспечением надежной аутентификации и управлением доступом:

- служба каталога (Active Directory Domain Services);
- инфраструктура PKI, шифрования, управления циклами безопасности, аутентификация с помощью сертификатов или смарткарт (Active Directory Certificate Services);
- управление федеративными отношениями (Active Directory Federation Service);
- управление правами доступа к информации (Active Directory Rights Management Services);
- управление идентификацией (Microsoft Identity Lifecycle Manager 2007).

Основой для построения системы безопасности является Служба каталога Active Directory Domain Services. Остальные решения могут использоваться в зависимости от потребностей организации. Первые четыре области представляют собой платформу для создания системы надежной аутентификации и управления доступом.

1.1.1. Служба каталога (Active Directory Domain Services)

Наиболее известная область (и технология), используемая в настоящее время — служба каталога Active Directory Domain Services, которая является основным компонентом безопасности Windows (рис. 1.1).

Основные цели и задачи службы каталога:

- обеспечение централизованного управления и хранения учетной информации;
- управление растущим количеством пользователей, ролей и устройств;
- упрощение внесения изменений в политики безопасности компании, например, включение многофакторной аутентификации, шифрование данных и контроль исполнения политик безопасности.

Преимущества при ее использовании:

- упрощение управления учетными записями через унифицированную консоль;
- повышение безопасности с возможностью использования различных средств безопасности внутри сети;
- возможность использования службы каталога в качестве средства аудита информации об учетных записях;
- снижение стоимости управления сетями.

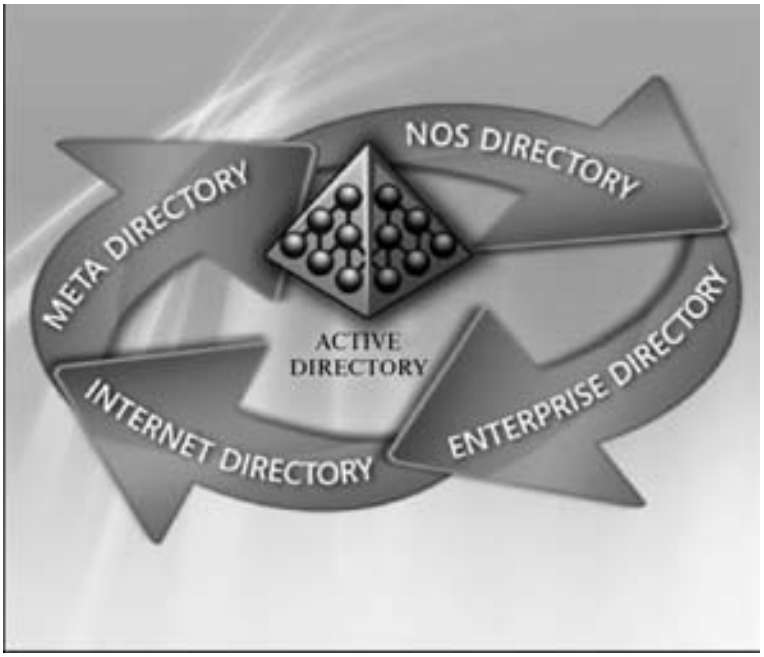

Рис. 1.1. Служба каталога

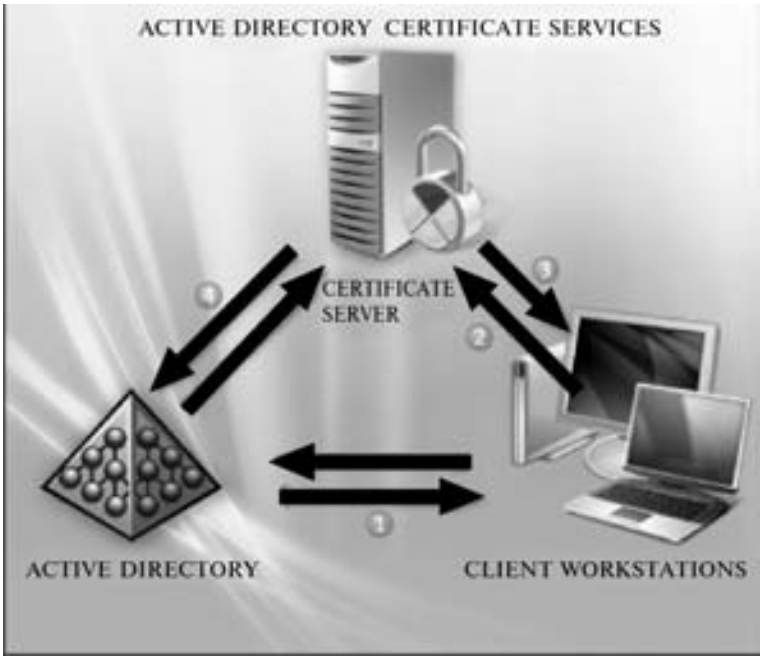

Рис. 1.2. Служба аутентификации с помощью сертификатов

1.1.2. Служба аутентификации с помощью сертификатов или смарт-карт (Active Directory Domain Services)

Основные цели и задачи этой службы (рис. 1.2):

- переход от традиционной аутентификации на основе имени и пароля пользователя к более стойкой и надежной схеме;
- поддержка индустриальных стандартов.

Преимущества при ее использовании:

- повышение защищенности сети с помощью средств многофакторной аутентификации и проверки подлинности цифровых сертификатов с помощью протокола Online Certificate Status Protocol (OCSP);
- управление цифровыми сертификатами объектов (пользователей и устройств) без вмешательства пользователей;
- снижение стоимости владения благодаря автоматизации регистрации, хранения и отзыва цифровых сертификатов с помощью Active Directory.

1.1.3. Управление федеративными отношениями (Active Directory Federation Services)

Служба Active Directory Federation Services в Windows Server 2003 R2 (рис. 1.3) является для администраторов основным инструментом в построении корпоративной инфраструктуры с возможностью защищенного обмена идентификационными данными. Здесь обыч-

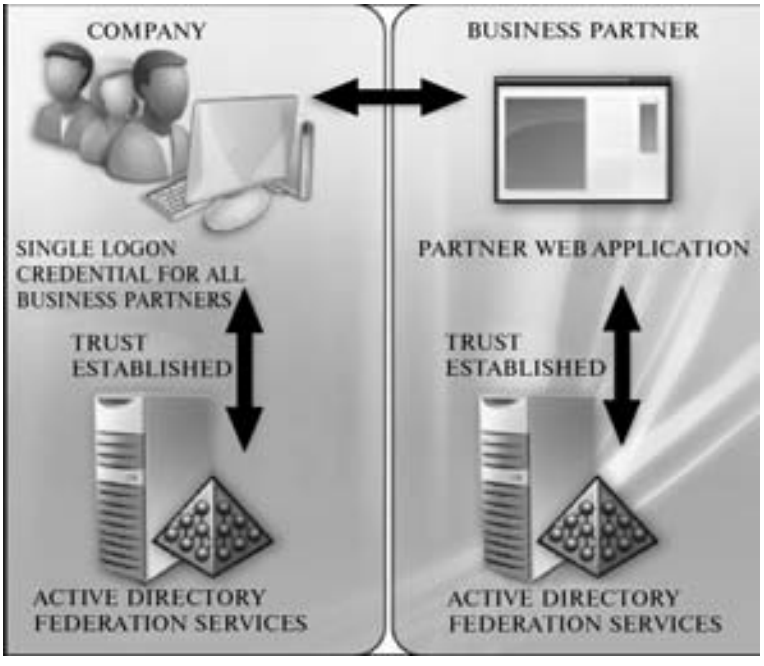

Рис. 1.3. Служба управления федеративными отношениями

но возникает ряд вопросов, разрешить которые позволяет именно Active Directory Federation Services. Интегрированные системы часто выходят за пределы организации и объединяют между собой множество различных технологий, носителей идентификационных данных, принципов реализации защиты и моделей программирования. В рамках интегрированной системы организации требуется надежный и отвечающий современным стандартам механизм, определяющий не только принцип предоставления клиентам и партнерам своих услуг, но также и соблюдение политик безопасности, т. е. порядок доверия конкретным пользователям и организациям, предоставления и сохранности того или иного рода персональных данных и обработки соответствующих запросов.

Основные цели и задачи Управления федеративными отношениями:

- защищенное взаимодействие с другими организациями;
- надежный контроль данных и предоставление доступа доверенным источникам;
- возможность задать политики безопасности с доверенными организациями;
- обеспечение единого входа в систему (Single Sign-On).

Преимущества при его использовании:

- использование Active Directory в качестве главного репозитория идентификационных данных;
- обеспечение взаимодействия и контроль доступа к данным;
- прозрачность взаимодействия с разделением прав и ролей;
- максимальное использование имеющихся компенентов (служба каталога Active Directory и системы безопасности);
- усовершенствованная система безопасности за счет применения службы Active Directory Federation Services, токенов SAML и аутентификации по протоколу Kerberos.

1.1.4. Служба защиты информации (Active Directory Rights Management Services)

Основные цели и задачи данной службы (рис. 1.4):

- исключение неавторизованного доступа и компрометации конфиденциальной информации (отметим, что RMS предназначен для защиты информации вне сети/инфраструктуры владельца);
- снижение рисков, связанных с потерей конкурентноспособности организации.

Преимущества при ее использовании:

- повышение безопасности информации с помощью постоянной защиты данных;
- простое внедрение готового решения с возможностью интеграции с приложениями (Microsoft Office System) почтовой системы и службой каталога Active Directory;
- интеграция с продуктами третьих фирм с помощью использования комплекта разработчика (RMS SDK).

1.1.5. Служба управления идентификацией (Identity Lifecycle Management)

Основные цели и задачи службы управления идентификацией (рис. 1.5):

- простое и эффективное управление большим количеством цифровых удостоверений различных форматов;
- снижение рисков и стоимости владения при ручном управлении (provisioning и de-provisioning) идентификаторами пользователей (user identities);

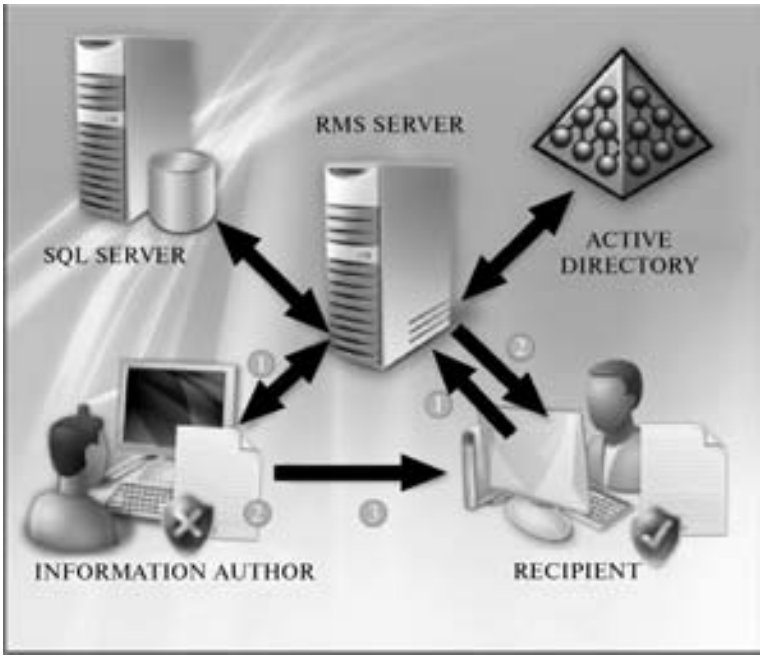

Рис. 1.4. Служба защиты информации

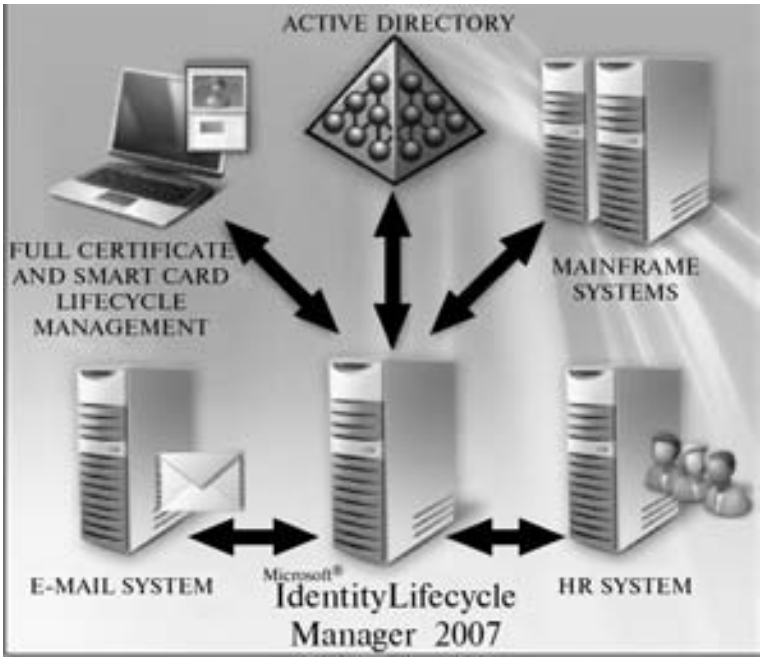

Рис. 1.5. Служба управления идентификацией

- упрощение управления средствами аутентификации пользователей, такими как смарт-карты и цифровые сертификаты;
- упрощение поддержки пользователей, например, при смене паролей.

Преимущества при ее использовании :

- реализация принципа «один пользователь — одна учетная запись в системе»;
- объединение управления всеми видами цифровых удостоверений и носителей;
- создание единого метакаталога организации;
- возможность автоматизации обслуживания и самообслуживания пользователей (например, при смене пароля или изменении PIN-кода смарт-карты).

1.1.6. Аутентификация в службе каталога Active Directory

Операционная система Windows Server по существу является платформой информационной системы. Поэтому изначально в нее заложены механизмы, реализующие защиту информации на всех уровнях:

- пользователь;
- рабочая станция;
- сеть;
- сервер;
- доступ во внешние сети, например — Интернет.

Весь инструментарий Windows, отвечающий за безопасность, можно сгруппировать по трем направлениям:

- аутентификация (проверка подлинности) субъектов;
- авторизация (контроль доступа субъектов к объектам);
- шифрование информационных хранилищ и потоков.

Работа любого пользователя в сети Windows Server 2003 начинается с обязательной аутентификации. По сути, аутентификация — это ответ на вопрос: «Кто ты и чем можешь это доказать?». Процесс аутентификации начинается с того, что пользователь сообщает системе свои регистрационные параметры, например, регистрационное имя и пароль.

Надо отметить, что регистрационное имя и пароль не являются надежным средством аутентификации, поэтому Microsoft рекомендует использовать средства многофакторной аутентификации пользователей.

Поскольку передавать пароль по сети небезопасно (он может быть перехвачен злоумышленником), необходимо обеспечить возможность подтверждения правильности пароля, введенного на рабочей станции пользователя, без передачи пароля по сети в открытом виде.

В семействе Windows Server 2003 реализованы следующие алгоритмы аутентификации:

- Lan Manager (LM);
- NTLM;
- NTLM v2;
- Kerberos v 5.

Windows Server 2003 также обеспечивает поддержку следующих протоколов:

- X.509 v3/Smartcard;
- проверка подлинности Digest;
- проверка подлинности .NET Passport;
- аутентификация удаленного пользователя — расширенный протокол EAP-TLS;
- аутентификация при установлении защищенного канала — протокол SSL/TLS;
- аутентификация хостов при установлении сеанса IP Security.

Использование протокола Lan Manager крайне нежелательно из-за его невысокой надежности. Вместе с тем, он нередко используется в сетях Active Directory. Это мотивируется необходимостью обеспечения «совместимости» с клиентами на основе Windows 9X. Однако, после установки клиента Active Directory Services (ADSC) в Windows 9X появляется возможность поддержки протокола аутентификации NTLM v2, что позволяет отказаться от использования LM в сети. Кроме того, установка клиента ADS предоставляет ряд других преимуществ, таких как поиск через Глобальный каталог, изменение пароля на любом контроллере домена и пр. В Windows NT 4.0 поддержка NTLM v2 появляется после установки пакета Service Pack 4.

Таким образом, в смешанной сети, где присутствуют pre-Windows 2000 компьютеры, для повышения безопасности аутентификации рекомендуется:

1) установить на все компьютеры Windows 9X клиент ADS;

2) установить на все компьютеры с Windows NT 4.0 пакет обновлений не ниже 4-го;

3) через групповую политику запретить использование LM и NTLM.

Дополнительную информацию см. в статье KB239869 на веб-узле корпорации Microsoft.

Наиболее защищенным является протокол аутентификации Kerberos, реализованный в ОС Microsoft, начиная с Windows 2000. Ниже перечислены его основные преимущества.

Более эффективная аутентификация на серверах. При аутентификации по протоколу NTLM серверу приложений приходится подключаться к контроллеру домена при проверке каждого клиента. С Kerberos такая необходимость отпадает — здесь аутентификация производится за счет проверки удостоверения, представленного клиентом. Индивидуальное удостоверение клиент получает от контроллера единожды, после чего может неоднократно использовать его на протяжении всего сеанса работы в сети.

Взаимная аутентификация. Протокол NTLM позволяет серверу идентифицировать своих клиентов, однако не предусматривает верификации сервера ни клиентами, ни другими серверами. Этот протокол разрабатывался для сетей, в которых все серверы считаются легитимными. В отличие от него, Kerberos такого допущения не делает, поэтому проверяет обоих участников сетевого подключения, каждый из которых в результате может точно узнать, с кем поддерживает связь.

Делегированная аутентификация. Когда клиент сети Windows обращается к ресурсам, службы операционной системы прежде всего производят его идентификацию. Во многих случаях для выполнения этой операции службе достаточно информации на локальном компьютере. Как NTLM, так и Kerberos, обеспечивают все данные, необходимые для идентификации пользователя на месте, однако иногда их бывает недостаточно. Некоторые распределенные приложения требуют, чтобы при подключении к серверным службам на других компьютерах идентификация клиента производилась локально службой самого этого клиента. Проблему помогает решить Kerberos, где предусмотрен специальный механизм представительских билетов, который позволяет на месте идентифицировать клиента при его подключении к другим системам. В протоколе NTLM такая возможность отсутствует.

Упрощенное управление доверительными отношениями. Одно из важных достоинств взаимной аутентификации по протоколу Kerberos состоит в том, что доверительные отношения между доменами Windows Server 2003 по умолчанию являются двусторонними и транзитивными. Благодаря этому в сетях с множеством доменов не придется устанавливать много явных доверительных отношений. Вместо этого все домены большой сети можно свести в дерево транзитивных отношений взаимного доверия. Удостоверение, выданное системой безопасности для любого домена, может приниматься во всех ветвях дерева. Если же сеть содержит несколько деревьев, то удостоверение любого из них будет приниматься по всему «лесу».

Совместимость. В основе своей реализации протокола Kerberos корпорация Microsoft использовала стандартные спецификации, рекомендованные группой IETF. Благодаря такому подходу удалось обеспечить аутентификацию клиентов Windows 2000/XP во всех сетях, которые поддерживают Kerberos 5.

Протокол Kerberos был создан в Массачусетском технологическом институте в рамках проекта Athena. Однако общедоступным этот протокол стал лишь после появления версии 4. После того как специалисты отрасли изучили новый протокол, его авторы разработали и предложили пользователям очередную версию — Kerberos v5, которая и была принята в качестве стандарта IETF (RFC 1510).

В Windows Server 2003 нашли применение расширения протокола Kerberos, упрощающие начальную аутентификацию клиентов. Обычно для этой цели используются секретные ключи, которыми должны заранее обменяться между собой участники сеанса, но теперь такую процедуру можно провести с помощью открытых ключей. Благодаря этому появилась возможность интерактивной регистрации пользователя с помощью смарт-карт. В основу расширений, обеспечивающих аутентификацию с открытым ключом, легла спецификация PKINIT.

Базовая концепция Kerberos. Описывает троих участников сетевого взаимодействия: клиент, пытающийся получить доступ к ресурсу, сервер, на котором расположен необходимый ресурс, и Центр распределения ключей (Key Distribution Center, KDC), выступающий в роли посредника между клиентом и сервером.

KDC выпускает специальные билеты (tickets), которые служат как бы «документами» в процессе аутентификации. Кроме того, в случае успешной аутентификации, в билет помещается информация, необходимая для последующей авторизации клиента при обращении к ресурсу.

Принцип работы протокола Kerberos. Для начала рассмотрим базовый принцип работы Kerberos. Протокол Kerberos активно использует технологии аутентификации, опирающиеся на «секреты для двоих». Основная идея довольно проста: если есть секретный ключ, известный только двоим, любой из его хранителей может легко удостовериться, что имеет дело именно со своим напарником. Для этого ему достаточно каким-либо способом проверить, знает ли собеседник их общий секретный ключ. Предположим, что некоторые клиент и сервер (и только они) обладают копией секретного ключа. Клиент формирует запрос на аутентификацию к серверу, помещает в этот запрос свое имя и текущее время и зашифровывает запрос своей копией ключа. Зашифрованная структура данных носит название аутентификатор (authenticator). Получив запрос, сервер расшифровывает его своей копией ключа и сравнивает метку времени из запроса с текущим временем на своих часах. Будем исходить из того, что часы на всех компьютерах сети синхронизированы. Если полученная метка времени расходится с текущим временем на сервере более чем на пять минут, аутентификатор отвергается. Если же время оказывается в пределах допустимого отклонения, можно с большой долей уверенности предположить, что аутентификатор поступил именно от данного клиента. Возможна однако и такая ситуация: кто-то перехватил предыдущую попытку клиента связаться с сервером и теперь пытается воспользоваться его аутентификатором. Но если на сервере сохранились записи о времени аутентификаторов, поступивших от данного клиента за последние пять минут, можно найти последний и отказаться от всех других сообщений, отправленных одновременно с ним или ранее. Иными словами, проверка временной метки позволяет существенно снизить вероятность перехвата и последующего подбора пароля.

Убедившись, что аутентификатор удалось расшифровать и временная метка в пределах допустимого, сервер формирует ответный пакет, помещает в него метку времени из аутентификатора клиента, зашифровывает пакет своей копией секретного ключа и отсылает клиенту.

Клиент получает ответ сервера, расшифровывает его, а затем сравнивает полученный результат со временем, которое было указано в исходном аутентификаторе. Если эти данные совпадают, можно быть уверенным, что аутентификатор дошел именно до требуемого сервера, и именно требуемый сервер на него ответил. Таким образом выполняется взаимная аутентификация клиента и сервера.

Остается решить одну проблему: каким образом безопасно передать клиенту и серверу (и только им) копии секретного ключа?

Для решения проблемы обмена ключами и был введен третий участник — посредник между клиентом и сервером. В протоколе Kerberos он называется KDC. KDC представляет собой службу, работающую на физически защищенном сервере. Эта служба ведет базу данных с информацией об учетных записях всех главных абонентов безопасности (security principals) своей области (realm) (области Kerberos в сетях Windows Server 2003 соответствует домен). Вместе с информацией о каждом абоненте безопасности в базе данных KDC сохраняется криптографический ключ, известный только этому абоненту и службе KDC. Данный ключ, который называют долговременным, используется для связи пользователя системы безопасности с центром распределения ключей. Долговременные ключи создаются на основе пароля пользователя. В реализации Microsoft функцию KDC выполняет контроллер домена (Domain Controller, DC).

Когда клиенту нужно обратиться к серверу, он прежде всего направляет запрос в центр KDC, который в ответ направляет каждому участнику предстоящего сеанса копии уникального сгенерированного именно для этой пары абонентов сеансового ключа (session key), действующие в течение короткого времени. Копия сеансового ключа, пересылаемая клиенту, шифруется с помощью долговременного ключа этого клиента, а направляемая серверу — долговременного ключа данного сервера.

Теоретически для выполнения функций доверенного посредника центру KDC достаточно направить сеансовые ключи непосредственно абонентам безопасности, как показано выше. Однако на практике реализовать такую схему чрезвычайно сложно. Прежде всего, серверу пришлось бы сохранять свою копию сеансового ключа в памяти до тех пор, пока клиент не свяжется с ним. А ведь сервер обслуживает не одного клиента, поэтому ему нужно хранить пароли всех клиентов, которые могут потребовать его внимания. В таких условиях управление ключами требует значительной затраты серверных ресурсов, что ограничивает масштабность системы. Нельзя забывать и о превратностях сетевого трафика. Они могут привести к тому, что запрос от клиента, уже получившего сеансовый пароль, поступит на сервер раньше, чем сообщение KDC с этим паролем. В результате серверу придется повременить с ответом до тех пор, пока он не получит свою копию сеансового пароля. Поэтому на практике применяется другая схема управления ключами, которая делает протокол Kerberos гораздо более эффективным.

В ответ на запрос клиента, который намерен подключиться к серверу, служба KDC направляет обе копии сеансового ключа клиенту. Сообщение, предназначенное клиенту, шифруется с помощью долговременного ключа клиента, а сеансовый ключ для сервера вместе с информацией о клиенте вкладывается в блок данных, получивший название сеансового билета (session ticket). Затем сеансовый билет целиком шифруется с помощью долговременного ключа сервера, который знают только служба KDC и данный сервер. После этого вся ответственность за обработку билета, несущего в себе зашифрованный сеансовый ключ, возлагается на клиента, который должен доставить его на сервер.

Обратите внимание, что в данном случае функции службы KDC ограничиваются выдачей билета. Ей больше не нужно следить за тем, все ли отправленные сообщения доставлены соответствующим адресатам. Даже если какое-нибудь из них попадет не туда, — ничего страшного не случится. Расшифровать клиентскую копию сеансового ключа может

только тот, кто знает секретный долговременный ключ данного клиента, а чтобы прочесть содержимое сеансового билета, нужен долговременный секретный ключ сервера.

Получив ответ KDC, клиент извлекает из него сеансовый билет и свою копию сеансового ключа, которые помещает в безопасное хранилище (оно располагается не на диске, а в оперативной памяти).

Когда возникает необходимость связаться с сервером, клиент посылает ему сообщение, состоящее из билета, который по-прежнему зашифрован с помощью долговременного ключа этого сервера, и собственного аутентификатора, зашифрованного с помощью сеансового ключа. Этот билет в комбинации с аутентификатором как раз и составляет удостоверение, по которому сервер определяет «личность» клиента.

Сервер, получив «удостоверение личности» клиента, с помощью своего секретного ключа расшифровывает сеансовый билет и извлекает из него сеансовый ключ, который затем использует для дешифрования аутентификатора клиента. Если все проходит нормально, делается заключение, что удостоверение клиента выдано доверенным посредником, то есть службой KDC. Клиент может потребовать у сервера проведения взаимной аутентификации. В этом случае сервер с помощью своей копии сеансового ключа шифрует метку времени из аутентификатора клиента и в таком виде пересылает ее клиенту в качестве собственного аутентификатора.

Одно из достоинств сеансовых билетов состоит в том, что серверу не нужно хранить сеансовые ключи для связи с клиентами. Они сохраняются в кэш-памяти удостоверений (credentials cache) клиента, который направляет билет на сервер каждый раз, когда хочет связаться с ним. Сервер, со своей стороны, получив от клиента билет, расшифровывает его и извлекает сеансовый ключ. Когда надобность в этом ключе исчезает, сервер может просто стереть его из своей памяти.

Такой метод дает еще одно преимущество: у клиента исчезает необходимость обращаться к центру KDC перед каждым сеансом связи с конкретным сервером. Сеансовые билеты можно использовать многократно. На случай же их хищения устанавливается срок годности билета, который KDC указывает в самой структуре данных. Это время определяется политикой Kerberos для конкретного домена. Обычно срок годности билетов не превышает 8 ч, т. е. стандартной продолжительности одного сеанса работы в сети. Когда пользователь отключается от нее, кэш-память удостоверений обнуляется, и все сеансовые билеты вместе с сеансовыми ключами уничтожаются.

Итак, в процедуре аутентификации используются:

- индивидуальный (он же долговременный) ключ компьютера (сервера и рабочей станции), который создается при включении компьютера в домен и хранится в Active Directory;
- сеансовый ключ, который генерируется KDC для конкретной пары абонентов безопасности, и используется при аутентификации.

При этом возникает вопрос: «Каким же образом клиент взаимодействует с KDC?». Ведь очевидно, что это взаимодействие также должно быть безопасным.

Когда пользователь проходит регистрацию, клиент Kerberos, установленный на его рабочей станции, пропускает введенный пароль через функцию хэширования. В результате формируется криптографический ключ, с помощью которого аутентификатор пользователя шифруется и затем пересылается ближайшему KDC. Получив запрос от клиента, KDC обращается в базу AD, находит в ней учетную запись нужного пользователя и извлекает из соответствующего ей поля долговременный ключ. Такой процесс — вычисление одной копии ключа по паролю и извлечение другой его копии из базы данных — выполняется всего лишь один раз за сеанс, когда пользователь входит в сеть впервые. Сразу же после получения пользовательского пароля и вычисления долговременного

ключа клиент Kerberos рабочей станции запрашивает сеансовый билет и сеансовый ключ, которые используются во всех последующих транзакциях с KDC на протяжении текущего сеанса работы в сети.

На запрос пользователя KDC отвечает специальным сеансовым билетом для самого себя, так называемый билет на выдачу билетов (ticket-granting ticket), или билет TGT. Как и обычный сеансовый билет, TGT содержит копию сеансового ключа для связи службы (в данном случае — KDC) с клиентом. В сообщение с билетом TGT также включается копия сеансового ключа, с помощью которой клиент может связаться с KDC.

Билет TGT шифруется с помощью долговременного ключа службы KDC, а клиентская копия сеансового ключа — с помощью долговременного ключа пользователя.

Получив ответ службы KDC на свой первоначальный запрос, клиент расшифровывает свою копию сеансового ключа, используя для этого копию долговременного ключа пользователя из своей кэш-памяти. После этого долговременный ключ, полученный из пользовательского пароля, можно удалить из памяти, поскольку он больше не понадобится: вся последующая связь с KDC будет шифроваться с помощью сеансового ключа. Как и все другие сеансовые ключи, он имеет временный характер и действителен до истечения срока действия билета TGT либо до выхода пользователя из системы. По этой причине такой ключ называют сеансовым ключом регистрации (logon session key).

С точки зрения клиента билет TGT почти ничем не отличается от обычного. Перед подключением к любой службе, клиент, прежде всего, обращается в кэш-память удостоверений и извлекает оттуда сеансовый билет для этой службы. Если его нет, он начинает искать в этой же кэш-памяти билет TGT. Найдя его, клиент извлекает оттуда же соответствующий сеансовый ключ регистрации и готовит с его помощью аутентификатор, который вместе с TGT высылает в KDC. Одновременно туда направляется запрос на сеансовый билет для требуемой службы.

По аналогии с аутентификацией на сервере аутентификация при входе в домен использует индивидуальный (долговременный) ключ пользователя, сеансовый ключ для связи пользователя и KDC и, наконец, долговременный ключ самого KDC, формируемый на основе учетной записи krbtgt, имеющейся на каждом DC.

В реализации Windows Server 2003 Kerberos содержит в себе три подпротокола. Первый из них используется службой KDC для передачи клиенту сеансового ключа регистрации и билета TGT. Он называется Authentication Service Exchange (обмен со службой аутентификации) или, сокращенно AS Exchange. Второй подпротокол под названием Ticket-Granting Service Exchange (обмен со службой выдачи билетов) или TGS Exchange служит для рассылки служебных сеансовых ключей и сеансовых ключей самой службы KDC.

Третий подпротокол Client/Server Exchange (клиент-серверный обмен) или CS Exchange используется клиентом для пересылки сеансового билета доступа к службам.

Такое разделение труда позволяет применять протокол Kerberos и за пределами его «родного» домена. Клиент, получивший билет TGT из службы аутентификации одного домена, может воспользоваться им для получения сеансовых билетов в службах выдачи билетов других доменов. Наладить аутентификацию между доменами нетрудно, для этого достаточно договориться о едином междоменном ключе (Inter-Realm key). В Windows Server 2003 такой ключ генерируется автоматически, когда между доменами устанавливаются доверительные отношения. Служба выдачи билетов каждого домена регистрируется в центре KDC другого домена в качестве главного абонента безопасности. В результате служба выдачи билетов каждого домена начинает рассматривать службу выдачи билетов второго домена, как еще одну свою службу. Благодаря этому клиент, прошедший аутентификацию и зарегистрировавшийся в системе, может запрашивать и получать сеансовые билеты для нее.

Теперь рассмотрим, что происходит, когда пользователь с учетной записью в домене West запрашивает доступ к серверу из домена East. Прежде всего, клиент Kerberos, установленный на рабочей станции этого пользователя, посылает запрос в службу выдачи билетов своего домена, в котором просит выдать сеансовый билет для доступа на нужный сервер. Служба выдачи билетов домена West проверяет список своих абонентов безопасности и убеждается, что такого сервера среди них нет. Поэтому она направляет клиенту так называемый билет переадресации (referral ticket), который представляет собой TGT, зашифрованный с помощью междоменного ключа, общего для служб KDC доменов West и Company. Получив билет переадресации, клиент использует его для подготовки другого запроса на сеансовый ключ. Однако на этот раз запрос пересылается в службу выдачи билетов домена Company, откуда в ответном пакете приходит билет переадресации для домена East, зашифрованный с помощью междоменного ключа, общего для служб KDC доменов Company и East. Наконец, направляется запрос на сеансовый ключ в домен, где находится учетная запись нужного сервера, то есть, в домен East. Его служба выдачи билетов пытается расшифровать билет переадресации с помощью собственной копии междоменного ключа. Если попытка удается, центр KDC направляет клиенту сеансовый билет на доступ к соответствующему серверу своего домена.

Определенную сложность для протоколов аутентификации создают многоуровневые клиент-серверные приложения. Здесь клиент может подключаться к серверу, который, в свою очередь, должен будет подключиться к другому серверу более высокого уровня. Для этого первому серверу понадобится билет на подключение ко второму. В идеале такой билет должен ограничивать доступ первого сервера ко второму лишь теми функциями, на которые клиент имеет права.

Для решения этой проблемы в протоколе Kerberos имеется специальный механизм — так называемое делегирование аутентификации. По существу в такой ситуации клиент поручает свою аутентификацию серверу. С этой целью он уведомляет службу KDC о том, что данный сервер имеет право представлять клиента. Такой подход называется *имперсонацией* (concept of impersonation).

Делегирование аутентификации возможно двумя способами. Во-первых, клиент может получить билет на подключение к серверу высшего уровня, а затем передать его ближайшему серверу. Билеты, полученные таким способом — клиентом для ближайшего сервера — называются *представительскими* (proxy tickets). Однако на этом пути имеется одна серьезная трудность: чтобы получить представительский билет, клиенту нужно знать имя сервера высшего уровня. Решить проблему помогает второй способ делегирования аутентификации. Здесь клиент передает на ближайший к нему сервер свой билет TGT, который тот по мере необходимости использует для запроса собственных билетов. Билеты TGT, полученные таким образом, т. е. по удостоверению клиента, называются *передаваемыми* (forwarded tickets). Какой из описанных способов применяется службой KDC, зависит от политики Kerberos.

Необходимо отметить, что предложенная в Kerberos схема зависит от сложности используемых паролей. Повысить надежность аутентификации позволяет применение смарт-карт и криптографии с открытым ключом. На смарт-карте хранятся личный ключ пользователя и цифровой сертификат с открытым ключом. Для доступа к личному ключу необходимо ввести уникальный для данной карты PIN-код (Personal Identification Number).

Повышение безопасности при использовании смарт-карт обусловлено несколькими факторами.

Во-первых, все операции с ключами выполняются непосредственно на смарт-карте, ключи никогда не хранятся в файловой системе компьютера и скомпрометировать их гораздо сложнее.

Во-вторых, аутентификация становится двухфакторной, т. е., чтобы зарегистрироваться в системе, необходимо:

1) обладать смарт-картой;

2) знать PIN-код.

В Windows Server 2003 аутентификация с помощью смарт-карт по протоколу Kerberos реализована с помощью расширения, называемого PKINIT.

PKINIT предусматривает следующий порядок использования пары ключей пользователя. Открытый ключ служит для шифрования сеансового ключа пользователя службой KDC, а личный — для расшифровывания этого ключа клиентом.

Регистрация начинается с того, что пользователь вставляет свою смарт-карту в специальное считывающее устройство, подключенное к компьютеру, и вводит PIN-код. Windows использует PIN-код пользователя для доступа к смарт-карте, где хранятся секретный ключ пользователя и сертификат X.509 v3, содержащий открытый ключ пары. В дальнейшем все криптографические операции с использованием данной пары будут производиться через смарт-карту.

Kerberos SSP клиентского компьютера направляет в службу KDC сообщение KRB_AS_REQ — первоначальный запрос на аутентификацию. В поле данных предварительной аутентификации этого запроса включается сертификат открытого ключа пользователя. Аутентификатор подписывается личным ключом пользователя. KDC проверяет подлинность сертификата и извлекает из него открытый ключ, которым проверяет корректность аутентификатора.

1.2. Авторизация при доступе к объекту

Итак, аутентификация однозначно идентифицирует субъект. Проще говоря, после успешной аутентификации система понимает, кто к ней обращается. Следующий шаг — выяснить, какими правами обладает данный субъект. Эту задачу решает механизм авторизации. Главные составляющие процесса авторизации — маркер доступа (access token), связанный с субъектом (пользователем), и дескриптор безопасности (security descriptor), связанный с объектом, к которому пользователь пытается обратиться.

Маркер доступа представляет собой структуру данных, в которую помещается идентификатор безопасности пользователя (Security Identifier, SID), SID всех групп, членом которых он является, а также список привилегий (User Rights), которыми пользователь обладает.

Напомним, что маркер доступа помещается в специальный раздел сеансового билета при аутентификации. Причем при входе в домен в маркере будет содержаться информация о членстве в локальных группах рабочей станции, в которой пользователь зарегистрировался. DC добавит в маркер сведения о членстве в глобальных и универсальных группах. А при обращении к конкретному компьютеру в сети маркер пополнится информацией о членстве в локальных группах этого компьютера.

Права доступа на объект перечислены в дескрипторе безопасности, связанном с этим объектом. В Windows Server 2003 дескрипторами безопасности обладают:

- общие папки (shared folders);
- принтеры;
- файлы и папки на разделах NTFS;
- все объекты Active Directory.

Собственно дескриптор безопасности представляет собой структуру данных, состоящую из двух списков управления доступом: Discretionary Access Control List (DACL) и System Access Control List (SACL). Оба списка имеют одинаковую структуру и, в свою очередь, состоят из набора элементов Access Control Entry (ACE). Однако ACE списка DACL содержит назначение прав для конкретного SID, в то время как ACE списка SACL указывает, какие действия конкретного SID должны протоколироваться системой аудита. Заметим, что DACL объекта Active Directory может содержать строки ACE, назначенные отдельным атрибутам. Тем самым в Active Directory администратор может назначать права доступа не только на уровне объекта, но и на уровне конкретного атрибута объекта. Например, можно разрешить/запретить редактирование номера рабочего телефона для пользователей такого-то подразделения.

В Active Directory и в файловой системе NTFS реализован механизм наследования прав доступа. Наследование позволяет существенно упростить назначение прав доступа в указанных иерархических структурах. По умолчанию, объект, создаваемый на каком-либо уровне иерархии, например, файл File.doc, унаследует права доступа с родительского уровня, что избавляет администратора от необходимости явно указывать права на объект. С другой стороны, администратор всегда может на любом уровне иерархии отключить наследование и задавать права доступа явным образом. В общем случае ACL объекта состоит из унаследованных с верхнего уровня списков управления доступом плюс прав, заданных непосредственно для данного объекта (явные назначения). Такой механизм формирования списков позволяет эффективно делегировать полномочия в каталоге AD.

ACE может содержать как разрешающее так и запрещающее право доступа, например, запрет на операцию записи. Запрещающее право доступа имеет приоритет, причем неважно, назначен запрет непосредственно пользователю или группе, членом которой он является.

Если при просмотре списка DACL выясняется, что пользователь не имеет доступа к объекту (встретился запрещающий ACE, содержащий SID пользователя или одной из его групп), то дальнейший просмотр списка прекращается.

Таким образом, для повышения эффективности Windows Server 2003 упорядочивает элементы ACE следующим образом:

- явные запреты;
- явные разрешения;
- унаследованные запреты;
- унаследованные разрешения.

Сумма полномочий пользователя после просмотра списка — личных, групповых, явных, унаследованных — образует его эффективные права.

1.3. Система аудита Active Directory

Даже если мы уверены в том, что в нашей сети используется надежный и безопасный протокол аутентификации, а списки управления доступом корректно настроены, мы, конечно же, хотим знать, кто и когда пытался проникнуть в нашу систему, кто и когда пытался получить доступ к папке с важной конфиденциальной информацией, удалось это злоумышленнику или нет. Ответы на эти и другие вопросы нам поможет получить система аудита.

При настройке аудита администратор должен указать, какие типы событий его интересуют и на каких машинах. После чего система аудита начинает отслеживать указанные события и фиксировать их в специальном журнале аудита — Security Log. Для каждого типа событий администратор может указать, интересуют ли его факты успешного завершения события, неуспешного или и те, и другие. Начиная с Windows 2000, аудит включается в объектах групповой (локальной) политики, причем в Windows Server 2003 аудит определенных действий включен по умолчанию.

Параметров аудита довольно много, и у начинающих администраторов часто возникает вопрос, какие конкретно опции следует включать. Строго говоря, это определяется целым набором критериев, таких как роль, выполняемая данным компьютером (рабочая станция, сервер приложений, контроллер домена), условия его эксплуатации (локальная сеть, демилитаризованная зона, сеть за пределами периметра), требования политики безопасности предприятия и т. д. Тем не менее в руководствах «Windows Server 2003 Security Guide» и «Windows XP Security Guide» даны некоторые общие рекомендации по настройке данных систем, а в прилагаемых к ним шаблонах безопасности можно найти примеры настроек аудита.

В систему управления можно включить все доступные параметры политики аудита. Некоторые из них используются довольно редко. Например, «Аудит отслеживания процессов» используется в основном для целей отладки и практически не применяется при администрировании. «Аудит доступа к службе каталогов» имеет смысл включать только на контроллерах доменов. Обратите внимание, что «Аудит доступа к службе каталогов» и «Аудит доступа к объектам» недостаточно просто включить в данной консоли.

Поскольку задача этих политик — отслеживать действия, совершаемые с объектами соответственно AD, NTFS и принтеры, то администратор должен еще указать:

1) какие конкретно объекты его интересуют (папка, файл, подразделение в AD);

2) чьи действия в отношении выбранных объектов необходимо протоколировать (например, пользователя Иванова и пр.);

3) наконец, какие конкретно действия следует заносить в журнал (чтение файла, удаление папки и пр.).

Технически эти настройки реализованы в виде списка System Access Control List (SACL), аналогичного по структуре списку прав доступа.

Аудит доступа к объектам может быть настроен довольно тонко. При этом работает механизм наследования, и выбранные параметры можно легко распространить на все уровни иерархии объектов.

После настройки требуемых параметров политики аудита администратору необходимо периодически просматривать журнал аудита и анализировать собранную информацию. Просмотр осуществляется стандартным образом с помощью утилиты Event Viewer (просмотр событий). Security Log хранит только информацию, собранную системой аудита. Естественно, что в зависимости от настроек записей в журнале может быть очень много. Для отображения только необходимой в данный момент информации можно использовать фильтры по различным критериям. Кроме того, следует еще до включения аудита изменить размер журнала, который по умолчанию всего 512 Кбайт, и указать алгоритм поведения системы при заполнении журнала. Для критически важных компьютеров рекомендуется не переписывать журнал, чтобы не терять записи, которые могут оказаться весьма важными для анализа потенциальных или возникших проблем. Более того, в объекте групповой или локальной политики существует настройка, согласно которой компьютер принудительно выключается, если журнал аудита переполняется и фиксировать события становится невозможно.

Поскольку Security Log является важной составляющей системы безопасности, содержимое журнала хранится в зашифрованном виде. По умолчанию настройка аудита разрешена только членам группы «Administrators», а рядовой пользователь не имеет даже права чтения журнала аудита. Пользователь, наделенный соответствующими полномочиями, может выполнять очистку и архивацию журнала аудита. При этом надо иметь в виду, что удаление отдельных событий журнала невозможно. Система фиксирует факт очистки журнала с указанием того, кто и когда выполнил очистку.

1.4. Назначение и решаемые задачи инфраструктуры открытых ключей

Система строгой двухфакторной аутентификации пользователей основана на применении методов асимметричной криптографии и использует в качестве атрибутов аутентификации цифровые сертификаты открытых ключей формата X.509, размещенные на персональных смарт-картах или USB-ключах пользователей. Централизованное применение сертификатов открытых ключей требует наличия в составе информационной системы организации инфраструктуры открытых ключей (Public Key Infrastructure, PKI), обеспечивающей выпуск и дальнейшее сопровождение цифровых сертификатов.

К основным задачам инфраструктуры открытых ключей (PKI) относятся:

- централизованное формирование, управление и хранение сертификатов открытых ключей;
- предоставление доступа прикладным информационным системам к сертификатам открытых ключей и спискам аннулированных сертификатов (Certificate Revocation List, CRL);
- поддержка многофакторной (двухфакторной) аутентификации пользователей в домене службы каталога, при доступе к корпоративным веб-ресурсам, а также поддержка шифрования и ЭЦП при обмене электронными сообщениями.

Дополнительно к PKI часто предъявляются следующие требования:

- интеграция с применяемой в организации службой каталога;
- обеспечение возможности гибкого масштабирования PKI с целью интеграции с новыми корпоративными прикладными системами и распределения нагрузки;
- поддержка основных промышленных стандартов PKI, используемых в приложениях со встроенными средствами работы с PKI:

— семейство стандартов X.509;

— стандарты серии PKCS;

— криптографические алгоритмы RSA, SHA-1, MD5;

— российские государственные стандарты в области криптографической защиты информации — ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94, ГОСТ 28147-89;

— протокол LDAP v2.

Удостоверяющий центр на Windows Server 2003 и 2008 может поддерживать следующие конфигурации:

- отдельный удостоверяющий центр либо полная интеграция с Active Directory;
- корневой или подчиненный удостоверяющий центр.

Обычно таких возможностей оказывается достаточно для решения большинства задач в организации.

1.5. Управление идентификацией (ILM)

Централизованная система управления идентификацией, представленная службами каталогов, не означает, что вся информация будет содержаться в центральном месте, она будет только управляться централизованно. В типичном решении различные данные идентификации управляются различными группами организации. Например, группе трудовых ресурсов требуется добавить новых работников, менеджерам нужно иметь возможность устанавливать отношения с деловыми партнерами, а администраторам необходимо иметь возможность управлять доступом к ресурсам.

Типичные проблемы:

- необходимость работать с различными хранилищами информации о пользователях;
- в сети имеется несколько систем с разными средствами аутентификации;
- растет число пользователей, использующих цифровые сертификаты;
- растет число выпущенных сертификатов.

В таких ситуациях одним из важнейших элементов управления является управление сертификатами (Certificate Lifecycle Management — CLM) и управление идентификационной информацией в гетерогенной среде (Identity Lifecycle Management — ILM).

Появляется задача обеспечения управления цифровыми удостоверениями и обеспечения единой аутентификации для поддержки принципа Single Sign-on и надежной защиты данных.

Решение для интеграции различных источников данных идентификации, имеющихся в организации, — использовать продукт синхронизации каталогов, например, продукт метакаталогов.

Метакаталоги помогают создать единое представление для отдельных данных идентификации, хранящихся в разных хранилищах. Они берут информацию о пользователе из различных утвержденных источников, таких как приложения трудовых ресурсов и учета, каталоги электронной почты и регистрационные базы данных веб-серверов, и заполняют каталог, чтобы создать такое представление. Самое главное заключается в том, что метакаталоги синхронизируют значения данных, предоставляемые каждым из утвержденных источников организации.

Для решения этих задач компания Microsoft выпустила продукт Identity Lifecycle Manager 2007, состоящий из двух компонентов (фактически, независимых продуктов):

- Certificate Lifecycle Manager (CLM);
- Microsoft Identity Integration Server (MIIS).

CLM позволяет организовать управление большим количеством цифровых удостоверений и носителей различных форматов и упростить поддержку пользователей с помощью портала самообслуживания.

Microsoft Identity Integration Server (MIIS) обеспечивает возможность интегрировать данные идентификации по многим репозиториям, системам и платформам.

1.6. Microsoft Identity Integration Server (MIIS)

MIIS поставляется с набором «коннекторов» (рис. 1.6), позволяющих клиенту интегрировать информацию по идентификации из множества различных источников, являющихся каталогами сетевой операционной системы, электронной почты или приложений, баз данных или форматированных текстовых файлов. MIIS также поддерживает производные форматы данных Интернета, такие как XML и DSML.

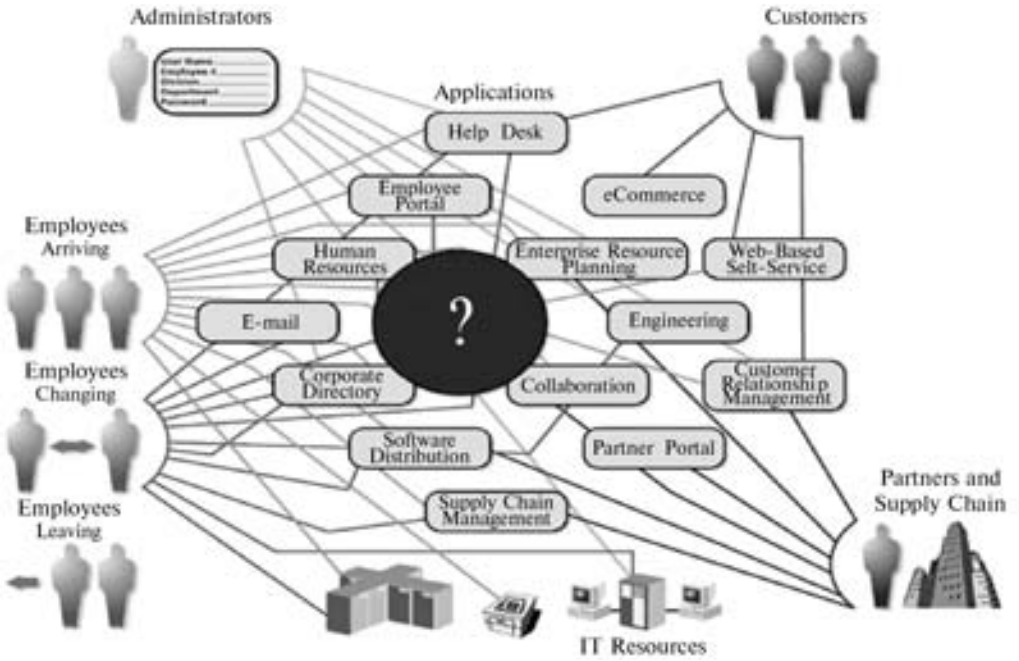

Рис. 1.6. MIIS с набором «коннекторов»

MIIS добавляет Active Directory, обеспечивая клиента широкими возможностями взаимодействия.

Классический «метакаталог»

- ○ Синхронизация атрибутов между множеством систем:
- множество каталогов LDAP: AD, ADAM, iPlanet, Novell;
- множество почтовых систем: Exchange (5.5, 2000, 2003), Notes;
- кадровые системы: SAP, PeopleSoft, Oracle HR;
- наследуемые системы (мэйнфреймы, Unix, и т.д.): обмен файлами, XML.

Управление паролями

- ○ Задание начального пароля, задание/изменение множества паролей одновременно.
- ○ Автоматическое распространение
- Автоматическое создание или запрет/удаление учётных записей/почтовых ящиков.

Multi-forest Active Directory

- ○ Сайты, подсети, принтеры, синхронизация реального времени.

Сценарии электронной почты

- Создание глобального списка рассылки (Global Address List):
- Объединение множества лесов Exchange, множества почтовых систем;
- Автоматизированное управление группами.

1.7. Системы обеспечения

Ключевая часть решений по управлению доступом и учетными записями — способ создания, изменения и удаления идентификационных данных. Этот жизненный цикл управления идентификацией обычно описывается как обеспечение. Оно использует информацию пользователя, содержащуюся в инфраструктуре каталогов организации, чтобы ускорить выдачу и аннулирование пользовательских учетных записей и прав доступа к информационным ресурсам: электронную почту, телефонную службу, приложения, трудовые ресурсы, бизнес-линейку, функциональные приложения, допуск в интрасеть и внешнюю сеть, а также сервисы службы поддержки.

Автоматизация данных процессов может снизить затраты и серьезно увеличить производительность. Например, подсчитано, что простое действие по автоматизации сбрасывания паролей составляет 48 % обращений в службу поддержки для организаций с 10 000 пользователей и более. Кроме того, автоматизация процессов может сократить время, требуемое для получения пользовательских учетных записей и прав доступа, более чем с недели до нескольких часов. Это также сильно снижает время, затрачиваемое управляющими делами на заполнение сопутствующей документации, так же как и время, затрачиваемое персоналом отдела финансов, отдела трудовых ресурсов и отдела ИТ на подтверждение и выполнение запросов на доступ.

Удаление и повторное обеспечение — другие ключевые функции систем обеспечения. Если работник покидает или меняет свою должность, система обеспечения может быстро изменить или аннулировать учетные записи и пользовательские права доступа.

Как говорилось выше, корпорация Microsoft обеспечивает данный уровень функциональных возможностей как часть MIIS. В перспективе системы обеспечения MIIS позволяют:

- «встроенным» работникам — автоматическое создание учетных записей в связанных системах, основанных на «триггерах» или событиях, таких, как приглашение на работу и добавление к системе трудовых ресурсов или другой официальной системе;
- «невстроенным» работникам — автоматическое удаление или приостановка учетных записей в связанных системах, когда работник удаляется из системы трудовых ресурсов или другой официальной системы;
- атрибутам идентификации «Брокер» — автоматическое создание или синхронизация данных идентификации между двумя или множеством систем.

Автоматизация деловых процедур — другая важная возможность системы обеспечения, которая используется больше всего во время встраивания работника. При встраивании нового работника компания может использовать MIIS для предоставления:

- простого обеспечения — работник впускается в различные связанные системы, которые для него открыты;
- одношагового обеспечения автоматизации деловых процедур — за один шаг менеджер или другое уполномоченное лицо уведомляется по электронной почте о том, что новый работник приглашен на работу и готов к обеспечению. Менеджер или

уполномоченное лицо выдает свое решение (да/нет), и учетные записи работника автоматически создаются или не создаются в зависимости от решения;

- многошагового обеспечения автоматизации деловых процедур — сходного с обеспечением автоматизации деловых процедур, исключая количество более одного работника в процессе обеспечения, который должен авторизовать новое приглашение на работу. Многошаговая автоматизация деловых процедур возможна при использовании BizTalk Server вместе с MIIS4;
- комплексное обеспечение — более редкий сценарий, в котором телефон, кредитная карта, пейджер или другие элементы внесистемной учетной записи работника обеспечиваются как часть процесса встраивания. Вместе со специализированными продуктами третьих фирм (т. е. Business Layers) MIIS может выполнять необходимые сложные задачи обеспечения.

MIIS предоставляет широкий набор возможностей обеспечения «из коробки» для удовлетворения нужд компании. Компании, для которых требуются возможности, превосходящие предоставляемые MIIS сегодня, могут выиграть от использования BizTalk Server или продуктов от различных партнеров корпорации Microsoft.

Для MIIS 2003 имеются следующие агенты управления (коннекторы):

- AD/Exchange 2000/Exchange 2003;
- Active Directory Application Mode (ADAM);
- Active Directory global address list (GAL);
- SunOne Directory Server 5.1 (iPlanet);
- SQL;
- Oracle8i Database / Oracle9i Database;
- NT4;
- Exchange 5.5;
- Microsoft Exchange Server 5.5 (bridgehead server);
- Lotus Notes 4.6 и 5.0;
- Novell eDirectory 8.62/8.7;
- Netscape Directory Server 6.1;
- Informix, DB2, dBase, Access, Excel, OLE DB через SQL DTS;
- LDAP Directory Interchange Format (LDIF);
- текстовый файл с разделителями;
- текстовый файл с полями фиксированной ширины;
- Directory Services Markup Language (DSML) 2.0;
- текстовый файл, состоящий из пар «атрибут + значение».

В заключение отметим, что список коннекторов постоянно расширяется.

Глава 2
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДОСТУПА К ДАННЫМ И ПРИЛОЖЕНИЯМ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНИЗАЦИИ НА ОСНОВЕ РЕКОМЕНДАЦИЙ И ПРОДУКТОВ ORACLE И ALADDIN. ТИПОВЫЕ РЕШЕНИЯ

2.1. Управление доступом в СУБД Oracle с помощью встроенных механизмов безопасности и криптографических средств защиты

2.1.1. Методы аутентификации в СУБД Oracle

Аутентификация в СУБД Oracle означает проверку подлинности субъекта (пользователя, приложения, устройства), которому требуется доступ данным, ресурсам или приложениям. СУБД Oracle предоставляет множество способов аутентификации и позволяет использовать один или несколько методов одновременно. В СУБД Oracle возможна аутентификация:

- средствами операционной системы;
- с помощью сетевых сервисов;
- средствами базы данных (БД);
- в многозвенных приложениях.

Аутентификация средствами операционной системы

Некоторые операционные системы позволяют СУБД Oracle использовать ту информацию о пользователях, которой они управляют. Это создает следующие преимущества:

- аутентификация может проходить без указания имени пользователя и пароля (например, пользователь, прошедший аутентификацию в ОС, может загрузить приложение SQL*Plus, выполнив команду: SQLPLUS /);
- при записи событий аудита средствами ОС и СУБД можно использовать одно и то же имя пользователя;
- сервер БД не должен хранить пароли и управлять ими (хотя необходимость хранения имен пользователей сохраняется).

Однако при этом возникают проблемы в распределенных системах, использующих различные ОС.

Аутентификация с помощью сетевых сервисов

Среди встроенных в СУБД Oracle средств защиты можно выделить опцию Oracle Advanced Security (OAS) — комплекс средств защиты данных, аутентификации и обеспечения сетевой безопасности, включающий поддержку защищенных протоколов передачи данных. Опция Oracle Advanced Security обеспечивает конфиденциальность информации, передаваемой по сети, исключая «прослушивание» и разнообразные виды атак. OAS позволяет защищать все входящие и исходящие соединения СУБД Oracle. Для каждого соединения создается секретный ключ, обеспечивающий безопасность сетевого трафика. OAS делает невозможным скрытую модификацию, добавление или удаление части передаваемых данных.

В Oracle Advanced Security предусмотрена аутентификация службами третьих сторон:

- Kerberos;
- Entrust/PKI;
- Remote Authentication Dial-In User Service (RADIUS);
- службой LDAP-каталога.

OAS позволяет организации использовать существующую инфраструктуру безопасности, например Kerberos, PKI, RADIUS для сильной аутентификации в СУБД Oracle 10g.

Аутентификация службами третьих сторон

Kerberos

Kerberos — система аутентификации доверенной третьей стороной, основанная на использовании сервером аутентификации и субъектом так называемого общего секретного ключа. Она гарантирует безопасность коммуникаций и надежность доверенной стороны. Kerberos обеспечивает однократную регистрацию, централизованное хранение паролей, прозрачную аутентификацию через связи БД, а также средства усиленной безопасности на рабочих станциях.

PKI

Аутентификация на основе цифровых сертификатов опирается на инфраструктуру открытых ключей (PKI) — современную технологию, использующую для идентификации субъектов в распределенной среде криптографию с открытыми ключами. При этом не требуется специального сервера аутентификации. Аутентификация пользователей (приложений) выполняется на серверах БД в рамках предприятия. СУБД Oracle располагает следующими возможностями и компонентами для аутентификации с помощью цифровых сертификатов:

- аутентификация и безопасная передача сеансовых ключей по SSL-протоколу;
- набор функций OCI (Oracle Call Interface — прикладного интерфейса доступа к БД) и PL/SQL, Java-библиотеки;
- доверенные сертификаты (trusted certificates) для проверки подлинности сертификатов, предъявляемых пользователями (приложениями);
- контейнеры Oracle wallets, содержащие секретные ключи пользователей, их сертификаты и цепочки доверенных сертификатов;
- Oracle Wallet Manager (OWM) — компонент СУБД для управления контейнерами.

RADIUS

Служба удаленной аутентификации пользователей по коммутируемой линии (Remote Access Dial-In User Service, RADIUS) фактически является стандартом (RFC 2138) для централизованной аутентификации и авторизации пользователей в крупных вычислительных сетях. СУБД Oracle поддерживает протокол RADIUS, при этом становятся доступны службы и устройства аутентификации третьих производителей, с которыми может взаимодействовать сервер RADIUS (например, устройства генерации одноразовых паролей, биометрические устройства и т. п.).

Аутентификация службой LDAP-каталога

Эффективное управление аутентификацией и учетными записями пользователей (приложений) может быть обеспечено с помощью службы LDAP-каталога. В инфраструктуре СУБД Oracle служба каталога представлена следующими компонентами:

- Oracle Internet Directory (OID) — специализированное хранилище информации на основе базы данных Oracle и тесно интегрированное с сетевыми службами и управляющими средствами Oracle. Oracle Internet Directory позволяет централизованно хранить информацию о пользователях (создавать одну учетную запись пользователя для многих баз данных). OID обеспечивает интеграцию со службами каталогов других производителей, например, MS Active Directory или iPlanet, позволяет гибко управлять атрибутами безопасности и привилегиями каждого пользователя, включая тех, кто для аутентификации применяет цифровые сертификаты. Для повышения безопасности соединений во время аутентификации может использоваться протокол SSL.
- Oracle Enterprise Security Manager — утилита управления приложениями, пользователями, группами, ролями и привилегиями.

Аутентификация средствами базы данных

СУБД Oracle может аутентифицировать пользователя (приложение), используя информацию, хранимую в базе данных. Если субъектом аутентификации является пользователь, то для проверки его подлинности может запрашиваться некоторая дополнитель-

Таблица 2.1

Особенности способов аутентификации в СУБД Oracle 9i/10g

Способ	*Хранение ключей*	*Преимущества*	*Недостатки*
Имя/пароль	БД	• Распространенность • Возможность выбора любой платформы клиента/сервера • Простота использования • Возможность задать правила формирования пароля (качество пароля)	• Пароль либо легко подбирается, либо сложно запоминается • Пароль доступен для компроментации
Kerberos	Файл	• Шифрование ключевой информации • Возможность временнОго ограничения действия ключа • Поддержка однократной регистрации Single Sign-On • Поддержка смарт-карт технологий	• Требуется дополнительная настройка сервера на протокол Kerberos • Небезопасное хранение ключей • Управление ключевой информацией не средствами Oracle
RADIUS	Файл/ Внешняя БД	• Сильная аутентификация • Возможность сочетать двухфакторную аутентификацию с другими методами • Возможность интеграции с любыми технологиями, поддерживающими данный протокол (TokenCard, SecurID, биометрические устройства) • Возможность выбора любой платформы клиента/сервера	• Возможность компрометации ключевой информации • Недостаточная надежность UDP-протокола • Требуется установка RADIUS-сервера • Возможно, потребуется дополнительное кодирование для клиента • Не рекомендуется использовать карты SecurID с версии 9i Oracle
SSL/PKI	Файл/Реестр/ Смарт-карта	• Двухфакторная аутентификация • Возможность централизованного управления пользователями и приложениями, а также ключевой информацией • Возможность выбора любой платформы клиента/сервера • Поддержка однократной регистрации Single Sign-On	• Возможность компрометации ключей при хранении в файле/реестре • Подтверждено со стороны Oracle только использование смарт-карт NCipher • При использовании смарт-карт других производителей требуется дополнительное ПО

ная информация, например, пароль. Пользователь может изменить собственный пароль в любое время. Информация о пользователе и пароле хранится в словаре БД, причем пароль криптографически защищен от несанкционированной модификации.

Программное обеспечение СУБД Oracle шифрует пароли пользователей в целях безопасной передачи по сети. После прохождения процедур аутентификации и авторизации субъекты могут выполнять свои роли и полномочия. Аутентификация администраторов СУБД Oracle требует специальной процедуры, что обусловлено спецификой выполняемых ими задач.

Аутентификация средствами БД (табл. 2.1) обеспечивает следующие возможности:

- шифрование пароля во время соединения (с помощью симметричного алгоритма шифрования Advanced Encryption Standard (AES), также известного, как Rijndael);
- блокирование учетной записи (возможна остановка числа неправильных попыток ввода пароля, а также варианта разблокировки, например, вручную администратором БД, автоматически через некоторое время и т. п.);
- управление жизненным циклом пароля;
- хранение истории паролей (это позволяет, например, отслеживать повторяющиеся варианты паролей);
- управление качеством паролей (проверка пароля на соответствие некоторым требованиям по качеству — длине, используемым символам, несовпадению со словарем и т. п.).

Аутентификация в многозвенных приложениях Enterprise User Security

Стандартный механизм аутентификации и авторизации в СУБД Oracle предполагает, что каждому пользователю соответствует учетная запись. Таким образом, если пользователь работает с несколькими базами данных, то в каждой хранится его учетная запись. В результате при большом количестве серверов баз данных происходит многократное дублирование учетной информации, что естественно усложняет процесс администрирования и увеличивает риски безопасной эксплуатации приложений.

Подобных проблем позволяет избежать подход, предлагаемый Oracle в решении **Enterprise User Security**: учетные записи пользователей создаются в едином LDAP-каталоге — Oracle Internet Directory, а ведение ролей пользователей, которым предоставляются необходимые привилегии, происходит в различных базах данных. При этом аутентификация и авторизация пользователей СУБД Oracle выполняются на основе информации LDAP-каталога и правил соответствия (mapping) ролей в OID и ролей в базах данных. Важной особенностью данного решения является то, что существующие приложения не нуждаются в модификации, а их защищенность возрастает: появляется возможность аутентифицировать пользователей в LDAP-каталоге на основе паролей, а также цифровых сертификатов X.509.

Аутентификация пользователей в Enterprise User Security выполняется по-разному для приложений, работающих в архитектуре клиент—сервер (двухзвенной), и для приложений, работающих в Web-архитектуре (трехзвенной).

В *двухзвенной архитектуре* пользователь непосредственно подключается к базе данных, используя свои идентификационные данные (имя/пароль или цифровой сертификат). Сервер базы данных передает данные пользователя в Oracle Internet Directory, который их проверяет и в случае успешной проверки организует соединение пользователя с так называемой разделяемой схемой, к которой ему разрешен доступ. Корпоративные пользователи не являются пользователями базы данных и поэтому могут не иметь собственных схем в базе. Пользователи соединяются с базой данных и работают с требуемыми объек-

тами в разделяемой схеме в соответствии с привилегиями, предоставленными им сервером Oracle Internet Directory. Для получения привилегий пользователям назначается одна или несколько корпоративных ролей, созданных в LDAP-каталоге.

Существует прямое соответствие между корпоративными ролями и ролями в базе данных. После успешной аутентификации сервер базы данных запрашивает у Oracle Internet Directory набор всех корпоративных ролей пользователя, создает сессию и предоставляет этой сессии роли (привилегии), закрепленные за корпоративными ролями в базе данных. В результате пользователь, зарегистрированный в LDAP-каталоге, получает возможность работать с базой данных с правами, описание которых хранится в OID. В этом случае в СУБД Oracle отсутствует необходимость создавать учетные записи пользователей и управлять ими.

В *многозвенной архитектуре* аутентификация пользователей происходит на сервере приложений. Между сервером приложений и сервером базы данных устанавливаются доверительные отношения, и все пользователи, зарегистрированные в OID, открывают сессии от имени одного или нескольких так называемых прокси-пользователей БД. В этом случае пользователи LDAP-каталога не могут напрямую соединяться с сервером базы данных. Доверительные отношения между сервером приложений и сервером базы данных означают, что всем пользователям, которые успешно прошли аутентификацию на сервере приложений, используя имя/пароль или цифровые сертификаты, разрешен доступ к объектам базы данных. Совместное использование механизмов аутентификации (однократной регистрации SSO), LDAP-каталога и Enterprise User Security обеспечивает возможность создания информационных систем, удовлетворяющих самым высоким требованиям безопасности.

2.1.1.1. Управление доступом к базе данных Oracle с помощью механизма Enterprise User Security

Постановка задачи

На предприятии существует несколько прикладных программных систем (в архитектуре «клиент—сервер» и в Web-архитектуре), работающих с базами данных Oracle. С целью снижения затрат на управление учетными записями пользователей и повышения уровня информационной безопасности принимается решение о переносе учетных записей пользователей, зарегистрированных в различных экземплярах Oracle, в единое хранилище учетных записей и введении процедур единой регистрации и авторизации пользователей при доступе к прикладным программным системам.

Описание решения

Основой архитектуры решения служит механизм Enterprise User Security. Как говорилось выше (см. разд. 2.1.1), аутентификация пользователей выполняется по-разному для приложений, работающих в архитектуре «клиент—сервер» (двухзвенной), и для приложений, работающих в Web-архитектуре (трехзвенной). Если приложения, работающие в трехзвенной архитектуре, уже использовали сервер приложений Oracle iAS 10g, то чтобы перенести учетные записи всех пользователей, зарегистрированных в разных экземплярах СУБД Oracle, в единое хранилище, не требуется устанавливать дополнительные компоненты, достаточно зарегистрировать серверы баз данных Oracle в Oracle Internet Directory и перевести данные пользователей БД в OID. В этом случае код приложений не меняется, все действия сводятся к изменению конфигурации серверов приложений и баз данных.

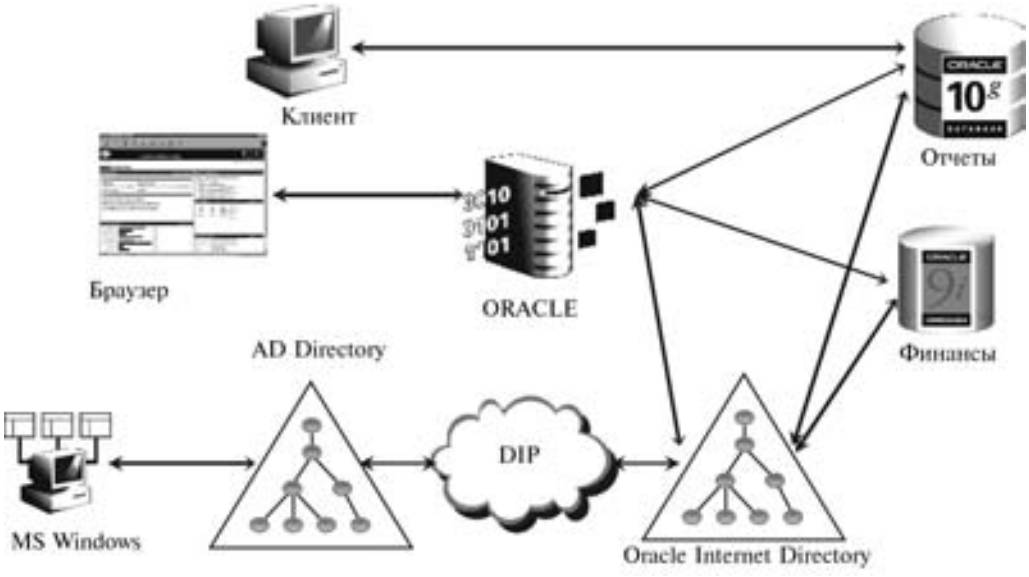

Рис. 2.1. Управление доступом с помощью механизма Enterprise User Security

Если на предприятии используются дополнительные LDAP-каталоги, например, MS Windows Active Directory (MS AD), и требуется предоставить доступ пользователей доменов Windows к корпоративным приложениям, достаточно организовать синхронизацию между каталогами (OID и MS AD) (рис. 2.1). Синхронизация осуществляется средствами Directory Integration Platform (DIP), поставляемыми Oracle в составе сервера приложений Oracle iAS 10g. DIP позволяет синхронизировать Oracle Internet Directory с другими LDAP-каталогами (MS AD, SUN Java System Directory Server, OpenLDAP, Novell eDirectory), репозиториями (Oracle Human Resource) и таблицами базы данных Oracle через стандартный интерфейс.

DIP обеспечивает создание и управление учетными записями пользователей и их привилегиями для внешних приложений, имеет механизмы внешней аутентификации, позволяющие передавать функции проверки пользователей во внешние сервисы, например, в каталог MS AD. После проведения синхронизации пользователи, зарегистрированные в домене Windows, получают возможность автоматически без дополнительной регистрации подключаться к СУБД Oracle и работать с приложениями с помощью механизмов аутентификации Kerberos и Oracle Enterprise User Security.

Механизм Enterpise User Security позволяет обеспечить единую точку входа для аутентификации пользователей, а также единую регистрацию и авторизацию пользователей для доступа к информационным ресурсам. При этом хранение информации о пользователях в централизованном и внешнем по отношению к базам данных LDAP-каталоге Oracle Internet Directory позволяет снизить затраты на администрирование учетных записей пользователей.

Поскольку Enterprise User Security является расширением популярных серверных продуктов Oracle, его применение открывает новые возможности, не требуя дополнительных затрат на развертывание системы и обучение администраторов. Механизм Enterprise User Security позволяет не только повысить безопасность данных и удобство управления

учетными записями пользователей, но и обеспечивает более гибкое управление системой безопасности предприятия в условиях изменения организационной структуры или политики безопасности, а также при появлении новых информационных систем.

2.1.1.2. Двухфакторная аутентификация в СУБД Oracle на основе встроенных средств безопасности Oracle Advanced Security

Постановка задачи

На предприятии для доступа к прикладным программным системам, реализованным на базе СУБД Oracle, и данным, которые обрабатываются и хранятся на серверах Oracle, используется самый простой метод — аутентификация по имени пользователя и паролю. Однако удобство и безопасность этого метода не устраивают руководство предприятия. Требуется обеспечить сильную аутентификацию в корпоративной сети (под управлением Microsoft Windows Server 2000/2003) и защиту доступа к конфиденциальным данным с помощью механизмов безопасности (инфраструктуры открытых ключей и организации доступа пользователей к информации), реализованных в самой СУБД Oracle.

Описание решения

Метод аутентификации пользователей по имени и паролю заменяется на более надежный. Решение базируется на применении цифровых сертификатов формата X.509 и протокола Secure Sockets Layer (SSL), поддерживающего строгую двухфакторную аутентификацию пользователей СУБД Oracle, а также позволяющего передавать информацию по сети между сервером БД и клиентским компьютером (рис. 2.2) в зашифрованном виде. При этом используются лишь штатные настройки СУБД и клиента Oracle, предусмотренные опцией Oracle Advanced Security.

СУБД Oracle поддерживает аутентификацию по сертификату X.509. Сертификаты пользователей и секретные ключи могут храниться либо в файлах стандартного формата PKCS#12, размещенных на отчуждаемых носителях, либо в реестре Windows на рабочих станциях, при этом они защищаются паролем. Однако парольная защита порождает проблемы безопасности — ключевые контейнеры могут быть скопированы и впоследствии

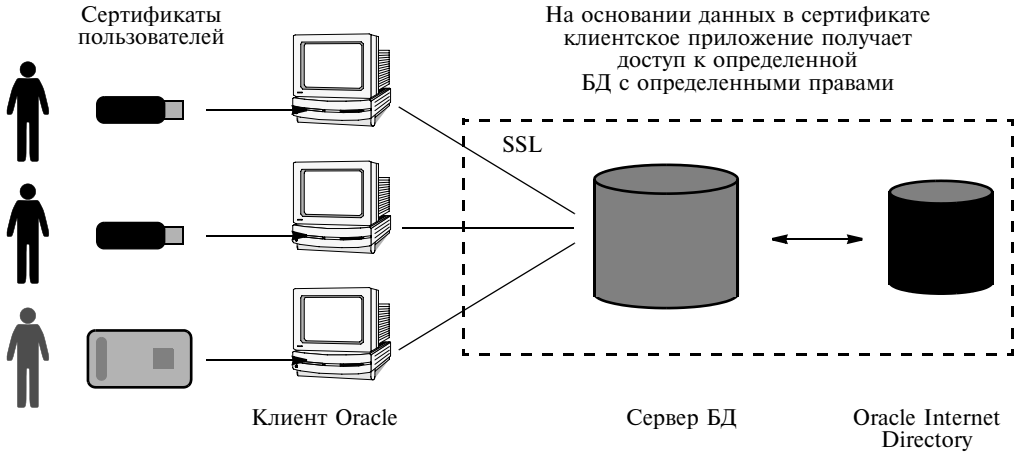

Рис. 2.2. Архитектура предоставления доступа

«взломаны» методом простого перебора паролей. Определенные неудобства вызывает и привязка ключевого контейнера к конкретной рабочей станции. Хранение идентификационных данных и ключей шифрования пользователей на персональных съемных носителях eToken компании Aladdin решает обе проблемы. Во-первых, сертификаты хранятся непосредственно в смарт-карте или USB-ключе eToken, секретный ключ находится в защищенной памяти и никогда ее не покидает; во-вторых, сертификаты «мобильны» — работать с приложениями Oracle можно с любой рабочей станции и от имени любого пользователя корпоративной сети. Все, что требуется для настройки на стороне клиента, — это указать, что ключевой контейнер помещен в хранилище сертификатов (Certificate Store) Microsoft.

В момент запроса на соединение с БД служба eToken SecurLogOn позволяет сетевым драйверам Oracle «видеть» сертификаты, установленные на eToken. Аутентификация проходит в два этапа:

1) запрос на выбор сертификата (в зависимости от выбранного сертификата пользователь будет работать с определенной БД, схемой и правами). Если сертификат единственный, он выбирается автоматически;

2) запрос PIN-кода смарт-карты или USB-ключа eToken для авторизации на операции с секретным ключом.

Когда клиенту требуется предъявить свой сертификат, служба смарт-карты «подсказывает» ему, какой сертификат следует брать из смарт-карты. Для подтверждения подлинности сервера клиенту необходим секретный ключ для расшифрования ответа сервера. Секретный ключ находится в защищенной памяти смарт-карты, и все операции с ним выполняет встроенный в карту криптопроцессор. Для таких операций требуется дополнительная авторизация, т. е. запрашивается PIN-код. Когда между клиентом и сервером установлены доверительные отношения, сервер проверяет наличие отличительного имени пользователя, для которого издан сертификат клиента, в LDAP-каталоге — Oracle Internet Directory. Если он найден, дополнительно определяются экземпляр БД, схема и набор прав для клиента. После этого сервером создается сессия пользователя с указанными параметрами. Сетевой обмен между клиентом и сервером происходит по соединению, защищенному определенным криптоалгоритмом.

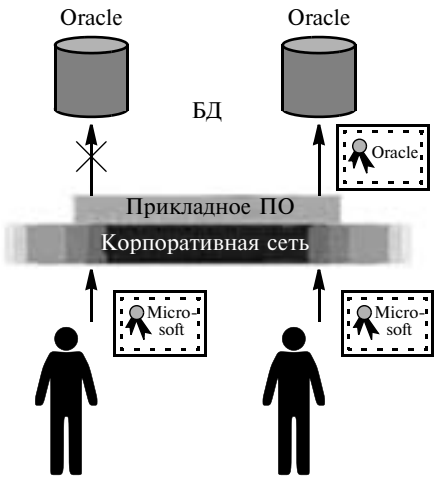

Рис. 2.3. Двухуровневая модель доступа к защищенным данным с помощью цифровых сертификатов X.509

Такой подход позволяет на практике реализовать двухуровневую модель организации защищенного доступа пользователя к данным (СУБД) с помощью цифровых сертификатов X.509, установленных в eToken. Легальные пользователи корпоративной сети (под управлением контроллера домена Windows 2000/2003) могут авторизоваться в сети (рис. 2.3) только после успешной аутентификации по смарт-карте, включающей предъявление соответствующего сертификата (первый уровень). На втором уровне защиты доступ авторизованных пользователей корпоративной сети к защищенным данным СУБД возможен только при предъявлении соответствующего сертификата Oracle.

Результатом настройки сервера БД, клиентских рабочих станций и установки сертификатов пользователей на смарт-карты является надежная аутентификация, шифрованный трафик между рабочими станциями и сервером, и самое главное — строгая персонализация доступа в БД. Помимо повышения надежности, аутентификация с использованием eToken дает ряд преимуществ по сравнению с традиционным (логин/пароль) методом. Прежде всего, электронный ключ дает возможность пользователю различных приложений не хранить «где попало» и не запоминать необходимые имена и пароли. Зная один PIN-код и выбрав сертификат из предложенного списка, можно, имея соответствующие права и привилегии, обращаться к конкретной БД, причем с любой рабочей станции.

Администратор безопасности получает при этом дополнительные удобства в виде централизованного управления доступом и контроля работы системных администраторов. Все эти возможности управления обеспечивает единый инструмент — служба каталогов Oracle Internet Directory. Существующие получают в «лице» службы каталогов единую точку входа — своего рода портал архитектуры клиент—сервер. При этом в большинстве случаев изменений в прикладном ПО не требуется.

2.1.1.3. Варианты усиления безопасности доступа в СУБД Oracle с помощью сертифицированных криптографических средств защиты

Для решения задачи, описанной в предыдущем разделе, предлагаются два варианта усиления безопасности на основе сертифицированных криптографических средств защиты.

Базовая аутентификация/авторизация и защита канала связи

Архитектура типового решения и аутентификация представлены на рис. 2.4. В данном варианте используются следующие компоненты:

- прикладное ПО, которое реализует интерфейс пользователя для решения бизнес-задач прикладной системы;
- ПО Oracle Client, которое обеспечивает взаимодействие между клиентом и сервером по сети;

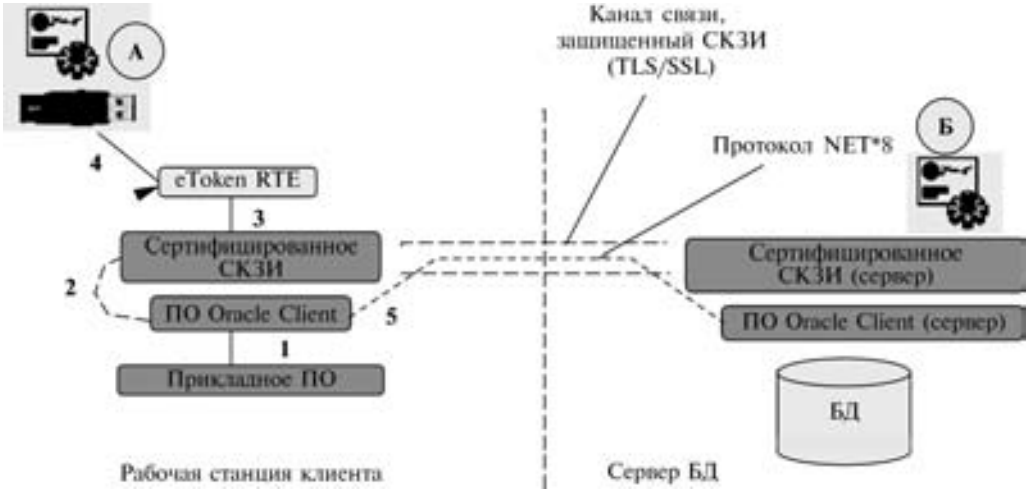

Рис. 2.4. Базовая аутентификация/авторизация и защита канала связи. Общая схема решения

- сертифицированное средство защиты информации (СКЗИ), которое устанавливает защищенное соединение между клиентом и сервером по протоколу SSL/TLS, использует сертификаты/ключи для аутентификации на серверном компоненте;
- eToken RTE — драйверы смарт-карт и USB-ключей eToken и дополнительное ПО компании Aladdin для работы с ними.

Личное хранилище сертификатов и секретных ключей пользователя на рис. 2.4 обозначено буквой А, в качестве физического носителя используется USB-ключ или смарт-карта eToken. Хранилище сертификатов и секретных ключей, используемое ПО СКЗИ на стороне сервера, обозначено буквой Б. Как правило, оно представляет собой файл формата PKCS#12.

Аутентификация выполняется за несколько шагов:

1. Прикладное ПО посылает запрос серверу БД на соединение.
2. Oracle Client делает попытку соединиться с сервером БД по обычному протоколу.
3. СКЗИ перехватывает запрос от Oracle Client и перенаправляет его в защищенный канал. Если защищенный канал еще не установлен, ПО СКЗИ выполняет аутентификацию на серверном компоненте с помощью ключа, который хранится на USB-ключе или смарт-карте eToken. В случае успешной аутентификации создается защищенный канал передачи данных.
4. В процессе аутентификации eToken RTE осуществляет дополнительную авторизацию (запрос PIN-кода) для выполнения операций с секретным ключом.
5. Oracle Client авторизует пользователя по имени и паролю.

Дальнейшее взаимодействие между клиентом и сервером осуществляется по защищенному каналу прозрачно для прикладного приложения.

В качестве ПО для выпуска сертификатов могут использоваться программные продукты, которые автоматизируют функции удостоверяющих центров (УЦ). Эти программные продукты должны быть сертифицированы ФСТЭК, ФСБ РФ (например, программный комплекс «Удостоверяющий Центр «КриптоПро УЦ»).

Базовая аутентификация/авторизация по протоколу Kerberos и защита канала связи

Второй вариант усиления безопасности на основе сертифицированных криптографических средств защиты отличается от первого только тем, что аутентификация выполняется по протоколу Kerberos. Это дает возможность отказаться от ввода имени пользователя и пароля в процессе авторизации в БД.

Архитектура типового решения и процесс аутентификации представлены на рис. 2.5. В данном варианте используются следующие компоненты:

- прикладное ПО, которое реализует интерфейс пользователя для решения бизнес-задач прикладной системы;
- ПО Oracle Client, которое обеспечивает взаимодействие между клиентом и сервером по сети. В данной схеме используется функциональность опции Advanced Security Options; это расширение СУБД Oracle устанавливается на стороне сервера баз данных;
- сертифицированное СКЗИ, которое устанавливает защищенное соединение между клиентом и сервером по протоколу SSL/TLS, использует сертификаты/ключи для аутентификации на серверном компоненте;
- eToken RTE — драйверы смарт-карт и USB-ключей eToken и дополнительное ПО компании Aladdin для работы с ними.

Личное хранилище сертификатов и секретных ключей пользователя на рис. 2.5 обозначено буквой А, в качестве физического носителя используется USB-ключ или смарт-кар-

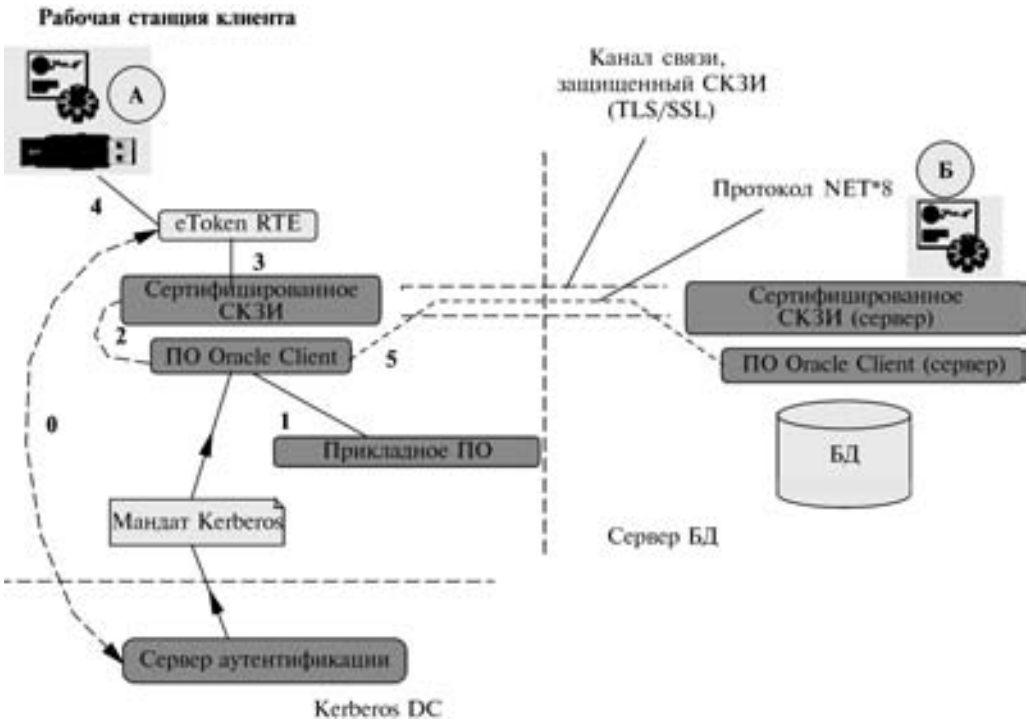

Рис. 2.5. Аутентификация/авторизация по протоколу Kerberos и защита канала связи. Общая схема решения

та eToken. Хранилище сертификатов и секретных ключей, используемое ПО СКЗИ на стороне сервера, обозначено буквой Б. Как правило, оно представляет собой файл формата PKCS#12.

В процессе аутентификации пользователя в ОС (домене) по сертификату пользователя, установленному на USB-ключе или смарт-карте eToken, сервер аутентификации возвращает на рабочую станцию клиента так называемый билет (ticket). В дальнейшем он используется для аутентификации и авторизации в БД. Аутентификация выполняется за несколько шагов:

1. Прикладное ПО посылает запрос серверу БД на соединение.
2. Oracle Client делает попытку соединиться с сервером БД по обычному протоколу.
3. СКЗИ перехватывает запрос от Oracle Client и перенаправляет его в защищенный канал. Если защищенный канал еще не установлен, ПО СКЗИ выполняет аутентификацию на серверном компоненте на основе информации о сертификате и ключах пользователя, которая хранится на токене eToken. В случае успешной аутентификации создается защищенный канал передачи данных.
4. В процессе аутентификации eToken RTE осуществляет дополнительную авторизацию (запрос PIN-кода) для выполнения операций с секретным ключом.
5. Oracle Client авторизует пользователя по билету Kerberos, полученному ранее. Дальнейшее взаимодействие между клиентом и сервером ведется по защищенному каналу прозрачно для приложения.

В качестве ПО для выпуска сертификатов могут использоваться программные продукты, которые автоматизируют функции удостоверяющих центров (УЦ). Эти программные продукты должны быть сертифицированы ФСТЭК, ФСБ России (например, программный комплекс «Удостоверяющий Центр «КриптоПро УЦ»).

2.1.2. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе Oracle Application Server

2.1.2.1. Усиленная аутентификация пользователей в неоднородной среде приложений на основе Oracle Application Server — Oracle iAS 10g

Постановка задачи

Компании необходимо обеспечить надежную аутентификацию пользователей в сложной среде распределенной обработки данных в условиях работы большого количества приложений управления предприятием. Для аутентификации пользователей при доступе к ресурсам Oracle E-Business Suite должны использоваться цифровые сертификаты формата X.509.

Описание решения

Для решения поставленной задачи выбрана комплексная инфраструктура управления учетными записями пользователей, которую сервер приложений Oracle Application Server (Oracle iAS 10g) использует для обеспечения комплексной безопасности в сложных средах распределенной обработки данных. Oracle iAS 10g Infrastructure включает следующие продукты:

- Oracle Database 10g (Metadata Repository, MR) — сервер баз данных, в таблицах которого сохраняется вся информация, необходимая для предоставления услуг управления учетными записями; является репозиторием для других продуктов Oracle iAS 10g Infrastructure, таких как Oracle Internet Directory;
- Oracle Internet Directory (OID) — каталог LDAP v.3, использующий для хранения идентификационных данных СУБД Oracle;
- Oracle Single Sign-On Server (OSSO) — сервис, выполненный на базе Oracle HTTP Server и контейнеров OC4J (Oracle Containers for JAVA). Предоставляет административные и пользовательские интерфейсы по протоколу HTTP(S), в свою очередь взаимодействует с Oracle Internet Directory для проверки аутентификационных данных и хранения ряда конфигурационных параметров; OSSO имеет встроенные функции поддержки цифровых сертификатов формата X.509;
- Delegated Administration Services (DAS) — субкомпонент OSSO, предназначенный для делегированного администрирования идентификационных и аутентификационных данных, сохраненных в Oracle Internet Directory;
- Directory Integration Platform (DIP) — сервис, выполненный на базе OC4J и предоставляющий услуги интеграции идентификационных данных между гетерогенными источниками. В качестве таких источников могут быть базы данных (например, таблица FND_USERS, хранящая пользовательские данные Oracle E-Business Suite) либо LDAP-каталоги (например, MS Active Directory). Взаимодействие DIP с источниками осуществляется с помощью профилей (коннекторов, плагинов), определяющих правила и направления миграции данных.

Рис. 2.6. Архитектура управления учетными записями пользователей

Архитектура управления учетными записями пользователей, реализованная на сервисах Oracle iAS 10g, представлена на иллюстрации (рис. 2.6).

Принцип работы Single Sign-On Oracle iAS 10g заключается в следующем: приложения Oracle (по умолчанию либо с добавленным функционалом) способны осуществлять аутентификацию пользователя на основании заголовка Cookie, формируемого сервером Single Sign-On после успешной аутентификации пользователя в системе однократной регистрации. В заголовке Cookie содержится зашифрованная информация об имени пользователя и идентификатор успешного прохождения аутентификации.

Уровень безопасности решений на основе Oracle iAS 10g

В решениях на основе Oracle iAS 10g могут быть применены следующие методы защиты аутентификационных данных:

- сложные пароли;
- генерация паролей по установленной парольной политике (настраивается средствами Oracle Internet Directory);
- сертификаты формата X.509;
- защита секретного ключа пользователя PIN-кодом.

Таким образом, Oracle iAS 10g обеспечивает максимальную защищенность аутентификационных данных.

Двухфакторная аутентификация в Oracle iAS 10g

В решениях на базе Oracle iAS 10g может быть реализован механизм двухфакторной аутентификации на базе сертификатов X.509. При этом в качестве первого фактора аутентификации выступают сертификаты, а в качестве второго фактора — аппаратные носители сертификатов и секретных ключей пользователей. Аппаратные носители — смарт-карты — способны осуществлять генерацию секретного ключа пользователя и выполнять с его помощью криптографические операции. Секретный ключ в данном случае не покидает физические границы аппаратного носителя. В качестве аппаратных носителей ключевой информации могут использоваться аппаратные носители, которые способны взаимодействовать с криптопровайдером операционной системы Windows. Таким решением, например, является USB-ключ или смарт-карта eToken PRO компании Aladdin. Взаимодействие eToken с криптопровайдером Windows осуществляется с помощью ПО eToken RTE (Run-Time Environment).

Способы аутентификации

Сервер Single Sign-On в составе Oracle iAS 10g может использовать в качестве пользовательского интерфейса протокол HTTP(S). Таким образом, возможны следующие способы аутентификации:

- аутентификация по имени и паролю пользователя;
- SSL-аутентификация по протоколу HTTPS с предъявлением сертификатов X.509.

Любой из приведенных методов может быть усилен применением аппаратных носителей. Пример аутентификации по имени и паролю пользователя приведен на рис. 2.7.

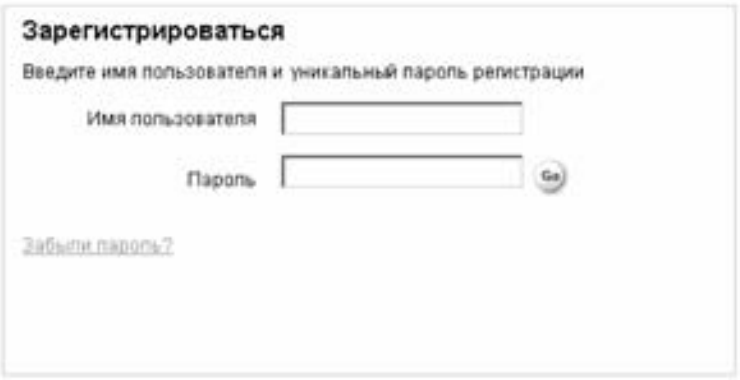

Рис. 2.7. Форма аутентификации Oracle Identity Management с вводом имени пользователя и пароля

Пример SSL-аутентификации по протоколу HTTPS с использованием USB-ключей и предъявлением сторонами своих сертификатов иллюстрируют рис. 2.8 и 2.9. При под-

Рис. 2.8. Окно выбора сертификата

ключении к компьютеру USB-ключа (или смарт-карты) eToken, на котором (-ой) хранятся сертификаты открытых ключей пользователя, появляется окно выбора нужного сертификата (единственный сертификат выбирается автоматически).

Пользователь выбирает сертификат, но для работы с ним система просит предварительно ввести PIN-код.

Рис. 2.9. Окно ввода PIN-кода

Серверное и клиентское ПО

Решение для Oracle iAS 10g не требует установки какого бы то ни было специализированного ПО на рабочие места пользователей, если выполняется парольная аутентификация пользователей. При аутентификации пользователей с помощью цифровых сертификатов, установленных на электронных ключах eToken Pro, на рабочие места пользователей необходимо установить клиентское ПО eToken Real-Time Environment (RTE).

Количество единиц серверного оборудования может варьироваться в зависимости от топологии развертывания решения. Компания Oracle рекомендует разворачивать решение Oracle Identity Management в следующей конфигурации:

- 2 сервера Oracle Database 10g с установленной опцией Real Applications Clusters;
- 2 сервера для размещения компонентов Oracle Internet Directory и Directory Integration and Provisioning;
- 2 сервера для размещения компонентов Single Sign-On и Delegated Administration Services;
- 2 устройства балансировки нагрузки.

Рекомендуемая топология приведена на рис. 2.10.

На данной иллюстрации:

- LBR#1, LBR#2 — Load Balancer — устройства балансировки нагрузки;
- IM1, IM2 — серверы с размещенными компонентами OSSO и DAS;
- OID1, OID2 — серверы с размещенными компонентами OID и DIP.

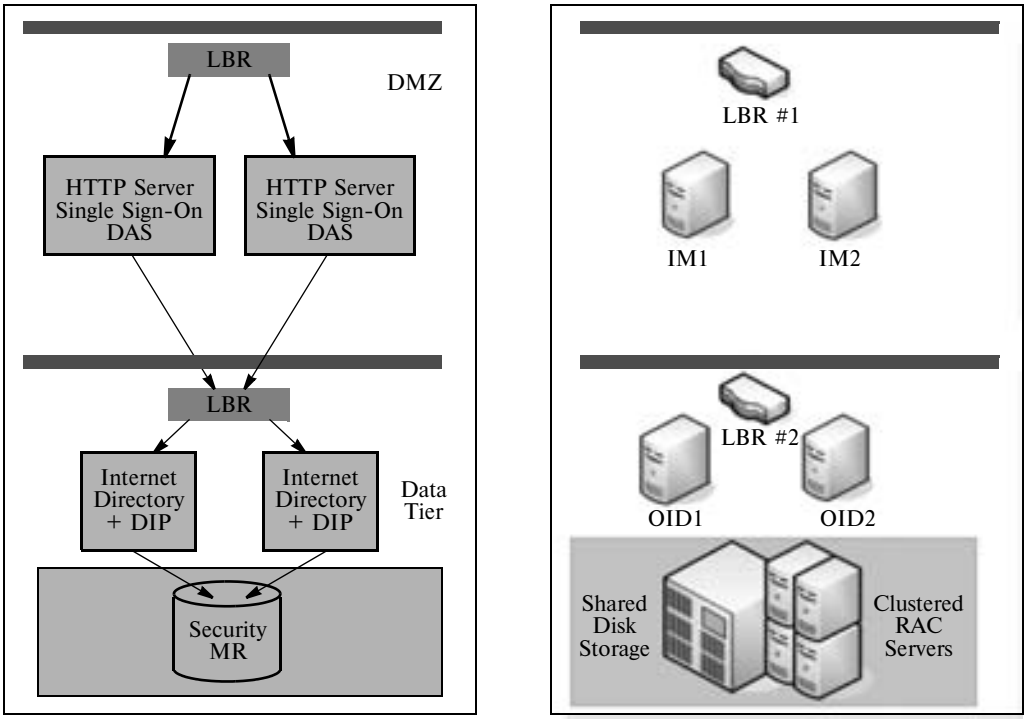

Рис. 2.10. Рекомендуемая топология развертывания решения Oracle Identity Management

Нижний слой представлен двумя серверами баз данных с размещенными агентами Real Application Clusters и данными, вынесенными на сетевое хранилище (Shared Disk Storage).

Возможности авторизации

Решения на основе Oracle iAS 10g не реализуют авторизационные требования при доступе к не-Oracle-приложениям. Доступ пользователей к тем или иным данным после пройденной аутентификации (авторизации) осуществляется собственно средствами не-Oracle-приложений.

Oracle Internet Directory позволяет группировать пользователей в зависимости от их прав доступа, однако в данном случае авторизация носит бинарный характер, т. е. пользователи из выделенных групп могут проходить авторизацию средствами Single Sign-On, а другим в доступе будет отказано.

Поддерживаемые платформы

Решения на основе Oracle iAS 10g ориентированы на совместимость с решениями Oracle, такими как Oracle E-Business Suite, Oracle Portal и др. Информационные системы и платформы от сторонних производителей в явном виде не поддерживаются. Такие решения позволяют также обеспечить SSO по отношению к трехзвенным приложениям других поставщиков.

Поддерживаемые аутентификационные устройства

Так как платформа Oracle iAS 10g в первую очередь ориентирована на поддержку тонких веб-клиентов, допускается использование любых аутентификационных устройств, совместимость которых с веб-браузерами и операционной системой предусмотрена производителем устройства.

Решение eToken SecurLogon для Oracle Application Server

Решение компании Aladdin eToken SecurLogon для Oracle Application Server предназначено для аутентификации в Oracle iAS 10g с помощью смарт-карт. Поддержка устройств eToken обеспечивается с помощью драйвера eToken Run-time Environment, который взаимодействует с криптопровайдером операционной системы и позволяет осуществлять операции с ключевой информацией, сохраненной в аппаратном носителе, через криптопровайдер операционной системы прозрачно для пользователя. Благодаря eToken SecurLogon пользователям не нужно запоминать имена и пароли, следить за сложностью и качеством паролей, периодически их менять — нужно только носить с собой USB-ключ или смарт-карту и знать PIN-код.

eToken SecurLogon для Oracle Application Server обеспечивает взаимную аутентификацию клиента и сервера приложений при доступе к приложениям и шифрование согласно протоколу SSL с помощью цифровых сертификатов X.509. Такую же связь можно установить между сервером приложений и сервером базы данных. Благодаря этому на серверах может быть введен явный запрет на соединения по открытому протоколу (не SSL). При этом для приложений, требующих соединения с каким-либо сервером по открытому протоколу (например, для администрирования сервера), в сетевых настройках данного сервера явно указываются IP-адреса, для которых действует исключение из общего запрета.

eToken SecurLogon для Oracle Application Server можно интегрировать с Token Management System (TMS) — системой управления жизненным циклом USB-ключей и смарт-карт. eToken SecurLogon встраивается в различные инфраструктуры открытых ключей — не только Oracle iAS 10g, но и Microsoft Windows 2000/XP/2003, RSA Keon и т. п., что обеспечивает возможность централизованного выпуска сертификатов и управления правами пользователей в рамках всей информационной инфраструктуры предприятия, а не только подсистем на основе продуктов Oracle.

Преимущества

Решение eToken SecurLogon для Oracle Application Server обеспечивает значительно более высокую безопасность за счет:

- отказа от передачи имен пользователей и паролей по сети в открытом виде;
- применения двухфакторной программно-аппаратной аутентификации вместо однофакторной;
- использования защищенного шифрованием канала передачи данных;
- взаимной аутентификации сервера и клиента;
- эффективного применения встроенных средств и механизмов защиты Oracle Application Server.

Способы аутентификации, применяемые в eToken SecurLogon для Oracle Application Server на основе технологии авторизации Oracle Single Sign-On, удобнее для пользователей, чем стандартные способы, поскольку требуют запоминания единственного PIN-кода, а не множества имен пользователя и сложных паролей, необходимых для доступа к различным приложениям.

Принципы работы и архитектура eToken SecurLogon для Oracle Application Server

Процесс аутентификации иллюстрирует рис. 2.11, на котором цифрами обозначены этапы аутентификации:

1 и 2 — взаимная аутентификация клиента и сервера приложений с помощью цифровых сертификатов X.509. Сертификат пользователя с секретным ключом установлен в памяти eToken, а сертификат сервера приложений (HTTP-сервера) с секретным ключом — в контейнере wallet (файле формата PKCS#12).

3 — после успешной аутентификации компонент Single Sign-On сервера приложений проверяет в LDAP-каталоге (Oracle Internet Directory, OID) наличие учетной записи пользователя, для которого издан этот сертификат. Причем проверка может выполняться по всем полям сертификата или просто по отличительному имени владельца сертификата.

4 — если учетная запись пользователя найдена, то устанавливается защищенное соединение по протоколу SSL и пользователь получает доступ к приложению с правами, соответствующими его учетной записи.

Сервер приложений должен быть настроен на аутентификацию с помощью протокола SSL. Сервер приложений выступает по отношению к серверу базы данных как обычный клиент и имеет одно или несколько постоянных соединений с сервером базы данных.

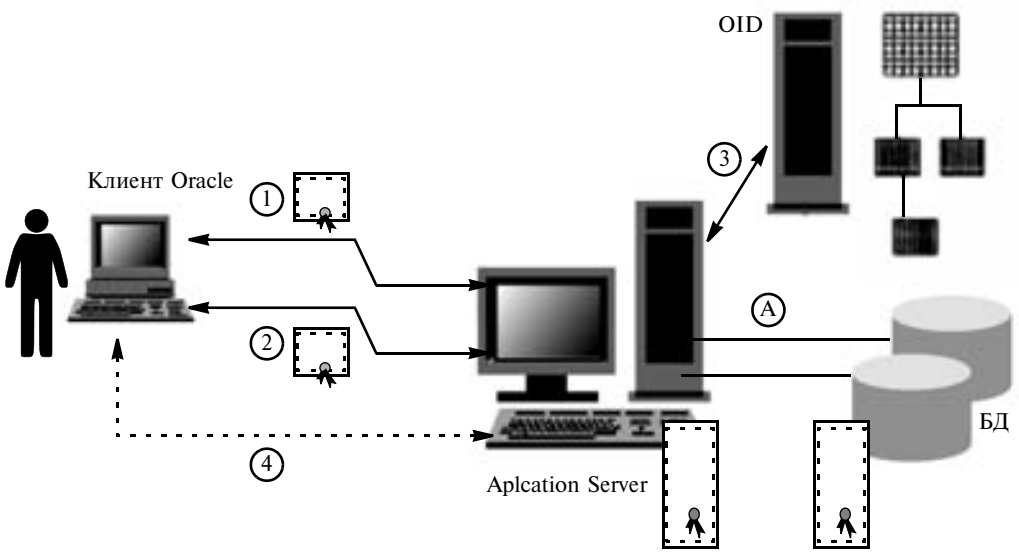

Рис. 2.11. Процесс аутентификации с помощью eToken SecurLogon для Oracle Application Server

2.1.2.2. Встраивание сертифицированных криптографических средств в информационные системы на платформе Oracle Application Server

Постановка задачи

Основной задачей является построение защищенной информационной системы, использующей технологии и инфраструктуру Oracle Application Server. Данная задача делится на три подзадачи:

- защита канала передачи данных криптографическими методами;
- усиленная аутентификация пользователей при доступе к приложениям информационной системы;
- интеграция со штатными механизмами аутентификации/авторизации Oracle Application Server.

Решение предусматривает использование программных продуктов, реализующих российские криптоалгоритмы. Поставщики криптографических средств защиты должны иметь лицензии ФСБ России, а само ПО — сертификаты по соответствующему классу защищенности. Применяемые методы встраивания решения в инфраструктуру Oracle Application Server не должны нарушать лицензионных соглашений на использование ПО поставщика (Oracle, поставщиков ОС для сервера или клиентских рабочих станций).

Описание решения

Основными компонентами решения, представленного на рис. 2.12, являются:

- приложения (applications), которые реализуют интерфейс пользователя и бизнес-логику информационной системы;
- клиент (Web-браузер), который обеспечивает взаимодействие между клиентом и сервером приложений;
- сертифицированное СКЗИ (подключаемый модуль сервера Apache (mod_ssl), адаптированный для работы с российской криптографией), который устанавливает защищенное соединение между клиентом и сервером по протоколу SSL/TLS, использует сертификаты/ключи для аутентификации на серверном компоненте;
- eToken RTE (драйверы смарт-карт и USB-ключей eToken компании Aladdin и дополнительное ПО для работы с ними).

В качестве физических носителей ключей и сертификатов пользователей применяются USB-ключи или смарт-карты eToken. Физическое хранилище сертификатов и секретных ключей, используемое модулем СКЗИ в составе прокси-сервера, определяется производителем СКЗИ.

В качестве ПО для выпуска сертификатов могут использоваться программные продукты, которые автоматизируют функции удостоверяющих центров (УЦ). Эти программные продукты должны быть сертифицированы ФСТЭК, ФСБ РФ (например, программный комплекс «Удостоверяющий Центр «КриптоПро УЦ»).

Принцип функционирования

1. Пользователь информационной системы пытается получить доступ к защищенному ресурсу (приложению). Клиент посылает запрос на аутентификацию прокси-серверу.

2. Производится стандартная аутентификация по SSL-протоколу. При этом eToken RTE осуществляет дополнительную авторизацию (запрос PIN-кода) для выполнения операций с секретным ключом. Логику работы с сертификатами, изданными с использованием российских криптоалгоритмов, реализует модуль СКЗИ (mod_ssl), имплементированный в сервер Apache.

3. При успешной аутентификации создается защищенный канал передачи данных между клиентом и прокси-сервером, а все запросы в дальнейшем перенаправляются на Oracle HTTP Server (OHS). Необходимые для авторизации заголовки запросов устанавливаются прокси-сервером на основании информации, полученной из сертификата, предъявленного клиентом в процессе аутентификации.

4. Затем обращение к приложению перехватывается компонентом Single Sign-On (SSO) Oracle Application Server, который обеспечивает штатный процесс авторизации пользователя и использует вызов подключаемого модуля авторизации (Custom SSO plug-in).

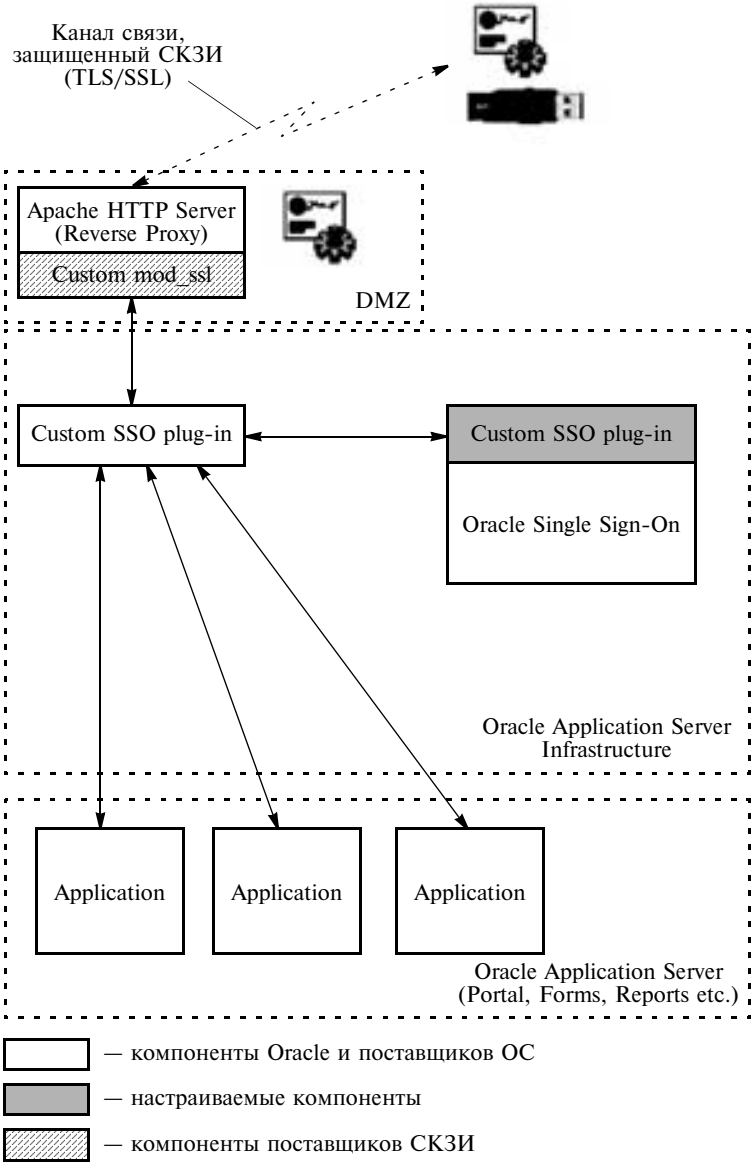

Рис. 2.12. Аутентификация и защита канала передачи данных с помощью eToken SecurLogon для Oracle Application Server и средств криптографической защиты

Решение позволяет создавать информационные системы на платформе Oracle Application Server, которые не только обладают повышенной безопасностью, но и соответствуют требованиям лицензирующих организаций. Описанная выше схема опирается только на документированные возможности используемого ПО и соответственно не нарушает лицензионных соглашений на его применение.

2.1.2.3. Смарт-карты и USB-ключи eToken для аутентификации и авторизации в приложениях Oracle Business Intelligence EE

Постановка задачи

Основной задачей является построение защищенной информационной системы, использующей технологии и инфраструктуру Oracle Application Server. Данная задача делится на четыре подзадачи:

- защита канала передачи данных криптографическими методами;
- усиленная аутентификация пользователей при доступе к приложениям информационной системы;
- безопасное хранение ключей и сертификатов;
- интеграция со штатными механизмами аутентификации/авторизации Oracle Application Server.

Применяемые методы встраивания решения в инфраструктуру и/или приложения Oracle Application Server не должны нарушать лицензионных соглашений на использование ПО поставщика (Oracle, поставщиков ОС для сервера или клиентских рабочих станций).

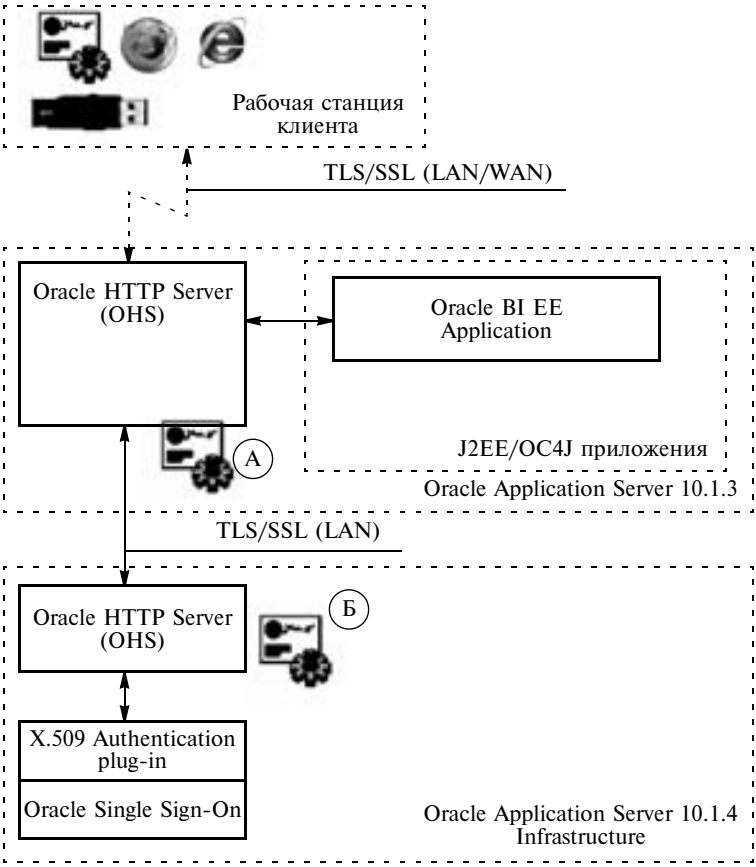

Рис. 2.13. Аутентификация и авторизация в приложениях Oracle Business Intelligence EE посредством смарт-карт и USB-ключей eToken

Описание решения

Основными компонентами решения, представленного на рис. 2.13, являются:

- приложения (applications), которые реализуют интерфейс пользователя и бизнес-логику приложений Oracle BI EE и Oracle BI Publisher (XML Publisher);
- инфраструктура, которая обеспечивает хранение информации о пользователях, ролях, приложениях, а также реализует механизмы авторизации и однократной регистрации (Single Sign-On);
- клиент (Web-браузер), который реализует взаимодействие по сети между клиентом и сервером приложений.

В качестве физических носителей ключей и сертификатов пользователей используются USB-ключи или смарт-карты eToken. Сертификаты и секретные ключи, используемые компонентом Oracle HTTP Server (OHS) в составе сервера приложений и инфраструктуры, хранятся в файле формата PKCS#12.

Принцип функционирования

1. Пользователь информационной системы пытается получить доступ к защищенному ресурсу (приложению), вводя соответствующий URL в адресной строке браузера. Браузер клиента посылает запрос на http-сервер (OHS) сервера приложений.

2. OHS выполняет стандартную SSL-аутентификацию, используя свой сертификат и секретный ключ из файлового хранилища.

3. Пользователь предъявляет свой сертификат, хранящийся на смарт-карте или USB-ключе eToken.

4. При успешной аутентификации создается защищенный канал передачи данных между браузером клиента и сервером приложений. Необходимые для процедуры авторизации заголовки запросов устанавливаются http-сервером на основании информации, полученной из сертификата, предъявленного клиентом в процессе аутентификации.

5. Затем обращение к приложению перехватывается компонентом Single Sign-On (SSO) инфраструктуры Oracle Application Server, SSO обеспечивает штатный процесс авторизации пользователя и использует вызов подключаемого модуля авторизации по цифровому сертификату.

6. При успешной авторизации пользователь получает доступ к выбранному приложению.

7. Если сессия пользователя не прерывалась (браузер не был закрыт), то последующие обращения к другим приложениям Oracle Business Intelligence или иным, развернутым на Oracle Application Server, не потребуют повторных процедур аутентификации и авторизации.

В качестве ПО для выпуска сертификатов могут использоваться программные продукты для автоматизации функций удостоверяющих центров (УЦ) от разных производителей. Все используемые технологии, компоненты и настройки на стороне сервера приложений и инфраструктуры предоставляются в составе соответствующих компонентов Oracle и описаны в штатной документации.

2.1.3. Обеспечение безопасности доступа к бизнес-приложениям Oracle E-Business Suite

Постановка задачи

В компании, работающей в сфере информационных технологий (крупный системный интегратор), необходимо реализовать внутренний проект по созданию корпоративной системы управления на базе комплекса бизнес-приложений Oracle E-Business Suite. Обладая

широким функционалом (от управления финансами и производством до отношений с поставщиками и клиентами), данный комплекс консолидирует в среде бизнес-приложений обширную конфиденциальную информацию о деятельности компании.

Основными целями проекта по обеспечению защищенного доступа к ресурсам программного комплекса являются:

- предоставление безопасного доступа с удаленных рабочих станций к корпоративным информационным ресурсам Oracle E-Business Suite;
- обеспечение как локальных, так и удаленных пользователей возможностями работы по единому защищенному протоколу;
- развертывание системы надежной двухфакторной аутентификации сотрудников компании в сети с помощью аппаратного ключа eToken и PIN-кода;
- построение инфраструктуры для защищенного документооборота на основе ЭЦП и корпоративного Удостоверяющего центра.

Для более полного понимания специфики решения задачи обеспечения защищенного доступа к Oracle E-Business Suite необходимо кратко описать архитектуру данного программного комплекса.

Архитектура Oracle E-Business Suite

Oracle E-Business Suite использует трехуровневую модель приложений (представлена на рис. 2.14):

- уровень клиента (Desktop Tier);
- уровень приложений (Application Tier);
- уровень базы данных (Database Tier).

Архитектура Oracle E-Business Suite позволяет выполнять распределенные вычисления и легко масштабируется на уровнях приложений и базы данных, что означает возможность установки нескольких экземпляров служб на уровне приложений, расположенных на разных компьютерах, объединенных в сеть.

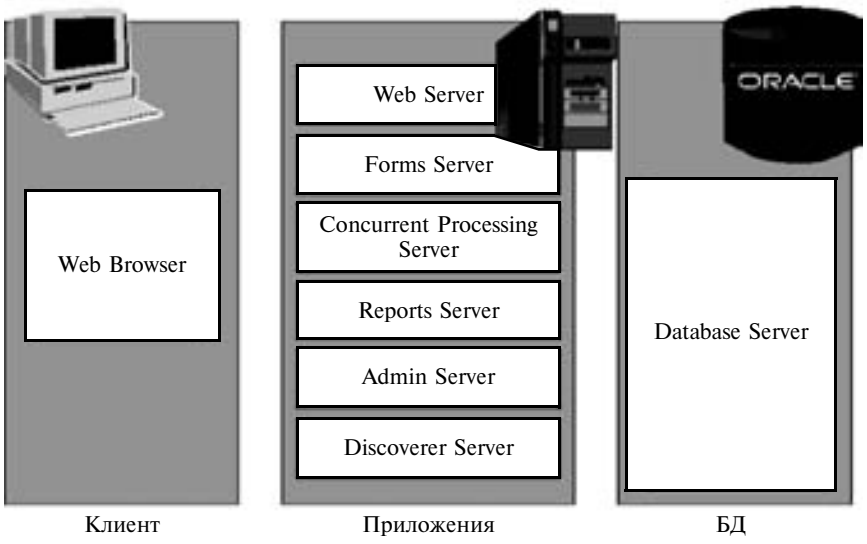

Рис. 2.14. Трехуровневая модель Oracle E-Business Suite

Уровень клиента

Уровень клиента представлен Интернет–браузером, а также Java-машиной, функционирующей как добавочный компонент (add-on) браузера; он обеспечивает визуальный интерфейс пользователя (рис. 2.15).

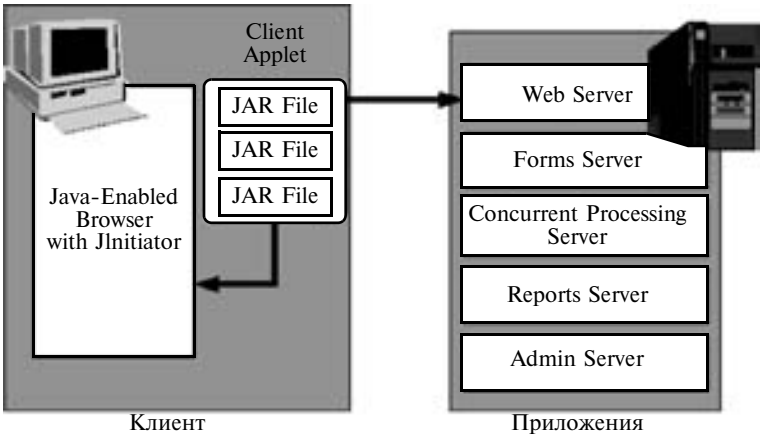

Рис. 2.15. Взаимодействие клиента и приложений

Компоненты уровня клиента и уровня приложений могут взаимодействовать как в рамках локальной (LAN), так и глобальной сети (WAN).

Пользователь в браузере вводит адрес (URL), являющийся адресом веб-сервера экземпляра Oracle E-Business Suite. Работа с Oracle E-Business Suite начинается с аутентификации и авторизации пользователя, т. е. с ввода имени и пароля (рис. 2.16).

При успешной аутентификации/авторизации браузер переадресуется на стартовую страницу, соответствующую введенному имени пользователя. Затем данное имя (учетная запись) используется для различных целей, в том числе аудита и ограничения доступа.

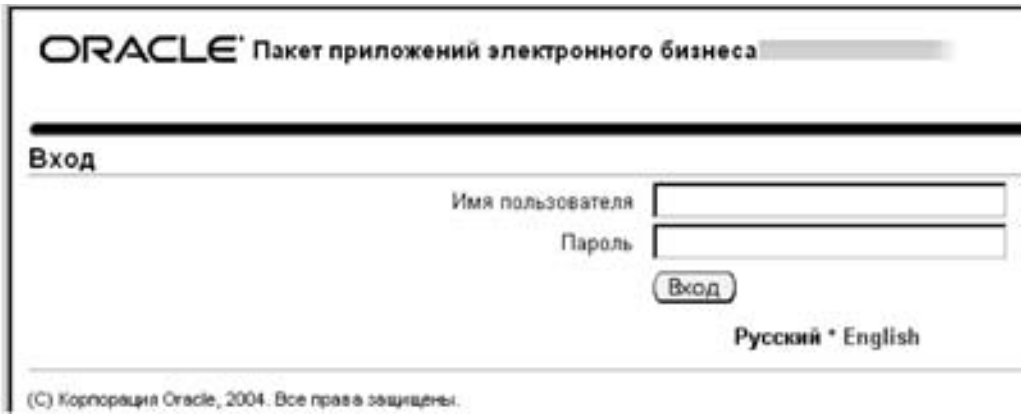

Рис. 2.16. Форма авторизации доступа к Oracle E-Business Suite с вводом имени пользователя и пароля

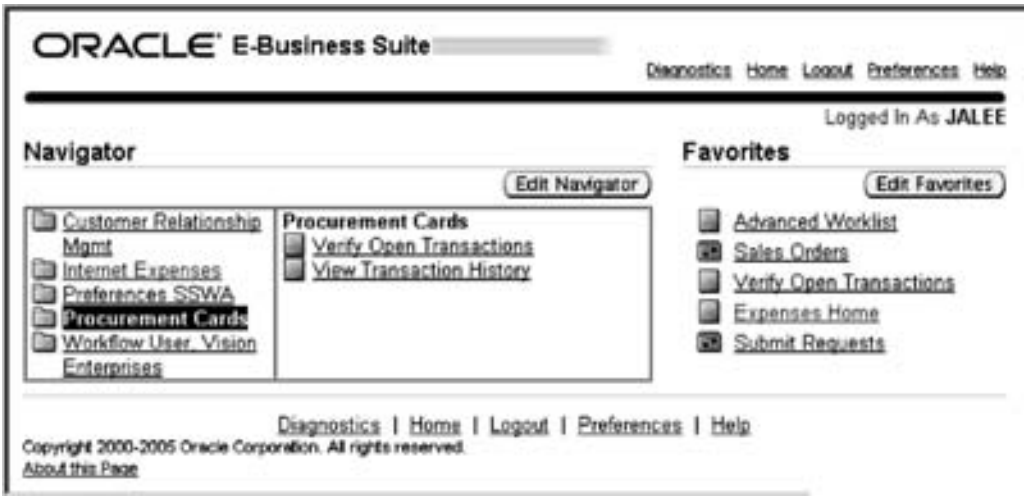

Рис. 2.17. Пример стартовой страницы пользователя

веб-сервер также посылает некоторый набор данных, идентифицирующий сессию (authentication cookie), которая существует до момента закрытия браузера или до завершения работы с Oracle E-Business Suite.

На стартовой странице (рис. 2.17) в виде ссылок перечислены приложения, к которым разрешен доступ пользователю. При навигации по ссылкам каждое из приложений, входящих в состав Oracle E-Business Suite, проверяет наличие authentication cookie для данной сессии. Если такая информация недоступна, то аутентификация/авторизация повторяется. Таким образом обеспечивается единая точка доступа ко всему набору приложений.

Презентационный уровень выполняемых в окне браузера приложений обеспечивает виртуальная машина Java и апплет клиента (Client Applet). Апплеты клиента содержат все необходимые визуальные и прикладные компоненты, реализующие клиентскую часть (Front End) Oracle E-Business Suite и представлены в виде набора jar-архивов. Виртуальная машина Java кэширует нужные jar-файлы на рабочей станции клиента, при необходимости обновляет их и выполняет апплеты клиента в окне браузера. В качестве виртуальной машины Java на рабочей станции клиента архитектура Oracle E-Business Suite предусматривает возможность использования одного из трех компонентов:

- Oracle Jinitiator;
- Sun Java RunTime Environment (JRE);
- Microsoft Java Virtual Machine (JVM).

Уровень приложений

Уровнень приложений представлен набором сервисов (Services), которые реализуют бизнес-логику компонентов Oracle E-Business Suite, а также обеспечивают управление компонентами и формирование страниц для отображения на уровне клиента. Основными компонентами уровня приложений являются веб-сервер и сервер форм. Приложения, выполняемые на данном уровне, могут быть разделены на два класса:

- приложения на основе HTML (HTML-based или Self Service Applications);
- приложения на основе Oracle Forms (Forms-based Applications).

Web-сервер

Web-сервер обрабатывает запросы от браузера клиента и формирует HTML-страницы для отсылки результата. Web-сервер содержит следующие компоненты (рис. 2.18):

- прослушиватель (Web-listener);
- сервер сервлетов (Java servlet engine);
- серверные страницы Java (Java Server Pages).

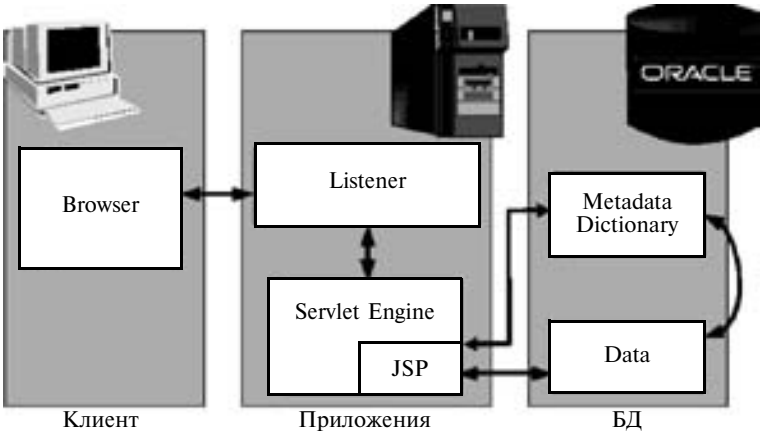

Рис. 2.18. Уровень приложений

По возможности Web-сервер обслуживает запросы самостоятельно, при необходимости передавая запросы в сервер сервлетов, например, для извлечения информации из базы данных.

Непосредственно Web-сервером выполняются HTML-приложения, которые имеют следующие особенности:

- не используют Oracle Forms;
- разработаны на чистом HTML и Java Script;
- динамически формируют HTML-страницы, исполняя Java-код;
- для формирования страниц используют репозиторий БД.

Сервер форм

Сервер форм Oracle Forms Server обслуживает формы Oracle E-Business Suite и обеспечивает графический интерфейс пользователя. Сервер форм взаимодействует с БД, извлекая нужную информацию, формирует и отображает окна на уровне клиента, инициирует изменения в БД (рис. 2.19). Дополнительно сервер форм кэширует необходимые данные (например, большие списки) на уровне клиента.

Сервер форм может взаимодействовать с браузером клиента по протоколам HTTP, HTTPS и Socket (TCP/IP), а с сервером БД — по протоколу Oracle Net*8.

Forms Listener Servlet

Для работы сервера форм в локальной сети, как правило, используется режим Socket. Такой режим является наиболее производительным, однако, не позволяет получить доступ к Oracle E-Business Suite через глобальную сеть, для этого используется специальная

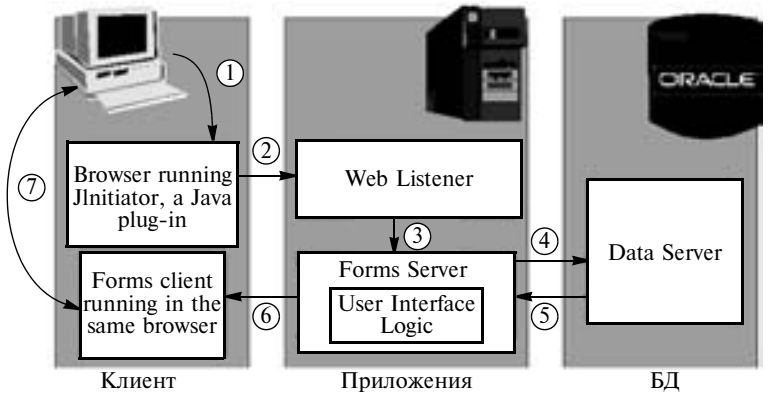

Рис. 2.19. Взаимодействие сервера форм с базой данных и браузером клиента

архитектура Forms Listener Servlet. Она дает возможность взаимодействовать процессам времени исполнения сервера форм с клиентом через Web-сервер и использовать HTTP- или HTTPS-протоколы. Помимо возможности работы по глобальной сети такая архитектура позволяет восстанавливать прерванные соединения, использовать меньшее количество портов и обеспечивает более высокий уровень безопасности при передаче данных в Интернете. Однако в рамках такой архитектуры возрастает сетевой трафик (в среднем на 40%). Это приводит к увеличению времени отклика для клиента LAN на 8—10 %, а для клиента WAN — до 30%.

Уровень базы данных

Уровень базы данных также представлен набором сервисов и обеспечивает хранение и манипулирование данными Oracle E-Business Suite.

Схема безопасности Oracle E-Business Suite

Стандартная система безопасности Oracle E-Business Suite базируется на четырех компонентах — аутентификации, авторизации, аудите и безопасности сети. Аутентификация осуществляется по имени пользователя и паролю. Возможности имеющейся специальной системы настройки политики управления паролями и их качеством, как правило, персоналом не используются, и все недостатки, присущие аутентификации по паролям, сохраняются. Короткие и простые пароли легко подбираются; длинные и сложные тяжело запомнить, и поэтому их часто записывают, что является грубым нарушением политики безопасности; слишком редкая смена пароля пользователями существенно снижает все усилия специалистов по информационной безопасности.

Система авторизации обеспечивает управление правами и привилегиями, назначенными определенной учетной записью, а система аудита позволяет протоколировать и обрабатывать информацию о транзакциях, выполненных от имени определенного пользователя по учетной записи. Oracle E-Business Suite поддерживает работу всех своих компонентов по протоколу HTTPS, что обеспечивает защиту каналов передачи данных.

Помимо своевременного обновления, повышения качества паролей и регулярного аудита для защиты приложений при доступе к ним через Интернет рекомендуется использовать протокол HTTPS. После выполнения ряда процедур (как автоматизированных,

так и выполняемых вручную) все компоненты Oracle смогут работать через защищенные каналы связи. Однако, если на веб-сервере, обрабатывающем запросы от браузера клиента и формирующем HTML-страницы, установить обязательную проверку подлинности сертификата клиента, работа на сервере форм становится невозможной.

Это происходит из-за того, что Oracle Jinitiator (встроенный в браузер компонент), используемый на уровне клиента, не поддерживает аутентификацию клиента по SSL-протоколу, поскольку не умеет извлекать сертификат клиента из хранилища браузера. Эта проблема может быть решена заменой на клиентской рабочей станции компонента Jinitiator от Oracle на подключаемый модуль Java Plug-In от Sun, при этом требуются дополнительные настройки на стороне сервера и клиента. Еще один недостаток такого решения — наличие дополнительного хранилища сертификатов и ключей, «понятных» Java-клиенту.

Сертификаты и ключи, установленные в браузере (т. е. в локальном хранилище сертификатов Microsoft), порождают как минимум две проблемы. Во-первых, они не могут считаться в достаточной мере защищенными, поскольку эта информация доступна для записи пользователя компьютера, на котором установлен браузер, и для администратора системы, следовательно, ею могут воспользоваться несанкционированно. Во-вторых, остается проблема удаленного доступа с произвольного компьютера, поскольку учетной записью можно воспользоваться через Интернет с удаленного компьютера.

Вариант с хранением ключевой информации на незащищенных носителях (дискеты, флэш-память и т. п.) неприемлем как с точки зрения безопасности, так и по соображениям надежности и удобства использования: удаленному пользователю, например, нужно установить ключевой контейнер с носителя на компьютер, а по завершении сеанса не забыть его удалить. Разумным выходом является хранение ключей и сертификатов на отчуждаемом защищенном носителе — USB-ключе или смарт-карте eToken компании Aladdin.

Описание решения

Авторизованный доступ пользователей к данным бизнес-приложений Oracle E-Business Suite осуществляется с помощью цифровых сертификатов, защищенного SSL-протокола взаимодействия пользователя и комплекса бизнес-приложений Oracle E-Business Suite на базе специализированных аппаратно-программных продуктов Aladdin.

Продукт eToken SecurLogon for Oracle E-Business Suite

Возможности

Программно-аппаратный продукт eToken SecurLogon для Oracle E-Business Suite компании Aladdin обеспечивает взаимную аутентификацию клиента и сервера Oracle E-Business Suite на основе цифровых сертификатов X.509 при доступе к серверу и шифрование согласно протоколу SSL. Благодаря этому на сервере может быть введен явный запрет на соединения по открытому протоколу (не SSL). При этом для приложений, требующих соединения с сервером Oracle E-Business Suite по открытому протоколу (например, для администрирования), в сетевых настройках сервера явно указываются IP-адреса, для которых действует исключение из общего запрета.

В продукте предусмотрена возможность интеграции с Oracle Application Server Single Sign-On. Такая интеграция обеспечивает однократную регистрацию пользователя при доступе к различным ресурсам и централизованное управление правами пользователей приложений. Продукт позволяет использовать один и тот же eToken для доступа в помещения (по встроенной в карту радиометке) и в различные системы приложения (не только входящие в пакет приложений Oracle для электронного бизнеса).

Продукт можно интегрировать с Token Management System (TMS) — системой управления жизненным циклом eToken в масштабах предприятия. С помощью TMS можно организовать централизованную подготовку eToken к работе, удаленное обслуживание (в том числе разблокирование PIN-кода), отзыв полномочий и т. д.

Продукт встраивается в различные инфраструктуры открытых ключей — не только Oracle Identity Management, но и Microsoft Windows 2000/XP/2003, RSA Keon и т. п. Это обеспечивает возможность централизованного издания сертификатов и управления правами пользователей в рамках всей информационной инфраструктуры предприятия, а не только подсистем Oracle.

Принципы работы продукта

Аутентификация и авторизация пользователей выполняется следующим образом. Пользователь вводит в окне браузера адрес защищенного Web-сервера Oracle E-Business Suite (используется протокол HTTPS). Для аутентификации пользователя на Web-сервере применяются секретный ключ и сертификат открытого ключа, установленный в памяти eToken. В процессе аутентификации у пользователя запрашивается PIN-код eToken. При успешной аутентификации между клиентом и сервером устанавливается защищенное соединение, и пользователь попадает на стартовую страницу Oracle E-Business Suite.

Аутентификация пользователя на сервере форм, осуществляется с помощью eToken Web Sign On. Затем пользователь выбирает приложение, в котором он будет работать. После этого на рабочей станции клиента активизируется Java-клиент, который также устанавливает с сервером защищенное соединение и загружает (при необходимости) нужные библиотеки с сервера.

Преимущества продукта

Продукт eToken SecurLogon обладает следующими преимуществами:

- не требует установки какого-либо дополнительного программного обеспечения на сервере, достаточно выполнения описанных настроек;
- поддерживает все серверные платформы, на которые может быть установлен пакет приложений Oracle для электронного бизнеса;
- предусматривает безопасное хранение секретных ключей и соответствующих сертификатов открытого ключа в энергонезависимой памяти ключа eToken;
- способы аутентификации, применяемые в продукте, удобны для пользователей, так как не требуют запоминания множества имен пользователя и сложных паролей, необходимых для доступа к разным приложениям.

Переход на аутентификацию по цифровым сертификатам

Вариант перехода на аутентификацию по цифровым сертификатам предполагает использование клонированных сервисов уровня приложений, работающих с той же базой данных, что и исходные сервисы, — Web- и Forms-серверами и др. Но в отличие от исходных сервисов, клонированные изначально настроены на использование HTTPS-протокола и обязательную двустороннюю аутентификацию с клиентом. Клон уровня приложений располагается в защищенном сегменте сети и доступен как для пользователей глобальной сети (например, через прокси-сервер), так и для пользователей локальной сети.

Такая схема (рис. 2.20) предоставляет следующие преимущества:

- возможность постепенного перевода пользователей с прежней системы аутентификации на новую систему;

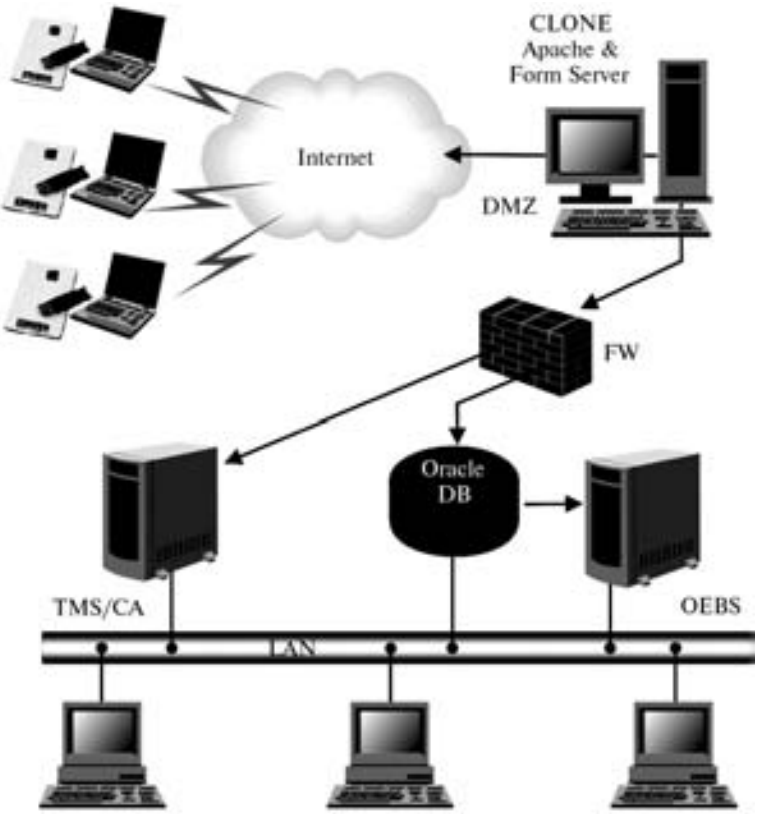

Рис. 2.20. Схема использования клонированных сервисов уровня приложений

- безопасное хранение ключевой информации;
- возможность безопасной работы в глобальной сети;
- возможность проверки подлинности клиентов, снижение рисков атак, например, путем подбора пароля.

На начальной стадии выполнения проекта необходимо развернуть следующие программные продукты: Oracle Internet Directory (OID), представляющий собой реализацию LDAP-каталога, и корпоративный удостоверяющий центр (УЦ) на базе Microsoft CA, который, помимо генерации цифровых сертификатов, обеспечивает организацию юридически значимого документооборота с применением ЭЦП в качестве аналога собственноручной подписи.

Двухфакторная аутентификация при доступе к СУБД позволяет на порядок повысить уровень информационной безопасности, проводить постоянный аудит всех действий в системе, а также полностью исключить перехват идентификационной информации пользователя потенциальным злоумышленником. Защита данных на рабочих станциях пользователей может быть реализована с помощью продукта Secret Disk компании Aladdin. Он обеспечивает защиту конфиденциальной информации, хранящейся и обрабатываемой на персональных компьютерах под управлением ОС Microsoft Windows.

Одним из преимуществ предложенного решения является организация удаленного доступа к бизнес-приложениям Oracle E-Business Suite с помощью защищенного SSL-протокола, обеспечивающего надежную защиту передаваемой информации. Соединение осуществляется в два этапа. Сначала в ходе двусторонней аутентификации сервера и пользователя происходит установление SSL-сессии и подтверждение подлинности обеих сторон. На втором этапе обеспечивается защита обмена данными с помощью шифрования канала, в результате чего достигается конфиденциальность и целостность передаваемой информации.

Предлагаемое типовое проектное решение позволяет существенно повысить уровень защищенности информации без внесения каких-либо изменений в систему. В результате компания получает возможность предоставлять пользователям безопасный доступ с удаленных рабочих станций к корпоративным информационным ресурсам на базе Oracle E-Business Suite. Доверенное информационное пространство можно расширить в случае роста потребностей компании, обеспечив при этом необходимый уровень информационной безопасности. Это решение необходимо, прежде всего, компаниям, располагающим развитой сетью удаленных филиалов или мобильных рабочих мест.

2.1.4. Управление доступом и учетными данными пользователей на основе программных продуктов Oracle Identity и Access Management Suite

Технологии Oracle для управления учетными данными пользователей, их правами и доступом

Приступая к реализации технологии управления учетными данными (реквизитами), правами и доступом пользователей, корпорация Oracle рассматривала три ключевых критерия, которые определяют современный подход к созданию корпоративных служб управления каталогами и учетными данными: полноту решения, интегрируемость, открытость и поддержку неоднородных сред.

Полнота решения. Современные требования к решениям по управлению учетными данными диктуют необходимость охвата полного спектра функциональных возможностей управления идентификацией — от первоначальной подготовки к работе до долгосрочного управления, от высокой безопасности доступа к развернутым в масштабах организации приложениям и информационным ресурсам до авторизации и аутентификации доступа с тонкой детализацией параметров доступа, определяемой политикой информационной безопасности организации.

Интегрируемость. Заказчики предпочитают работать с крупными производителями программного обеспечения, которые в состоянии тесно интегрировать технологии управления учетными данными и бизнес-приложения. Именно здесь достигается наибольший экономический эффект. Недостаточно просто предоставить инструменты для управления учетными данными и управления доступом. Заказчикам требуется, чтобы эти инструменты были полностью интегрированы в деловую активность организации. Технологии Oracle позволяют выполнять это критически важное требование и обеспечивают интеграцию с такими бизнес-приложениями, как Oracle E-Business Suite, mySAP Business Suite, PeopleSoft, JD Edwards, Siebel.

Открытость и поддержка неоднородных сред. Ключевое требование сегодняшнего дня состоит в том, что заказчикам необходимы решения, способные качественно работать в неоднородной ИТ-инфраструктуре. В ходе проектов по централизации ведения учет-

ных записей крупные организации часто встречаются с проблемой интеграции систем управления учетными данными с существующим ПО. Продукты Oracle специально разработаны так, чтобы упростить интеграцию. Существует библиотека заранее сконфигурированных коннекторов (адаптеров), которые обеспечивают доступ к большому количеству тиражируемых бизнес-приложений, использующихся в крупных организациях. Дополнительно каждый коннектор (адаптер) может быть переконфигурирован или доработан с помощью инструмента Oracle Adapter Factory. Запатентованная технология Oracle Adapter Factory позволяет быстро и без программирования выполнять интеграцию не только с тиражируемыми бизнес-приложениями, но и с приложениями, разработанными внутри организации.

Программные средства управления учетными данными пользователей, их правами и доступом Oracle Identity & Access Management Suite

В семейство программных продуктов компании Oracle под общим названием Oracle Fusion Middleware включено инфраструктурное программное обеспечение класса middleware (ПО промежуточного слоя) с широким спектром функциональных возможностей, в том числе — интегрированный набор средств управления учетными данными и управления доступом пользователей к корпоративным приложениям и информационным ресурсам. Данный интегрированный набор носит название Oracle Identity & Access Management Suite (Oracle IAMS), полный состав его компонентов представлен в табл. 2.2.

Кратко рассмотрим технологии хранения, доставки и управления учетными данными пользователей и их доступом к информационным ресурсам организации, а также программные продукты, входящие в состав Oracle Identity & Access Management Suite.

LDAP-каталог Oracle

Ядром службы управления LDAP-каталогами является программный продукт Oracle Internet Directory (OID).

Таблица 2.2

Функциональность и компоненты Oracle IAMS

Функциональность	*Название компонента*
Управление Web-доступом	Oracle Access Manager
Аудит и обеспечение соответствия законодательству	Oracle Identity Manager & Oracle Access Manager
Однократная регистрация в федеративных (партнерских) сетях	Oracle Identity Federation
Согласование идентификационных данных и их доставка во внешние хранилища	Oracle Identity Manager
Коннекторы (доставка ID-данных)	Oracle Identity Manager Connectors
Реализация LDAP-каталога	Oracle Inernet Directory
Виртуальный LDAP-каталог	Oracle Virtual Directory
Однократная регистрация на серверах приложений Oracle	Oracle SSO & Oracle Access Manager
Сервис делегирования прав администрирования	Delegated Administration Service
Платформа интеграции LDAP-каталогов	Directory Integration Platform

Oracle Internet Directory — это реализация протокола LDAP версии 3, объединяющая стандартные подходы к организации служб каталогов и опирающаяся на надежность и масштабность СУБД Oracle. Служба каталогов Oracle представляет собой приложение на основе СУБД Oracle, тесно интегрированное с сетевыми службами и управляющими средствами Oracle. Используя OID и применяя методы централизованной авторизации, можно хранить в едином хранилище данные о сервисах, предоставляемых продуктах, а также о пользователях и их правах в едином хранилище. OID опирается на СУБД Oracle и активно использует его возможности по обработке больших объемов данных и поддержке одновременной работы с базой данных большого числа пользователей. Емкость одного сервера каталогов оценивается в полмиллиарда записей.

СУБД Oracle — основа службы каталогов — спроектирована так, что системные операции, такие, как резервное копирование, добавление файлов данных, установка дополнительных приложений, могут проходить без остановки СУБД и не требуют отключения пользователей. Восстановление после системных сбоев происходит автоматически. Для обеспечения защиты от отказа аппаратных средств в архитектуру серверов LDAP заложена возможность развертывания распределенной системы, состоящей из нескольких отдельных серверов, обменивающихся информацией о происходящих изменениях и добавлениях. Во время простоя одного сервера LDAP другие берут на себя задачи обслуживания пользователей. После восстановления сервера, претерпевшего сбой, происходит полная синхронизация данных. Серверы OID пользуются проверенными на практике механизмами репликации данных Oracle Advanced Replication.

OID обеспечивает три уровня авторизации пользователей: анонимный доступ, доступ по паролю и авторизацию, основанную на сертификатах безопасности, распространяемых в рамках инфраструктуры SSL v3. Разграничение прав доступа осуществляется администратором. Он может гибко контролировать доступность элементов хранения каталога, предоставляя права и управляя доступом пользователей как к записям и их атрибутам, так и к целым ветвям дерева каталогов.

Управление Web-доступом

Технология разработана в целях обеспечения централизованного управления доступом корпоративных пользователей к информационным ресурсам организации с высокой степенью детализации прав и привилегий доступа, применяется для разнородных прикладных сред, а также интеграции с такими компонентами ИТ-инфраструктуры, как корпоративный информационный портал, программное обеспечение для организации коллективной работы с корпоративной информацией и бизнес-приложениями, например ERP, CRM, SCM.

Oracle Access Manager предоставляет комплексный набор сервисов по централизованному управлению доступом пользователей к различным информационным ресурсам предприятия, в том числе Web-ресурсам и приложениям. В программном продукте полностью реализована концепция защищенного доступа к ресурсам предприятия (аутентификация, авторизация и аудит). Развитые средства авторизации и аудита действий пользователей и администраторов системы позволяют существенно повысить уровень безопасности работы с информационными ресурсами.

Oracle Access Manager может работать с широким набором LDAP-каталогов, серверов приложений, Web-серверов, серверов порталов и бизнес-приложений, поставляемых ведущими производителями ПО.

Централизованное управление учетными записями пользователей, политиками доступа и аудита существенно снижает риски несанкционированного доступа к ресурсам, особенно для организаций с большим количеством сотрудников и различных информационных ресурсов.

Управлять учетными записями пользователей позволяют:

- развитые средства проектирования полей учетных записей пользователя, определения групп пользователей и организационной структуры предприятия, а также удобный интерфейс для создания учетных записей, групп, оргструктуры;
- широкий набор различных типов групп пользователей: статический, динамический, вложенный, гибридный, на основе подписки. Особенно интересны динамические группы, позволяющие определять группу на основе, например, условий назначения атрибутов учетных записей. Использование групп существенно упрощает администрирование политик доступа;
- средства автоматизации определения и исполнения потоков работ, состоящих как из шагов взаимодействия с различного рода администраторами/менеджерами, так и шагов по получению/передаче данных. Используются для реализации бизнес-процессов утверждения при регистрации пользователей, регистрации их в группах, для передачи идентификационных данных во внешние системы и др.;
- средства самообслуживания, которые дают возможность конечным пользователям самостоятельно создавать свои учетные записи, а также изменять в них данные (например, свои пароли) в рамках предоставленных им полномочий. В случае необходимости с изменением поля учетной записи может быть связан поток работ, который, может, например, запросить разрешение на конкретную операцию у руководителя данного сотрудника. Средства самообслуживания существенно снижают расходы организации на администрирование пользователей и их прав доступа;
- делегированное администрирование пользователей и политик доступа, которое обеспечивает создание многоуровневых иерархий администраторов, каждого со своими полномочиями, а также распределение нагрузки, и легко адаптируется к бизнес-структуре организации.

Особенностями управления доступом пользователей являются:

- поддержка аутентификации пользователей на основе имен и паролей, цифровых сертификатов, смарт-карт (в том числе — eToken), биометрии и др.;
- возможность взаимодействия с внешними системами с целью расширенной аутентификации и/или авторизации на основе имен и паролей, цифровых сертификатов, смарт-карт, биометрии и др.;
- поддержка авторизации пользователей и групп на основе политик авторизации (развитый аппарат для определения сложных политик доступа);
- наличие средств тестирования политик доступа и графического интерфейса для определения защищаемых информационных ресурсов и политик доступа;
- авторизация доступа к группе приложений на основе однократной аутентификации (Single Sign-On, SSO, федеративный SSO).

Oracle Access Manager позволяет осуществлять аудит действий, выполняемых средствами управления учетными данными и доступом пользователей, на основе политик аудита, при этом возможна запись данных аудита в базу данных, что повышает надежность и защищенность этих данных. Продукт поставляется с набором предопределенных отчетов, например, по неуспешным авторизациям (по пользователям или ресурсам), по созданию, активации, деактивации пользователей, по изменению данных в учетных записях.

Распространение и согласование учетных данных

Данная технология служит для автоматизации сложного и рутинного процесса регистрации и управления большим количеством учетных записей пользователей в неодно-

родной ИТ-инфраструктуре, когда имеется большое число различных LDAP-каталогов, разнородных приложений и общекорпоративных сервисов (таких, например, как электронная почта). Доставка учетных данных осуществляется с помощью программного продукта ***Oracle Identity Manager***, характерными особенностями которого являются:

- полный технологический цикл авторизации доступа, гарантирующий, что доступ к нужным ресурсам осуществляется быстро, непротиворечиво и в полном соответствии с корпоративными политиками доступа;
- прямое подключение (за счет использования коннекторов) к приложениям управления кадрами (Human Resourses Management Systems — HRMS) и их данным, что позволяет предоставлять сотрудникам организации санкционированный руководством доступ ко всем корпоративным приложениям и информационным ресурсам, которые им необходимы для выполнения должностных обязанностей;
- широкий спектр средств подключения (коннекторов) к операционным системам, базам данных, LDAP-каталогам, средствам обеспечения коллективной работы, приложениям и устройствам, что избавляет от рутинных работ по разработке дополнительных коннекторов.

Виртуальные каталоги

Программный продукт ***Oracle Virtual Directory*** позволяет отказаться от принципа физического хранения учетных данных в едином LDAP-каталоге. В качестве альтернативы Oracle Virtual Directory предоставляет возможность создавать представления, которые объединяют атрибуты идентификации данного объекта, взятые из других физически отделенных друг от друга хранилищ учетных данных, включая и LDAP-каталоги. Таким образом, создается виртуальный каталог, синдицирующий в режиме реального времени данные из различных хранилищ учетных данных и предоставляющий эти «взгляды» (views) общекорпоративным сервисам и приложениям. Особенно удобно использование виртуальных LDAP-каталогов при построении корпоративных порталов.

Однократная регистрация в федеративных (партнерских) сетях

По мере того как все больше организаций переносят свои бизнес-процессы в ИТ-инфраструктуру, появляется насущная потребность в расширении границ бизнес-процессов до дочерних структур и бизнес-приложений партнеров. Системы, которые помимо собственной ИТ-инфраструктуры, затрагивают также и ИТ-инфраструктуры партнерских организаций, носят название федеративных. Интеграция на федеративных началах (федерирование учетных данных) позволяет организациям работать независимо, но объединяться для достижения деловых целей.

Очевидно, что в федеративных системах для обеспечения доступа внешних пользователей к корпоративным приложениям и информационным ресурсам необходим жесткий учет регистрационных записей пользователей с целью защиты от несанкционированного доступа к корпоративным ресурсам. Работу с учетными данными в федеративных системах обеспечивает программный продукт Oracle Identity Federation, использующий для доступа к другим системам управления учетными данными пользователей многопротокольный шлюз, поддерживающий все стандарты федерирования, включая SAML, Liberty, WS-Federation.

В итоге успешно аутентифицированные в партнерской сети пользователи могут подключаться к ресурсам другой сети без повторной аутентификации.

2.1.4.1. Создание единой системы управления доступом, учетными данными и однократной регистрацией пользователей крупного предприятия на основе продуктов Oracle Identity Manager и Oracle Single Sign-On

Постановка задачи

Автоматизированная система управления (АСУ) крупного предприятия представляет собой информационно-технологическую систему, которая характеризуется:

- высокой степенью сложности,
- широким спектром прикладных задач, решаемых подсистемами, и
- разнообразием парка оборудования и базового программного обеспечения.

Структура АСУ предприятия, ее состав и взаимосвязи между подсистемами определяются функциональной структурой корпоративной системы управления предприятия. ИТ-инфраструктура предприятия состоит из множества разнородных автоматизированных систем, предназначенных для решения разных задач, обладающих различными функциональными возможностями и имеющих сложные связи между собой. Каждая из них использует собственные механизмы аутентификации и управления жизненным циклом учетных записей пользователей. Все идентификационные данные распределены по информационным системам, каждая система имеет собственное хранилище учетных записей, которыми управляют администраторы различных приложений. Подобный подход существенно усложняет процедуру управления доступом и учетными данными в рамках информационной системы всего предприятия, не позволяет централизованно управлять учетными записями и требует значительных затрат на администрирование приложений.

В качестве первоначального источника учетных записей пользователей на предприятии используется LDAP-каталог Microsoft Active Directory (MS AD). Кроме него существуют другие типы хранилищ учетных данных, которые используются различными приложениями (Lotus Notes, Oracle Financial Analyzer, Oracle E-Business Suite).

Для большинства приложений Oracle учетные данные хранятся в так называемой инфраструктуре сервера приложений, которая состоит из LDAP-каталога — Oracle Internet Directory (OID), системы однократной регистрации Web-приложений Oracle Single Sign-On (OSSO) и сервисов синхронизации учетных данных между OID и другими хранилищами Directory Integration Platform (DIP). Для работы с приложениями, работающими в архитектуре «клиент—сервер», пользователи регистрируются в базах данных Oracle как пользователи СУБД с соответствующими правами.

Цели и задачи решения

Важнейшими задачами проектирования системы управления доступом, учетными данными и однократной регистрации пользователей крупного предприятия являются:

- создание иерархии хранения учетных данных пользователей — работников предприятия;
- организация единого хранилища учетных записей;
- управление учетными данными и обеспечение их целостности и непротиворечивости;
- сокращение трудозатрат ИТ-специалистов и пользователей АСУ при управлении учетными данными;
- построение системы однократной регистрации, обеспечивающей подключение сотрудников со своих рабочих мест к информационным ресурсам предприятия без дополнительного предъявления учетных данных;
- синхронизация учетных данных в целевых системах в рамках всей информационной инфраструктуры предприятия.

В целях развития АСУ предприятия предусматривается совершенствование систем, автоматизирующих отдельные бизнес-процессы, более полная интеграция всех автоматизированных систем в единую АСУ предприятия, а также создание на предприятии единой системы управления доступом и учетными данными в рамках ИТ-инфраструктуры, которая объединяет:

- LDAP-каталог Microsoft AD;
- приложения Lotus Notes;
- информационную систему на основе БД Oracle;
- финансово-аналитическую систему Oracle Financial Analyzer;
- LDAP-каталог Oracle Internet Directory;
- комплекс бизнес-приложений Oracle E-Business Suite.

Кроме того, в ИТ-инфраструктуре крупного предприятия предусматриваются механизмы защиты от несанкционированного доступа к корпоративным приложениям и информационным ресурсам. Дополнительными требованиями к общему решению являются надежная аутентификация пользователей, а также консолидация средств контроля доступа для реализации полномасштабной политики информационной безопасности в рамках всех подсистем предприятия.

Описание решения

Система управления доступом, учетными данными и однократной регистрацией пользователей крупного предприятия строится на основе программных продуктов Oracle Identity Manager и Oracle Enterprise Single Sign-On Suite (ESSO). Особенность ESSO в том, что этот программный комплекс для прозрачного подключения пользователей к приложениям путем подстановки за них учетных данных работает и на рабочих станциях пользователей.

На первом этапе создается единое хранилище учетных данных (репозиторий), объединяющее учетные данные всех пользователей предприятия. Репозиторий управляется с помощью Oracle Identity Manager (OIM) и механизмов согласования с информационными ресурсами. Учетные данные пользователей из различных источников (в нашем случае это MS AD, OID и Oracle DB) собираются в репозитории OIM, где создаются глобальные учетные записи. Доверенным источником для таких записей может выступать LDAP-каталог MS AD. Далее глобальным учетным записям ставятся в соответствие учетные данные, которые необходимы для работы в прикладных системах.

Для построения системы управления учетными данными сначала обследуются выбранные прикладные системы (Microsoft Active Directory, Oracle E-Business Suite, приложения, хранящие учетные данные в БД Oracle) с целью получения информации, необходимой для проектирования архитектуры системы. На основании данных, полученных на этапе обследования, разрабатывается общая архитектура системы и упорядочиваются группы пользователей в рамках каждой из прикладных систем. Затем прикладная часть ПО Oracle Identity Manager устанавливается на сервер управления. Для интеграции с выбранными прикладными системами осуществляется необходимая доработка и установка адаптеров, позволяющих организовать информационный обмен учетными данными в прикладных системах. После этого определяются требования по управлению учетными данными и выполняется настройка политик управления этими данными.

После завершения работ по созданию единого корпоративного хранилища учетных данных пользователей и регистрации в LDAP-каталоге (MS AD) всех пользователей, которым разрешен доступ к корпоративным приложениям, к LDAP-каталогу подключается администратор Oracle Enterprise Single Sign-On Suite. Он создает и публикует в LDAP-каталоге шаблоны, обеспечивающие автоматический вход зарегистрированных пользовате-

лей в приложения. Клиентская часть ESSO позволяет автоматически выгружать эти шаблоны на рабочие станции, опознавать окна и формы приложений для ввода атрибутов аутентификации и подставлять в эти формы данные пользователей.

Для организации сквозного управляемого процесса от заведения учетной записи пользователя в MS AD до его прозрачного подключения к разрешенным корпоративным приложениям требуется интеграция системы однократной регистрации ESSO с системой распространения учетных данных пользователей (Oracle Identity Manager). Без такой интеграции администраторы прикладных систем сами должны создавать учетные записи пользователей в приложениях и каким-то образом сообщать им их учетные имена и пароли. Для интеграции выполняется установка адаптера OIM для ESSO, который позволяет безопасно помещать в контейнер пользователя на LDAP-каталоге его учетные данные для подключения к целевым системам.

Итак, на первом этапе с помощью программных продуктов Oracle Identity Manager и Oracle ESSO строится единая система управления учетными данными, к которой подключаются Microsoft AD, Lotus Notes и одна информационная система, построенная на БД Oracle.

На втором этапе происходит увеличение количества пользователей системы, и существующая архитектура системы управления учетными данными расширяется за счет программных комплексов OID, OEBS, OFA.

Функциональная архитектура решения и потоки данных между информационными системами представлены на рис. 2.21.

Для распространения однократно введенных учетных данных сотрудников в инфраструктуру предприятия вводятся Oracle Identity Manager и коннекторы к различным ин-

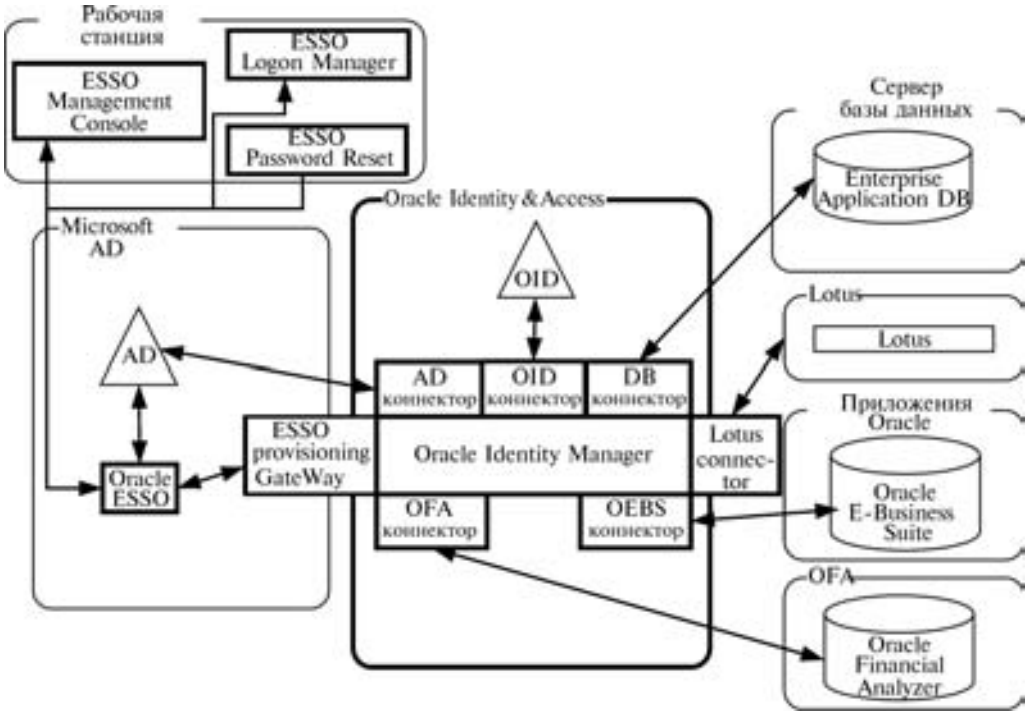

Рис. 2.21. Функциональная архитектура решения

формационным системам предприятия. Развертывание Oracle Enterprise SSO позволяет осуществлять прозрачное подключение пользователей при доступе к различным информационным системам предприятия на основе учетных данных приложений, которые клиентская часть ESSO извлекает из контейнера пользователя в MS AD.

Управление учетными записями и правами на информационные системы

OIM обладает функциональностью управления жизненным циклом учетных данных пользователей информационной системы. Для создания, изменения учетной записи, а также назначения, исключения прав на информационную систему предприятия либо администратор, либо сам пользователь инициирует запрос на выполнение потока работ в Web-интерфейсе OIM. Запрос проходит процесс согласования с уполномоченными лицами и после успешного утверждения OIM через соответствующие коннекторы осуществляет необходимые действия в конечных информационных системах и репозитории.

Применение Oracle Enterprise SSO

Для передачи на рабочие станции шаблонов и учетных данных ESSO может использовать LDAP-каталоги, базы данных и файловые хранилища. В данной архитектуре в качестве репозитория ESSO (и точки синхронизации с клиентами) используется MS AD.

На рабочие места администраторов устанавливается ESSO Management Console, с помощью которого администраторы настраивают пользовательские шаблоны для ESSO Logon Manager, а также управляют в целом функциональностью ESSO.

На рабочие места пользователей устанавливаются ESSO Logon Manager, который в автоматическом режиме скачивает из MS AD и применяет изменения, сделанные администратором ESSO. Logon Manager без вмешательства пользователей распознает окно запроса ввода имени и пароля (а также окно смены пароля) и автоматически вводит туда соответствующие учетные данные для информационной системы. Детали работы модуля и события подключения пользователя к приложениям аудируются.

Опциональный модуль ESSO Password Reset позволяет пользователям, забывшим свой пароль к MS AD, сменить его на контроллере домена после успешного ответа на несколько контрольных вопросов.

Oracle ESSO Provisioning Gateway позволяет заполнять пользовательский контейнер репозитория ESSO теми же данными из OIM, которые получают конечные информационные системы. Пользователь может не знать свой пароль и учетное имя в информационной системе, но при этом иметь доступ к информационной системе через ESSO Logon Manager.

Применение ESSO позволяет предоставлять доступ к информационным системам предприятия на основе единственной аутентификации на Microsoft Windows. Опционально ее можно заменить на более сильную аутентификацию с использованием, например, ключей или смарт-карт eToken компании Aladdin. Смена пароля или учетного имени в приложениях происходит без участия и ведома пользователя. Парольная политика ведется в OIM, пароли распространяются в информационные системы через соответствующие коннекторы.

В OIM предусмотрена возможность создания исторических отчетов о предоставленных пользователям правах доступа к прикладным системам.

Интеграция Oracle Identity Manager и Oracle ESSO в информационную систему предприятия позволяет создать единую систему управления учетными данными пользователей и их правами в корпоративной информационной системе, развернуть систему однократной регистрации, обеспечивать ведение общей политики паролей в информационной системе, а также аудит учетных данных и прав на ресурсы предприятия.

2.1.4.2. Организация единого доступа пользователей компании-оператора мобильной связи к сервисам, предоставляемым через web, на основе продуктов Oracle Virtual Directory и Oracle Access Manager

Постановка задачи

Компания — оператор мобильной связи предлагает своим клиентам различные Wap-сервисы и услуги, предоставляемые через Web, например, сервис самообслуживания (контроль счетов, смена тарифов), сервис загрузки контента, поисковый сервис и т. д. Для обслуживания пользователей (абонентов) в компании используется несколько Web-приложений, при этом часть их них принадлежит партнерам компании. Большинство приложений имеет собственную инфраструктуру:

- различные технологии формирования интерфейса пользователя (php, .NET);
- разные серверы приложений (MS IIS, Apache, SunJavaWS, JBoss);
- разные серверы баз данных (Oracle, MS SQL, MySQL, SunJavaDS).

Каждое приложение имеет собственных внутренних пользователей, для каждого из которых создается учетная запись. Если пользователь работает с несколькими приложениями, то для него создается несколько учетных записей. Учетные записи абонентов хранятся в базах данных приложений, т. е. каждое приложение располагает собственным, уникальным репозиторием пользователей (рис. 2.22). Все приложения оснащены инструментами управления учетными записями и правами доступа пользователей. Работа каждого приложения контролируется администраторами.

Цели и задачи решения

В связи с диверсификацией бизнеса, территориальным расширением и развитием деловых отношений с партнерскими организациями, предоставляющими услуги клиентам оператора мобильной связи, компании необходимо обеспечить качество, гибкость и

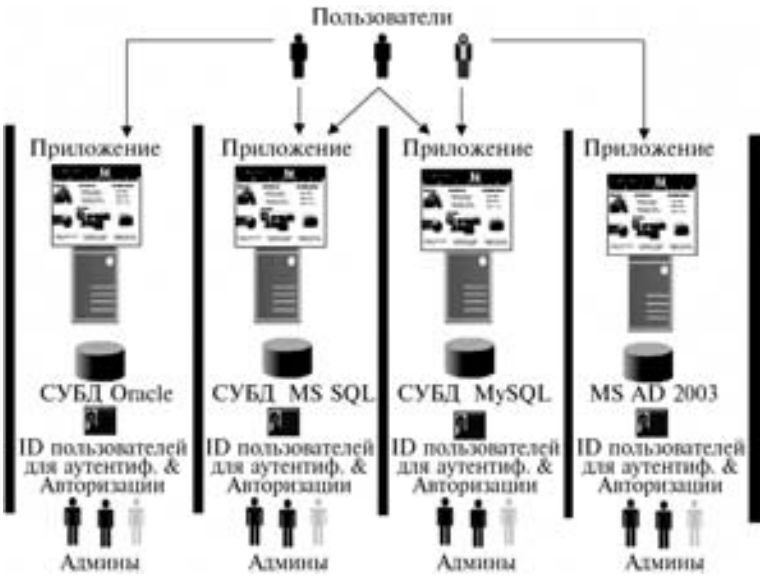

Рис. 2.22. Первоначальная организация доступа пользователей к сервисам, предоставляемым через Web

надежность сервисов и предложить своим абонентам и партнерам ряд дополнительных услуг для повышения безопасности и удобства работы с Web-приложениями.

Для организации единого доступа пользователей к сервисам, предоставляемым компанией через Web, необходимо создать единую базу учетных данных пользователей, минимально изменяя приложения и среду, в которой работают пользователи, и обеспечить плавный переход от существующих разрозненных систем аутентификации к системе однократной регистрации пользователей при работе со всеми Web-приложениями, консолидированными на портале (Web Single Sign On — WSSO).

Описание решения

Предлагается построить систему WSSO на базе программных продуктов ***Oracle Virtual Directory (OVD)*** и ***Oracle Access Manager (OAM)***, используя промышленное решение компании Oracle по консолидации учетных данных, расположенных в хранилищах различных типов, без их синхронизации. Oracle Access Manager может работать с широким набором LDAP-каталогов, серверов приложений, Web-серверов, серверов порталов и прикладных приложений, поставляемых ведущими производителями программного обеспечения. Oracle Access Manager предоставляет набор сервисов централизованного управления учетными данными пользователей и их доступом к различным информационным ресурсам компании, в том числе Web-ресурсам и приложениям. Oracle Access Manager обладает удобными средствами работы с различными группами пользователей, имеет встроенный механизм workflow для управления аутентификацией, авторизацией и созданием групп, развитые средства определения политик аутентификации, авторизации и аудита. Oracle Access Manager позволяет обеспечить однократную регистрацию пользователей (SSO) при работе с приложениями в архитектуре клиент—сервер.

Задача построения единого пространства для поиска учетных данных решается с помощью ***Oracle Virtual Directory (OVD)***, который обеспечивает представление существующих учетных данных пользователей в унифицированном виде (в форматах LDAP или XML) без синхронизации или перемещения данных из исходных мест хранения (баз данных и других источников).

Oracle Virtual Directory состоит из интерфейса LDAP, Web-шлюза, механизма Virtual Directory и адаптеров (рис. 2.23). Гибкий базовый механизм позволяет системным администраторам задавать сложные правила преобразования данных из формата хранения в исходном репозитории в форматы, необходимые различным клиентским приложениям. Если адаптер настроен для доступа к одному или нескольким источникам информации, запросы к различным частям иерархического дерева единого каталога автоматически перенаправляются серверам, содержащим достоверную информацию. Каждый источник

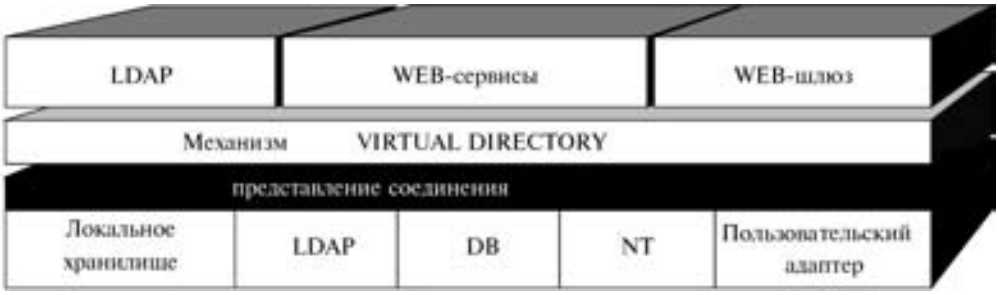

Рис. 2.23. Oracle Virtual Directory

можно настроить таким образом, чтобы поддерживался необходимый уровень его доступности и безопасности.

Внутри виртуального каталога в дереве данных о каталоге (Directory Information Tree — DIT) для каждого приложения создается своя ветвь пользователей, в результате возникает единое пространство для поиска пользователей. Именно на основе виртуального каталога

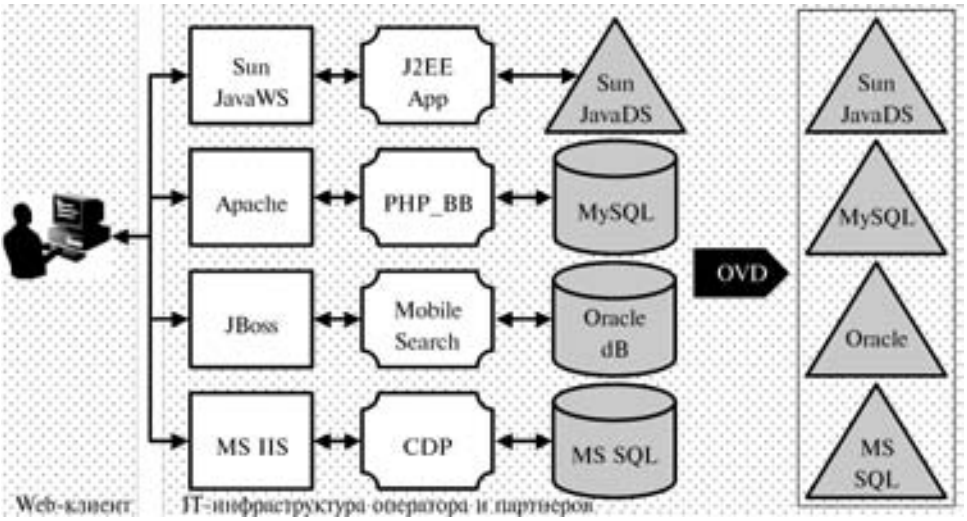

Рис. 2.24. Приведение всех ID-данных к одному формату и определение атрибутов для аутентификации

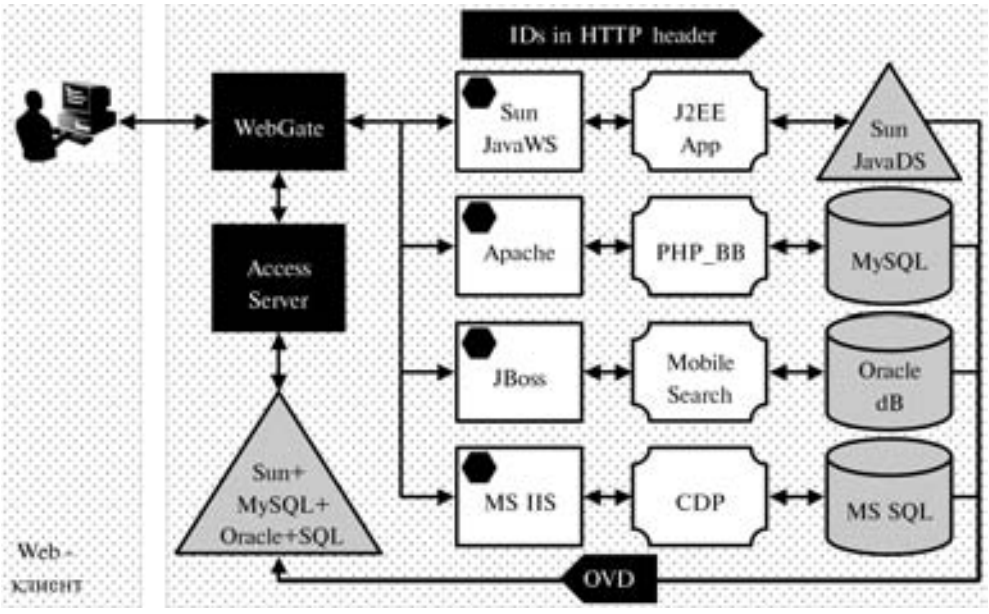

Рис. 2.25. Внешняя аутентификация пользователей приложениями по контексту http-заголовков

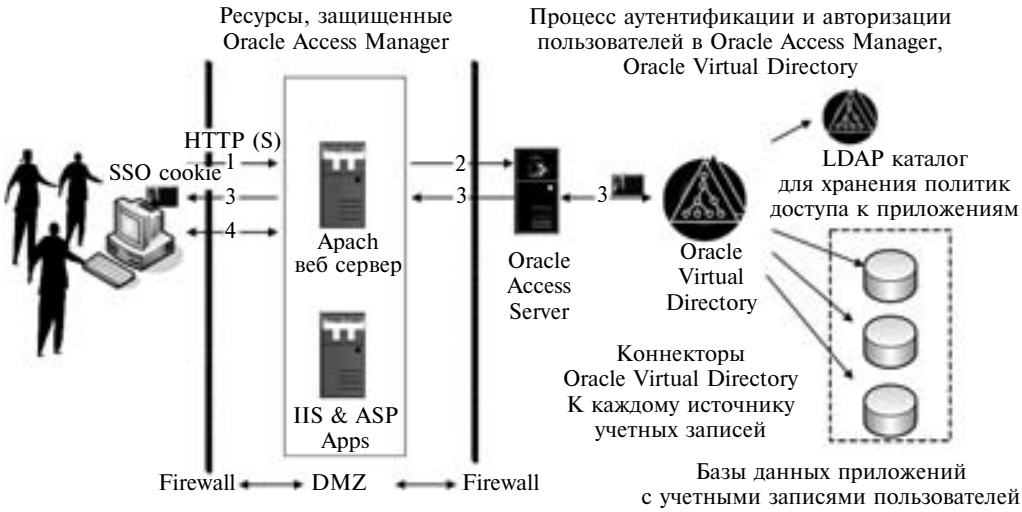

Рис. 2.26. Архитектура решения

в дальнейшем строится система проверки доступа пользователей к Web-приложениям. Схема реализации системы WSSO показана на рис. 2.24 и 2.25.

На первом этапе выполняется подключение Oracle Virtual Directory к различным хранилищам идентификационных данных с помощью стандартных адаптеров (см. рис. 2.24). Затем происходит связывание учетных данных, которые описывают одного и того же пользователя в разных системах, и формирование общего списка аутентификационных атрибутов.

На втором этапе устанавливается режим внешней аутентификации Web-приложений и с помощью специализированного шлюза Oracle Access Manager всем приложениям передается общий список аутентификационных атрибутов в http-заголовке сессии клиента (см. рис. 2.25). В результате обеспечивается однократная регистрация пользователей: пройдя аутентификацию в одном из Web-приложений, пользователи получают доступ ко всем приложениям.

Oracle Access Manager использует представление, полученное в Oracle Virtual Directory, в качестве основного источника информации о пользователях и их правах доступа. Каждое Web-приложение защищается шлюзом (модулем, входящим в составе OAM). Все обращения пользователей к приложениям контролируются этими шлюзами, где с помощью сервера Access Server выполняются аутентификация, авторизация и аудит действий пользователей. Процесс аутентификации и авторизации пользователей в системе представлен на рис. 2.26.

Ниже приведен алгоритм работы совместной работы приложений, Oracle Virtual Directory и Oracle Access Manager:

1. Пользователь запрашивает необходимое ему Web-приложение.

2. Запрос перенаправляется к Oracle Access Manager, который выполняет аутентификацию и авторизацию пользователя в Oracle Virtual Directory, а соответственно и в источниках учетной информации (например, в таблицах БД Oracle или MySQL).

3. Доступ к Web-приложению разрешается в случае успешной аутентификации и авторизации пользователя.

4. В ответ на запрос пользователя возвращается контент приложения и текстовый файл SSO cookie, который необходим для идентификации пользователя при работе с другими приложениями (WSSO).

Решение технических проблем

Аутентификация в обход стандартных механизмов

Решение Oracle предусматривает, что Web-серверы переводятся в режим внешней аутентификации, т. е. приложения считывают учетные записи из http-заголовков, а не проверяют правильность пары «имя—пароль» в своем хранилище. Эта работа возлагается на виртуальный каталог.

Аутентификация особых типов клиентов

В мобильной связи возможна аутентификация устройств по MSISDN при доступе абонента через сеть компании — оператора мобильной связи. В этом случае решение можно дополнить хранилищем атрибутов на RADIUS-сервере.

Для доступа к системе делегированных администраторов из филиалов и партнерских организаций решение Oracle может быть дополнено системами сильной аутентификациии с использованием жетонов/смарт-карт.

Первичная авторизация клиентов

После аутентификации пользователя одним из описанных ранее способов может быть сделан запрос в биллинговую систему для получения его статуса. В зависимости от результата (например, пользователь заблокирован) могут быть введены ограничения на доступ к определенным сервисам.

Отказоустойчивость системы

Для обеспечения работы системы в целом необходимо обеспечить отказоустойчивость модулей «сервер доступа» и «виртуальный каталог». Архитектура Oracle Access Manager позволяет осуществлять баллансировку нагрузки между несколькими серверами доступа, каждый из которых может обращаться к нескольким каталогам.

Мониторинг системы

Поскольку модули системы могут быть расположены далеко друг от друга, необходимо, по крайней мере, контролировать их доступность. Для этого можно использовать встроенные агенты SNMP-мониторинга Oracle Access Manager. В случае необходимости контролировать производительность различных компонентов системы и отслеживать уровни сервиса решение может быть дополнено подключаемым модулем для Oracle Enterprise Manager, который называется Identity Management Pack.

2.1.4.3. Создание единой службы управления доступом и учетными данными пользователей в государственной организации федерального уровня

Постановка задачи

Автоматизированная система управления (АСУ) крупной государственной организации федерального уровня представляет собой распределенную по территории Российской Федерации информационно-технологическую систему, которая характеризуется высокой степенью сложности, широким спектром решаемых подсистемами прикладных задач и разнообразием парка оборудования и базового программного обеспечения.

Клиентами информационных ресурсов организации федерального уровня являются пользователи, подключающиеся через специализированное клиентское ПО в удаленных отделениях организации. Информационные ресурсы, к которым они получают доступ, — специализированное серверное ПО, работающее с данными, хранящимися в базе данных Oracle DB. Для обеспечения масштабности и отказоустойчивости системы на региональном

уровне установлены серверы промежуточного слоя, которые являются точками контакта для клиентов, где необходимо осуществлять аутентификацию и авторизацию клиентов.

Аутентификация и авторизация выполняются на основе цифровых сертификатов, выдаваемых головным Удостоверяющим Центром. Авторизованные клиенты получают доступ к информационным ресурсам и в зависимости от предоставленных им прав могут читать или изменять хранящуюся в базе данных информацию. Подключение клиентов проходит в защищенном режиме с помощью шифрования.

Цели и задачи решения

Централизованная система управления доступом является одной из ключевых служб, штатная работа которой позволяет решить широкий спектр задач обеспечения информационной безопасности организации. Необходимость предоставлять авторизованным пользователям право изменять данные организации федерального уровня и в то же время обеспечивать защиту от несанкционированного доступа — наиболее очевидные из них. Учитывая ценность конфиденциальных данных организации, решение должно предусматривать механизмы, позволяющие быстро реагировать на изменяющиеся требования со стороны пользователей и владельцев информации.

Права пользователей на доступ к ресурсам наиболее удобно определять в LDAP-каталогах, предоставляющих универсальный способ хранения и обработки регистрационных данных пользователей информационных систем, учетных данных субъектов информационно-вычислительных процессов, компонентов инфраструктуры и т. д. Наличие LDAP-каталогов позволяет целиком вынести за рамки приложений все, что касается обработки учетных данных, и предоставлять эту обработку приложениям по стандартизованному LDAP-протоколу как общедоступный сервис. Следующие задачи — аутентификация пользователей, анализ их запросов на доступ к ресурсам и собственно предоставление доступа к ресурсам — требуют обращений к LDAP-каталогам и формируют дополнительные требования к общему решению по управлению доступом.

Необходимо также иметь в виду, что в ряде подсистем идентификационные данные пользователей могут храниться не в LDAP-каталогах, а непосредственно в базах данных, с которыми работают корпоративные приложения, или в доменах Microsoft Windows NT. Все эти хранилища учетных данных нужно интегрировать. Однако простое хранение идентификационных данных пользователей в LDAP-каталогах и их использование в локальных приложениях не являются комплексным решением, необходима единая служба управления LDAP-каталогами и идентификационными данными пользователей.

Должны быть предусмотрены механизмы интеграции со средствами сильной аутентификации, территориальная распределенность и достаточное количество точек аутентификации, наличие интерфейсов администрирования (в том числе — делегированного) и самообслуживания, проверка политик (например, диапазонов IP-адресов), поддержка федеративного доступа с установлением доверительных отношений между хранилищами учетных данных нескольких организаций, аудит действий пользователей организации и т. п.

Основными целями создания единой службы управления доступом АСУ организации федерального уровня являются:

- консолидация средств контроля доступа, аутентификации и аудита для реализации полномасштабной политики информационной безопасности в рамках всех подсистем организации, организация единой точки входа для тех подсистем, где это необходимо;
- автоматизация процессов регистрации учетных записей клиентов АСУ организации, назначения им прав пользования ресурсами АСУ организации, выдачи и аннулирования сертификатов;

- максимально возможная централизация решения с учетом специфики территориальной распределенности организации и необходимости обеспечивать точки доступа для представителей других государственных структур по всей Российской Федерации;
- повторное использование компонентов решения для обеспечения федеративного доступа.

Важнейшими задачами являются создание надежной, гибкой и открытой для контроля соответствующими органами инфраструктуры управления доступом, обеспечивающей бесперебойное функционирование АСУ организации федерального уровня и ее развитие в перспективе.

Описание решения

Концепция защищенного доступа к информации (авторизации, аутентификации и аудита) может быть в полной мере реализована только в системе, где обеспечены единство и унификация средств управления отдельными компонентами информационной инфраструктуры. При проектировании подобных систем необходимо применять модульный принцип, позволяющий интегрировать и повторно использовать при необходимости отдельные компоненты. Решение задачи создания единой службы управления доступом — это, прежде всего, построение правильной архитектуры, позволяющей логически выделить и сгруппировать специализированные модули. Типовая архитектура развертывания единой службы управления доступом, обычно бывает представлена пятью уровнями:

- службы каталогов;
- репозитория (хранилища) политик;
- принятия решений (слоем приложений);
- применения политик;
- интеграции (слоем программных интерфейсов).

Для объединения существующих подсистем в рамках АСУ организации федерального уровня используется интегрированный набор средств управления учетными данными Oracle Identity & Access Management Suite, компоненты которого функционально соответствуют всем пяти уровням. Создание единой службы управления доступом АСУ организации федерального уровня осуществляется на базе программных продуктов Oracle Access Manager и Oracle Identity Federation. В случае необходимости синхронизации учетных данных эти продукты могут быть дополнены Oracle Identity Manager.

На рис. 2.27 представлена схема возможной интеграции служб управления доступом и учетными данными при наличии нескольких хранилищ учетных данных.

Рис. 2.27. Схема интеграции служб управления доступом и учетными данными

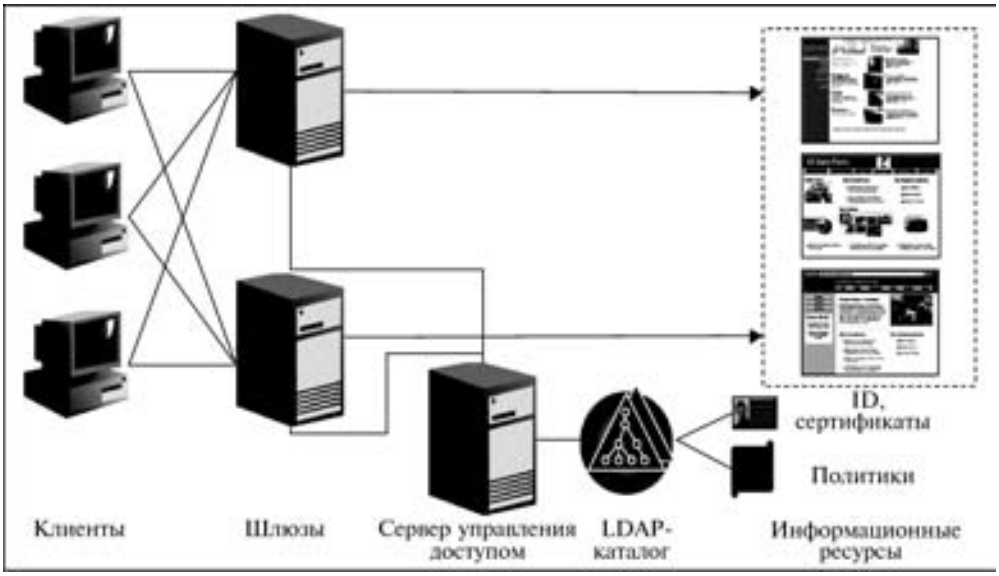

Рис. 2.28. Схема взаимодействия компонентов единой службы управления доступом

Рис. 2.28 иллюстрирует схему взаимодействия компонентов единой службы управления доступом. Подобная схема позволяет обеспечивать гибкость при централизованном управлении доступом территориально распределенных клиентов к информационным ресурсам организации.

Архитектурное решение

Архитектурное решение, которое может быть внедрено в ИТ-инфраструктуре крупной организации федерального уровня при создании полномасштабной службы управления доступом, представлено в виде схемы на рис. 2.29.

Пилотный проект

Предлагаемое решение целесообразно внедрять в рамках пилотного проекта на стенде, воспроизводящем топологию работы АСУ: «клиент — сервер промежуточного слоя — сервер приложений — база данных». На этапе пилотного проекта необходимо продемонстрировать жизнеспособность решения и оценить ресурсы, необходимые для полномасштабного внедрения.

В первую очередь надо обеспечить интеграцию специализированного приложения для доступа удаленных клиентов к информационным ресурсам организации федерального уровня и программного продукта Oracle Access Manager. Эта интеграция позволит переложить решение многих проблем обеспечения безопасности с прикладной системы на централизованную систему управления доступом.

Интеграцию целесообразно осуществлять с использованием интерфейсов, на которых написано приложение, а для подключения к Oracle Access Server использовать AccessGates (блок «1» на рис. 2.29). AccessGates являются теми самыми шлюзами, которые перехватывают запросы клиентов к ресурсам и проводят их авторизацию. После этого можно развернуть основную инфраструктуру (Oracle Access Server, Oracle Identity Server и Oracle Access Manager — блок «2» на рис. 2.29) и связать ее со службой каталогов (блок «3» на рис. 2.29).

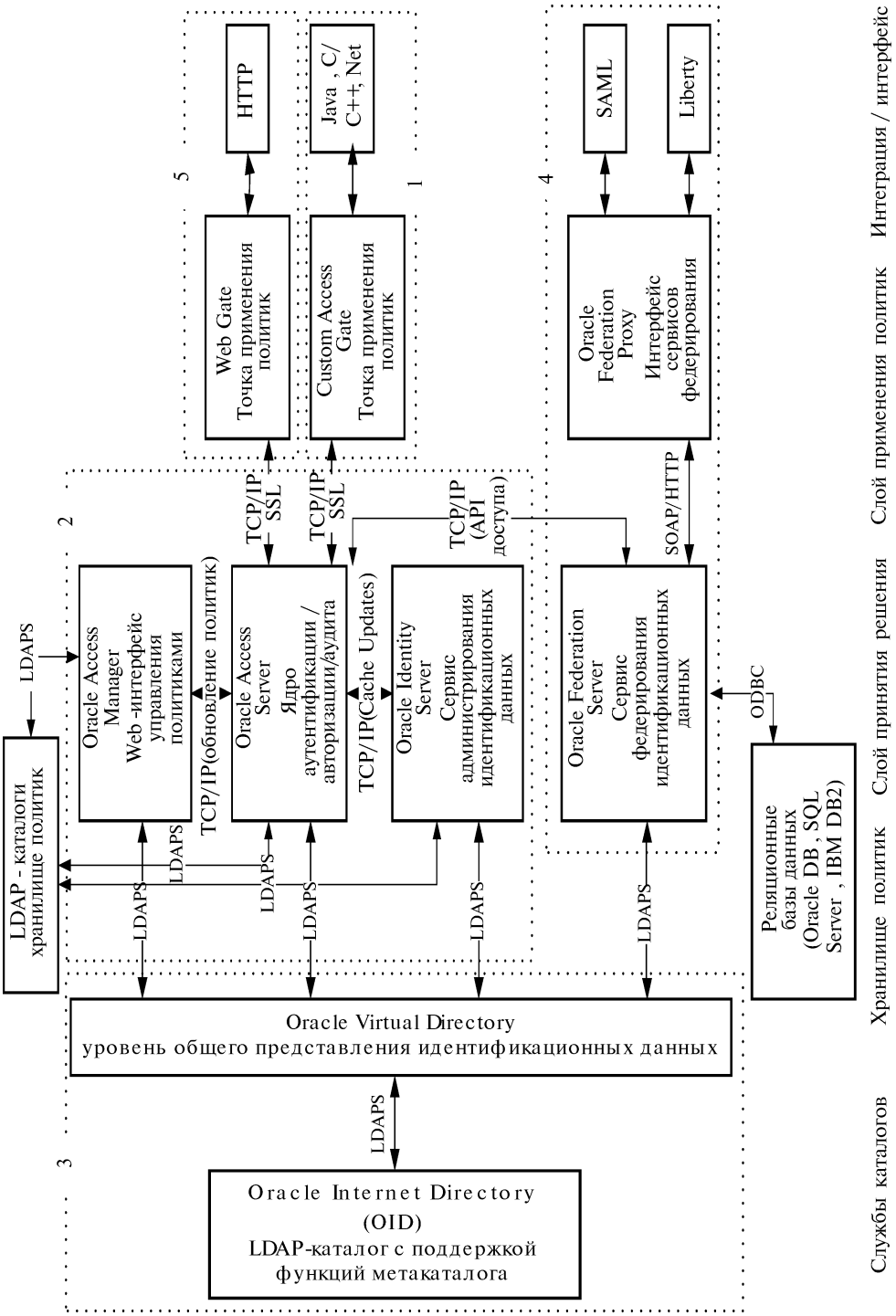

Рис. 2.29. Модульная схема развертывания единой службы управления доступом

Первый этап проекта — создание службы управления доступом в одном регионе

На этом этапе на передний план выступают вопросы оптимизации; в частности — обеспечения отказоустойчивости системы и минимизации расходов. Схема развертывания предполагает установку точек доступа AccessGates во всех региональных центрах, а серверов Access Server — в самых крупных из них. Точки доступа AccessGates настраиваются на последовательный опрос списка из ближайших серверов Access Server и при отсутствии у какого-нибудь сервера Access Server соединения с другими компонентами Oracle Identity & Access Management Suite или со службой каталогов переключаются на следующий.

Также на этом этапе оценивается, стоит ли использовать стандартную службу каталогов (Oracle Internet Directory или MS Active Directory) или перенести их представление на базе Oracle Virtual Directory на уровень крупных региональных центров (см. блок «3» на рис. 2.29).

Еще одна задача на этом этапе — настройка аудита; точнее — выбор наиболее актуальных типов отчетов, предоставляемых Oracle Access Manager, и создание собственных типов отчетов.

Второй этап проекта — построение службы управления доступом во всех регионах

В связи с ожидаемым резким ростом числа пользователей системы на этом этапе особое внимание следует уделить административным задачам, которые неизбежно возникнут в процессе внедрения. Совместное применение регламентов и инструментов управления действиями пользователей, которые предоставляет Oracle Access Manager, позволяет решить эти задачи.

На этом этапе можно внедрить дополнительные средства — средства самообслуживания, которые позволят запускать потоки работ для автоматизированного создания учетных записей и сертификатов пользователей и предоставления им прав на ресурсы. При этом возможны варианты с оповещением владельцев ресурсов или делегированных администраторов. Кроме того, необходимо настроить систему мониторинга, отслеживающую состояние территориально распределенных компонентов Oracle Access Manager. Использование поставляемого файла спецификации MIB позволяет дистанционно получить детальную информацию и быстро локализовать неисправности.

Третий этап проекта — обеспечение федеративного доступа

При построении системы доступа других государственных организаций к ресурсам организации федерального уровня логично повторно использовать готовую инфраструктуру, созданную на предыдущих этапах. Oracle Identity Federation позволяет использовать на стороне поставщика услуг (которые будет оказывать организация федерального уровня в виде Web-доступа к своим данным) Oracle Access Manager. Решение обеспечивает безопасную передачу результата успешной аутентификации пользователей на стороне потребителя услуг и его прозрачное подключение к партнерским Web-сервисам с заранее предопределенными правами.

Также ранее созданная инфрастуктура Oracle Access Manager позволит пользователям АСУ организации федерального уровня через Oracle Identity Federation в будущем получать доступ к Web-сервисам других государственных организаций. Для этого они могут использовать те же сертификаты, но точками доступа будут не требующие разработки AccessGates, а готовые WebGates (см. блок «5» на рис. 2.29).

Предложенное архитектурное решение может служить стандартом при построении систем управления доступом для организаций федерального масштаба.

Глава 3
ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ДОСТУПА К ДАННЫМ И ПРИЛОЖЕНИЯМ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНИЗАЦИИ НА ОСНОВЕ ПРОДУКТОВ КОМПАНИИ CITRIX SYSTEMS

3.1. Описание продуктов компании Citrix Systems

Развитие информационных технологий привело к тому, что теперь обыкновенные пользователи могут получить доступ к своим данным и приложениям, находясь вне офиса. И для получения доступа нет необходимости обладать какими-либо «тайными знаниями», эта возможность сегодня встраивается в современные операционные системы. Естественно, рассматривая возможность предоставления сотрудникам такого доступа, необходимо особенно тщательно проработать вопросы обеспечения безопасности этого доступа. С одной стороны, консолидация данных и приложений в Дата-центре повышает безопасность, так как нам достаточно обеспечить их защиту (физическую, электронную и др.) всего лишь в одном или очень небольшом количестве мест. Дата-центр — Центр Обработки Данных (ЦОД) — это специализированная площадка, на которой организация размещает серверное и телекоммуникационное оборудование. Данная площадка (здание) обеспечивает все необходимые требования по электропитанию, охлаждению, физической безопасности. К данной площадке подводятся используемые организацией каналы связи. Крупные организации обычно располагают своим собственным ЦОД, средние и мелкие могут арендовать такие помещения у специализированных организаций (обычно провайдеров).

Но, с другой стороны, пользователи которые получают доступ к этим данным и системам часто находятся не в «мирном» офисе, подключенном к Дата-центру своими защищенными каналами, оснащенные системами обнаружения и предотвращения атак, антивирусными средствами и межсетевыми экранами, а используют любое доступное им устройство (ноутбук, Интернет-киоск, смартфон) и доступные каналы связи, где никто не гарантирует отсутствие лиц, которые могут быть заинтересованы в незаконном получении доступа к ценной информации. Задача архитектора таких систем, с одной стороны, обеспечить максимальную защищенность, а с другой стороны, не усложнить пользователю работу настолько, что последний просто откажется использовать данную возможность.

Компания Citrix Systems разработала систему продуктов, которые обеспечивают выполнение приведенных выше требований.

Рассмотрим сначала продукты компании Citrix Systems в целом, а затем более подробно остановимся на некоторых из них. Чтобы нам было проще описывать всю систему, обратимся к рис. 3.1.

С левой стороны мы видим пользователей информационных систем, а справа располагается Дата-центр, где установлены корпоративные приложения.

Итак, начнем с Дата-центра.

Citrix XenServer — программный продукт, предназначенный для виртуализации операционных систем. Виртуализация — технология или набор технологий, позволяющих сделать вычислительные ресурсы автономными и независимыми от окружающих компонентов. Особенностью данного продукта является использование гипервизора Xen, под-

Рис. 3.1. Инфраструктура доставки приложений компании Citrix Systems

держивающего паравиртуализацию. Гипервизор — микроОС, которая предоставляет сервис виртуальных машин операционным системам, установленным поверх нее, обеспечивая изоляцию гостевых ОС друг от друга, защиту, безопасность и эмуляцию определенных компонентов в случае необходимости, а также разделение и управление ресурсов хост-машины. Паравиртуализация — метод виртуализации, при котором операционная система виртуальной машины «знает» о том, что она работает в виртуальной среде. Это достигается за счет модификации виртуализированной операционной системы.

В поставку данного ПО в зависимости от редакции может входить Citrix Provisioning Server for Data Center.

Citrix Provisioning Server — программное обеспечение, позволяющее осуществлять потоковую доставку операционных систем (серверных или клиентских) по сети, в том числе на компьютеры, не имеющие жестких дисков. Здесь необходимо отметить, что в данном случае вся вычислительная работа выполняется на том устройстве, куда происходила потоковая доставка.

Citrix NetScaler — аппаратный комплекс, обеспечивающий доставку Web-приложений конечному пользователю. В этот комплекс заложены механизмы, обеспечивающие: мультиплексирование запросов, сжатие информации и ее кеширование, перенаправление запросов, балансировку нагрузки, анализ трафика как в направлении Web-сервера, так и в обратном, защита трафика и логики приложений с помощью межсетевого экрана приложений.

Citrix XenApp — программное обеспечение, отвечающее за доставку пользователям приложений Windows. Пользователь получает на используемое устройство, на котором запущен клиент Citrix Application, изменения экрана, а на сервер, в свою очередь, передаются коды нажатых на клавиатуре клавиш и изменения позиций курсора. Приложение в данном случае выполняется на стороне сервера и использует его вычислительные ресурсы. Таким образом, мы получаем независимость от операционной системы и аппаратного обеспечения на стороне клиента, так как основная функция клиента — только отображение информации.

Citrix XenDesktop — система доставки персональных компьютеров из Дата-центра на устройство пользователя. Под доставкой персонального компьютера понимается доставка графического интерфейса клиентской операционной системы. При этом персональный компьютер, находящийся в Дата-центре, может представлять собой виртуальную машину или аппаратный комплекс, например блейд-ПК. Блейд-ПК — разновидность персонального компьютера, представляющего собой модуль, содержащий в себе процессор, память,

материнскую плату и устанавливаемый в специализированное шасси. Жесткий диск и видеоподсистема могут быть опциональными. Все операции ввода-вывода осуществляются через шасси, которое также содержит в себе модули управления. Доступ пользователей к таким ПК осуществляется только по сети.

Необходимо отметить, что в этом продукте используются технологии, заложенные в Citrix XenApp, и в зависимости от редакции могут быть доступны дополнительные компоненты. Редакция ПО — это разновидность ПО от одного производителя, имеющая одинаковый базовый функционал и отличающаяся друг от друга дополнительным функционалом или дополнительными продуктами, поставляющимися в рамках той или иной редакции.

Citrix Access Gateway — аппаратный комплекс, обеспечивающий безопасный доступ пользователей к своим данным и приложениям. Предоставляет SSL-VPN-доступ, основным отличием от других решений является наличие технологии SmartAccess. Данная технология позволяет контролировать доступ, основываясь не только на аутентификации, но также и на параметрах устройства, с которого осуществляется доступ.

Все перечисленные компоненты устанавливаются в Дата-центре, а сейчас мы перейдем к тем программным и аппаратным комплексам, которые могут также быть установлены и на стороне клиента, на его устройстве доступа или находиться в его удаленном офисе.

Citrix WANScaler — программно-аппаратный комплекс, обеспечивающий оптимизацию использования WAN-каналов. Ускорение работы достигается за счет использования технологий: сжатия, битового кеширования, оптимизации работы некоторых протоколов, присвоения приоритета различным видам трафика. Это решение — симметричное, т. е. для своей работы требует установки двух аппаратных комплексов, по одному с каждой стороны WAN-канала или установки аппаратной части с одной стороны, и программной части с другой стороны.

Citrix EdgSight — группа программных продуктов, осуществляющих мониторинг производительности клиентских систем или терминальных сессий. Также существует специальная версия EdgeSight for LoadTesting для проведения нагрузочного тестирования.

На данной схеме указаны не все продукты, поэтому еще хочется отметить программу **Citrix Password Manager** — решение Single Sign-On в масштабе всего предприятия. Данный продукт осуществляет управление паролями для Web, Windows или Хост-приложений, а также подстановку учетных записей для этих приложений в соответствующие диалоговые окна.

В данной книге мы будем рассматривать только программное обеспечение для доставки Windows-приложений — **Citrix XenApp**.

3.2. Компоненты систем, построенных с использованием XenApp

Прежде чем начать обсуждение процесса аутентификации и авторизации в системах, построенных с использованием XenApp, необходимо остановиться на компонентах, из которых эти системы строятся.

Существует несколько версий и редакций программного обеспечения Citrix Systems, с помощью которого строятся системы удаленного доступа.

1. **Citrix Access Essentials 2.0** — версия для малого бизнеса, с ограничением в максимальное количество пользователей — 75.

2. **Citrix Presentation Server 4.0 for UNIX** — версия для заказчиков, использующих IBM AIX, HP-UNIX или Solaris. Эту версию в данной книге мы не рассматриваем.

3. **Citrix XenApp Server 4.5** — версия, работающая под ОС Microsoft Windows Server 2003. (В середине 2008 г. планируется выпуск новой версии, которая будет работать, используя новую версию ОС Microsoft Windows 2008, представленную в феврале 2008 г.).

Версия Citrix XenApp Server 4.5 существует в трех редакциях — Advanced, Enterprise и Platinum. Для процессов аутентификации и авторизации они не различаются, так же как не различаются Citrix Presentation Server и Citrix Access Essentials.

Итак, в системе присутствуют следующие компоненты.

1. **Citrix Secure Gateway** — предназначен для обеспечения шифрования SSL/TLS между безопасным сервером-шлюзом и клиентским ПО с поддержкой SSL, а также для шифрования данных http-трафика, передаваемого между веб-сервером и веб-браузером.

2. **Citrix Web Interface** — веб-сервер, предназначенный для представления приложений и данных пользователю информационной системы в виде веб-страницы. Возможна интеграция с портальными решениями, такими как IBM WebSphere и Microsoft SharePoint. Портал — веб-сайт (чаще внутренний) организации, тесно интегрированный с корпоративными информационными системами. Обычно имеют модульную структуру, а также возможность персональной настройки для конкретного пользователя или группы пользователей.

3. **Citrix License Server** — обрабатывает запросы на установление соединения с фермой серверов XenApp Server и предоставляет необходимую для работы пользователя лицензию. Ферма — в терминологии Citrix Systems группа серверов XenApp.

4. **Secure Ticket Authority (STA)** — XML Web служба, которая обменивается информацией с сервером XenApp с помощью случайно сгенерированных билетов. Используется для контроля доступа к серверу Citrix Secure Gateway.

5. **Citrix XenApp Server** — предоставляет пользователю возможность выполнения «опубликованных» на сервере или группе серверов приложений.

6. **Citrix XenApp Client** — программное обеспечение, предназначенное для подключения и использования ресурсов Citrix XenApp Server.

На приведенной ниже схеме (рис. 3.2) можно увидеть одну из возможных конфигураций использования Citrix XenApp Server.

Для проверки подлинности и прав доступа пользователей программное обеспечение Citrix Systems активно использует возможности служб каталога, совместно с которыми

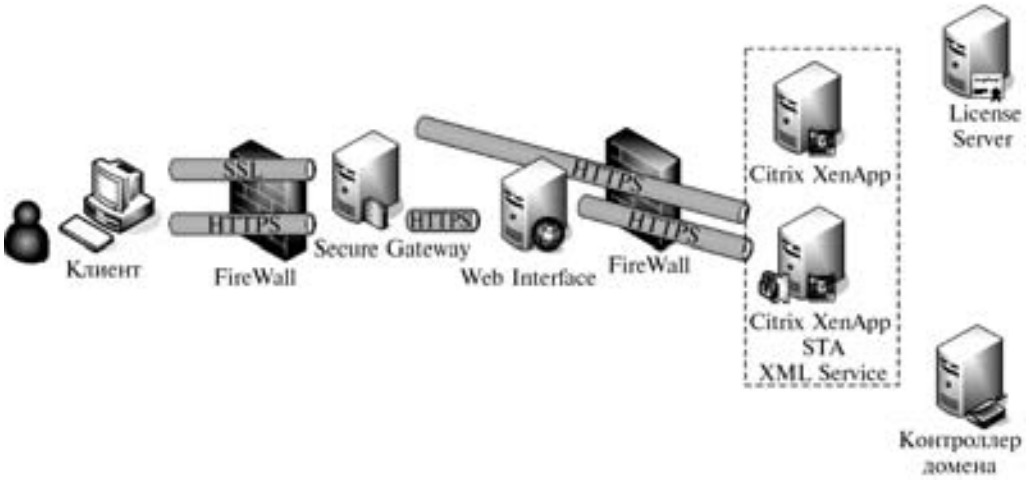

Рис. 3.2. Примерная схема подключения пользователя к Citrix XenApp

это ПО работает. Служба каталогов — иерархическая служба, содержащая в себе информацию об объектах организации и их свойствах. Так, Citrix XenApp поддерживает работу при использовании в организации как службы каталога Active Directory компании Microsoft, так и Novell Directory Services (NDS).

Аутентификация

Аутентификация в среде Citrix XenApp осуществляется с помощью следующих механизмов:

- пароли;
- смарт-карты;
- токены;
- биометрические решения.

Некоторые из этих решений могут потребовать дополнительные программно-аппаратные комплексы, которые приобретаются у других поставщиков.

Вышеперечисленные механизмы для своей работы используют один из следующих протоколов аутентификации:

- Windows NT LAN Manager (NTLM);
- Kerberos.

Каждый из рассматриваемых механизмов обладает как достоинствами, так и недостатками. Для выбора механизма аутентификации при внедрении решения необходимо учитывать множество факторов, таких, например, как цена решения, возможность подключения дополнительного оборудования к клиентским устройствам, необходимость обучения пользователей и т. д. Заметим также, что смарт-карты, токены и средства биометрии предоставляются сторонними поставщиками и должны иметь явную поддержку от Citrix Systems или поставщика решения для функционирования в среде Citrix. Некоторые из этих решений могут потребовать дополнительных аппаратных или программных компонентов или не поддерживаться в среде Citrix. Поэтому перед выбором решения необходимо учитывать эти факторы и проконсультироваться с поставщиком решения.

Протоколы аутентификации WINDOWS NT LAN Manager (NTLM)

NTLM (Windows NT LAN Manager — протокол типа отклик—отзыв) — сетевой протокол аутентификации. Он встроен в Windows и является методом аутентификации по умолчанию между хост-машинами Windows в сети. Этот протокол позволяет пользователям аутентифицироваться на удаленных машинах. NTLM может быть использован для аутентификации напрямую между двумя узлами в сети или с помощью контроллера домена как доверенного источника.

Оригинальный протокол NTLM работал поверх протокола Server Message Block (SMB). ПО Citrix использующее NTLM для аутентификации применяет более новый стандарт, который туннелирует аутентификацию NTLM с использованием протокола Hypertext Transfer Protocol (HTTP).

Аутентификация Kerberos

Citrix XenApp расширяет использование протокола Kerberos. После того, как пользователь входит в систему на клиентском устройстве, он может подключиться к Citrix XenApp без необходимости проходить снова аутентификацию. Пароль пользователя не передается на Citrix XenApp, вместо этого происходит обмен токенами аутентификации согласно Generic Security Services API (GSSAPI) стандартизованного в Internet RFC 1509.

Этот аутентификационный обмен происходит внутри виртуальных каналов протокола Citrix ICA и не требует никаких дополнительных протоколов или портов. Также нужно отметить, что этот аутентификационный обмен не зависит от метода входа в систему, и поэтому может быть использован совместно с паролями, смарт-картами или биометрическими методами. Для использования аутентификации Kerberos в Citrix XenApp клиент и сервер должны быть правильно сконфигурированы. При необходимости Групповые Политики Службы Каталога Microsoft могут быть также использованы для выборочного отключения аутентификации Kerberos для определенных пользователей или серверов.

Безопасные коммуникации

Коммуникации между продуктами Citrix должны быть аутентифицированы и иметь защиту целостности. Одним из вариантов обеспечения безопасности коммуникаций является использование технологий шифрования, таких как SSL, Transport Layer Security (TLS) или IPSec. В ряде решений эти технологии безопасных коммуникаций усиливают безопасность продуктов Citrix. В других решениях безопасные коммуникации являются обязательной составляющей для функционирования продуктов Citrix.

SSL/TLS

SSL и TLS — стандартные протоколы для обеспечения безопасных коммуникаций. Эти протоколы используют сертификаты для аутентификации вовлеченных в процесс передачи участников и договариваются о ключах сессии, которые будут использованы для шифрования трафика между участниками. SSL/TLS также использует клиентские сертификаты для взаимной аутентифкации. SSL/TLS может инкапсулировать и шифровать трафик других протоколов, таких, например, как HTTP, и защищать их от разглашения и фальсификации.

HTTPS

Использование безопасного HTTP (HTTPS) показывает, что SSL/TLS используется для шифрования трафика HTTP.

IPSec

IPSec — протокол для шифрования и/или аутентификации IP-пакетов. IPSec имеет два режима: туннельный и транспортный. С точки зрения продуктов Citrix интерес представляет транспортный режим, который обеспечивает сквозную безопасность для всего IP-трафика, пересылаемого между двумя узлами. Так же как и SSL/TLS, IPsec требует наличия на каждом узле ключа шифрования, который используется для установления и шифрования туннеля. IPSec рекомендуется использовать, когда недоступны все остальные протоколы безопасной коммуникации.

Рекомендации по использованию Citrix XenApp в среде Microsoft Active Directory

Ниже мы приведем некоторые рекомендации по использованию Citrix XenApp в среде Microsoft Active Directory.

Компания Citrix рекомендует следующие конфигурации фермы серверов, использующей Active Directory:

- все серверы должны находиться в одном домене;
- у домена фермы серверов нет доверительных отношений с доменами, не использующими Active Directory;
- ферма серверов находится в одном лесу Active Directory.

Заметим, что это рекомендации, а не требования. Тем не менее, наличие нескольких доменов или доверительных отношений с доменами, не использующими Active Directory, может повлиять на все аспекты, касающиеся аутентификации пользователя, что включает:

- проверку подлинности для администратора Citrix;
- доступ пользователей к опубликованным приложениям, опубликованное приложение (приложение, установленное на сервере Citrix XenApp и предоставленное пользователю для удаленной работы);
- назначение пользователей сетевым принтерам.

Использование лесов Active Directory

При использовании Windows Active Directory компания Citrix рекомендует, чтобы все серверы в ферме серверов относились к одному пространству Active Directory. Если в ферме имеются серверы, относящиеся более чем к одному лесу, пользователи не смогут зарегистрироваться, введя полное имя пользователя (UPN).

При регистрации в системе с помощью UPN используется формат «имя пользователя»@идентификатор UPN (Например: ivanov_aa@company.ru). В системе с Active Directory регистрация с помощью главного имени пользователя (UPN) не требует указания домена, поскольку Active Directory может полностью определить расположение регистрации с UPN в каталоге. Тем не менее, если в ферме имеется несколько лесов, может возникнуть проблема, поскольку один и тот же идентификатор UPN может существовать в двух доменах в разных лесах.

Реализация модели безопасности Active Directory

В Active Directory имеются следующие типы групп безопасности, к которым могут принадлежать пользователи:

- *Локальные доменные группы*. В модели Active Directory локальные доменные группы могут включать группы из других доменов, однако доменной локальной группе могут быть присвоены ресурсы только из того домена, в котором она присутствует.
- *Универсальные группы*. Они могут содержать группы из других доменов и сохраняются в глобальном каталоге Active Directory. Универсальные группы могут использоваться для присвоения полномочий на использование ресурсов в любом домене.
- *Глобальные доменные группы*. Глобальные группы включают группы в одном домене и им могут присваиваться ресурсы в любом домене. Компания Citrix рекомендует использовать доменные глобальные группы для обеспечения доступа пользователей к опубликованным приложениям и сетевым принтерам. Глобальные доменные группы эквивалентны глобальным группам, не относящимся к доменам Active Directory. Эти группы безопасности можно использовать при назначении пользователей для опубликованных приложений и сетевых принтеров.

Для получения дополнительных сведений о доменах, установлении доверительных отношений между доменами для настройки учетных записей пользователя в доменах или Active Directory, см. документацию по Windows.

Сценарии разрешений для пользователей при использовании Active Directory

При использовании Active Directory на решения по конфигурированию фермы серверов и управлению разрешениями пользователей могут повлиять следующие условия:

- Если для определения разрешений пользователям на запуск опубликованного приложения используются универсальные группы, то все серверы, на которых за-

пущено приложение (если для распределения нагрузки используется Load Manager (Диспетчер нагрузки)), должны находиться в домене Active Directory.

- Если для определения разрешений пользователям на запуск опубликованного приложения используются локальные группы, то все серверы, между которыми распределена нагрузка по данному приложению, должны находиться в одном домене. Кроме того, локальные доменные группы, которым разрешается использовать приложение, должны принадлежать первичному домену, общему для всех серверов, между которыми распределяется эта нагрузка. Если пользователь является членом локальной доменной группы, то группа принадлежит маркеру безопасности пользователя только тогда, когда пользователь входит в систему в том же домене, что и локальная доменная группа. Доверительная маршрутизация не гарантирует того, что запрос пользователя на вход в систему отправляется на сервер в том же домене, в котором находится локальная доменная группа.

Связывание клиентов и серверов

В ферме серверов основные процессы соединения клиентов и серверов — это перечисление приложения, рабочего стола и сеанса ICA (рис. 3.3).

Рис. 3.3. Схема перечисления приложений

На рис. 3.3 показан клиент, осуществляющий перечисление приложений с сервера. Для запуска приложения клиент инициирует сеанс ICA с сервером.

Перечисление

Перечисление — это процесс, при котором клиент передает данные, чтобы обнаружить серверы в сети и получает информацию по опубликованным приложениям фермы серверов.

В процессе перечисления клиенты общаются с Citrix XML Service или обозревателем ICA в зависимости от протокола просмотра, выбранного на клиенте.

Перечисление производится в случае, когда:

- Web Interface или клиентское ПО Program Neighborhood посылает запрос с целью обнаружения приложения на сервере. При использовании Load Manager (диспетчер нагрузки) компонента Citrix XenApp для Windows, Advanced Edition и Enterprise Edition, клиент получает адрес сервера с минимальной загруженностью.
- Пользователи Program Neighborhood выводят список Набора приложений в Мастере «Найти новый набор приложений».
- Пользователи Program Neighborhood выводят список серверов или опубликованных приложений в Мастере «Добавить новое ICA-подключение» для создания пользовательского ICA-подключения.

Сеансы ICA

Сеанс ICA — это канал связи клиента и сервера, создаваемый пользователем для запуска приложения. В рамках сеанса ICA сервер передает экран с окном приложения на клиентское устройство доступа, а устройство посылает приложению, запущенному на сервере, коды нажимаемых пользователем клавиш, операций мыши и локальные данные.

Порт по умолчанию для входящего трафика сеансов ICA на серверах — 1494.

Если включается функция надежного сеанса, то трафик ICA туннелируется с помощью общего шлюзового протокола, использующего по умолчанию TCP порт 2598. Как и в случае ICA-трафика, для входящих данных во время сеансов с XenApp используется выбранный порт, а динамически назначаемый порт используется для исходящего трафика. Порты 1494 и 2598 должны быть открыты только для внутреннего входящего трафика.

Исходящий порт на серверах, используемых для сеансов ICA, назначается динамически в момент создания сеанса.

Кроме компьютеров, на которых запущен Citrix XenApp, в создании сеанса ICA могут участвовать и другие компоненты, например, компьютеры, на которых запущен Web Interface, прокси-серверы и веб-обозреватели. В любом случае основной канал связи для сеанса ICA располагается между клиентом и сервером.

Конфигурирование перечисления

Пользователь подключается к серверам и приложениям из набора приложений или пользовательских ICA-подключений на клиенте. Перечисление — это процесс, позволяющий найти серверы и опубликованные приложения в ответ на запросы клиента.

- Когда пользователь запускает приложение из набора приложений, Citrix XenApp обнаруживает сервер, на котором находится данное приложение и, таким образом, клиент может подключиться к серверу и запустить приложение.
- Когда пользователь создает пользовательское подключение, то функция «перечисление» позволяет получить список опубликованных приложений или серверов в ферме. Пользователь выбирает приложение или сервер, для которого будет создаваться пользовательское подключение.

Безопасность сеансов, создаваемых клиентами, подключающимися через Интернет, должна обеспечиваться при помощи Secure Gateway или Access Gateway.

3.2.1. Настройка доступа пользователей к опубликованным ресурсам

Перед публикацией ресурсов необходимо проверить, как настройки учетных записей пользователей могут повлиять на их доступ к ресурсам. Ресурсы публикуются для определенных пользователей и групп пользователей. Мастер публикации приложений позволяет настроить два типа доступа к приложениям: анонимный доступ и доступ для явных (настроенных) учетных записей.

Анонимные пользователи

Во время установки Citrix XenApp программа создает специальную группу *анонимных* пользователей. По умолчанию анонимным пользователям предоставляются гостевые разрешения. Публикация приложений для группы анонимных пользователей позволяет полностью исключить необходимость проверки подлинности при доступе к этим приложениям. Когда пользователь запускает приложение, настроенное для анонимных поль-

зователей, сервер не требует указания явного имени пользователя и пароля для входа на сервер и запуска приложения. Анонимным пользователям предоставляются минимальные права на сеансы, включающие следующие ограничения:

- десятиминутный интервал ожидания при отсутствии действий пользователя;
- выход из системы при разрыве соединения или истечении интервала ожидания;
- пользователь не может изменить пароль (пароль не требуется).

По окончании сеанса анонимного пользователя пользовательские сведения не сохраняются. Сервер не сохраняет настройки рабочего стола, принадлежащие пользователю файлы и другие ресурсы, созданные или настроенные для клиента.

Примечание. Учетные записи анонимных пользователей, которые Citrix XenApp создает во время установки, не требуют дополнительной настройки. Если нужно изменить их свойства, можно сделать это с помощью стандартных средств управления учетными записями пользователей Windows.

Явные пользователи (Explicit Users)

Явный пользователь — это любой пользователь, не входящий в группу анонимных пользователей. У явных пользователей есть учетные записи, создаваемые, настраиваемые и обслуживаемые с помощью стандартных средств управления учетными записями.

Существуют ограничения для явных пользователей, входящих в систему фермы серверов для запуска приложений: администраторы могут указать тип профиля, параметры и другие настройки для этих пользователей.

Управление пользовательским доступом

Пользователи получают доступ к опубликованным ресурсам с помощью ICA-подключений и сеансов. *Подключения* — это порты сетевого протокола, настроенные на ожидание подключения на компьютере под управлением Citrix XenApp. Когда клиент соединяется с сервером через подключение, он устанавливает сеанс. Сеанс — это активный канал, который работает на сервере, пока пользователь не выйдет из системы.

В этой главе описывается управление доступом пользователей к ресурсам фермы серверов путем настройки входов в систему, конфигурации подключений, а также мониторинга, оптимизации и управления сеансами.

Настройка входов пользователей в систему

По умолчанию, когда вход в систему разрешен, Citrix XenApp не ограничивает пользовательский доступ к опубликованным приложениям. Следовательно, пользователи могут запускать несколько подключений и подключаться к любым опубликованным приложениям, на использование которых они имеют право. Вы можете контролировать способность пользователей подключаться к серверу, разрешая и запрещая вход в систему.

По умолчанию после установки Citrix XenApp входы активны.

Управление видом пользовательского входа

Во время подключения к серверу пользователи видят все сведения о подключении и состоянии входа в последовательности экранов, начиная с момента, когда они дважды щелкают по значкам приложений на клиентском устройстве до проверки подлинности и запуска опубликованного приложения в сеансе.

Citrix XenApp контролирует вид входа, пропуская окна состояния, созданные операционной системой Windows сервера, во время подключения пользователя. Для этого программа установки Citrix XenApp использует следующие локальные групповые политики Windows для сервера, на который вы устанавливаете продукт:

- Административные шаблоны → Система → Удалить сообщения о состоянии загрузки/завершения работы/входа/выхода;
- Административные шаблоны → Система → Подробные или обычные сообщения о состоянии.

Однако групповые политики, настроенные в Active Directory, имеют приоритет над эквивалентными локальными групповыми политиками, настроенными для отдельных серверов. Поэтому если вы установите Citrix XenApp на серверы, входящие в домен Active Directory, и настроите групповые политики Active Directory, эти политики могут помешать Citrix XenApp скрыть экраны состояния, сгенерированные операционной системой Windows на отдельных серверах. В этом случае пользователи увидят экраны состояния, созданные ОС Windows во время подключения к этому серверу. Для обеспечения оптимальной производительности не настраивайте такие групповые политики в Active Directory.

Предоставление пользователям функции Workspace Control

Функция Workspace Control позволяет пользователям быстро отключаться от всех работающих приложений и переподключаться к ним, или выходить из всех работающих приложений. Workspace Control позволяет пользователям перемещаться между клиентскими устройствами и получать доступ ко всем своим открытым приложениям после входа. Например, Workspace Control может помочь работникам, нуждающимся в быстром переходе между рабочими станциями и доступе к одному набору приложений при каждом входе в Citrix XenApp. Если вы разрешите этот режим в Workspace Control, работники смогут отключаться от нескольких приложений на одном клиентском устройстве, а затем подключаться к ним, чтобы открыть приложения на другом клиентском устройстве.

Для пользователей, подключающихся через Web Interface или Program Neighborhood Agent можно настраивать (или разрешить пользователям настраивать) следующие операции:

- **Вход.** По умолчанию Workspace Control позволяет пользователям переподключаться ко всем работающим приложениям во время входа без необходимости в повторном открытии отдельных приложений. С помощью Workspace Control пользователи могут открывать автономные приложения и приложения, активные на другом клиентском устройстве. После отключения от приложения оно продолжит работу на сервере. Если в организации есть пользователи, которые часто меняют рабочее место и которым необходимо, чтобы некоторые приложения работали на одном клиентском устройстве, когда они переподключаются к поднабору приложений на другом устройстве, можно настроить режим переподключения на открытие только тех приложений, от которых пользователь отключился ранее.
- **Переподключение.** После входа на ферму серверов пользователи могут переподключиться ко всем приложениям в любое время, нажав кнопку «Переподключить». По умолчанию переподключение открывает отключенные приложения и все активные приложения, работающие на другом клиентском устройстве. Переподключение можно настроить на открытие только тех приложений, от которых пользователь отключился ранее.
- **Выход из системы.** Для пользователей, которые открывают приложения через Web Interface, можно настроить команду «Выход» на выход только из Web Interface и всех активных сеансов или на выход только из Web Interface.

- **Отключение.** Пользователи могут отключиться от всех работающих приложений без необходимости в отключении всех приложений в отдельности. По умолчанию функция Workspace Control включена в ферме серверов и доступна только для пользователей, которые получают доступ к приложениям через Web Interface или Program Neighborhood Agent.

Когда пользователь переходит на новое клиентское устройство, пользовательские политики, назначение клиентских дисков и конфигурация принтеров изменяются соответственно. Политики и назначения применяются в соответствии с клиентским устройством, с которого подключается пользовательский сеанс. Например, медицинский работник завершает сеанс на клиентском устройстве в пункте первой помощи больницы, а затем выполняет вход на рабочую станцию в рентгеновской лаборатории больницы, при этом политики, назначения принтеров и назначения клиентских устройств для сеанса рентгеновской лаборатории применяются, как только пользователь выполняет вход на клиентское устройство лаборатории.

Дополнительные сведения о включении и настройке Workspace Control для пользователей см. в документе Citrix Web Interface Administrator's Guide.

Настройка пользовательских подключений

Citrix XenApp позволяет запускать приложения, опубликованные на сервере, обеспечивая подключение различных платформ через клиентское ПО Citrix XenApp.

Если подключение обрывается, сеанс, который его использует, останется активным, пока его состояние не будет изменено функцией автоматического переподключения, параметрами ICA Keep-Alive или администратором Citrix.

Несколько клиентов могут создавать сеансы, используя одно подключение к серверу. Citrix XenApp связывает идентификатор пользователя и подключение с каждым сеансом.

Защита ферм серверов

Здесь мы дадим общие указания по планированию безопасных сред Citrix.

Защита доступа к серверам

Первый и важный этап обеспечения безопасности фермы серверов — защита доступа к серверам и их консолям управления.

Защита Консоли XenApp Console

Консоль XenApp может подключаться ко всем серверам фермы. Запускайте консоль только в средах, в которых перехват пакетов невозможен. Убедитесь, что доступ к консоли имеют только администраторы. Можно настроить права NTFS так, чтобы пользователи без прав администратора не могли выполнять операцию Execute для исполняемого файла консоли (Ctxload.exe).

Использование разделов NTFS. Чтобы обеспечить необходимый уровень контроля доступа для всех файлов, установленных Citrix XenApp Server, устанавливайте XenApp Server только на разделы, отформатированные в NTFS.

Установка и настройка службы SNMP. По умолчанию служба SNMP не устанавливается на компьютеры под управлением Windows Server 2003. При установке службы необходимо задать параметр community string. Может потребоваться создание «белого списка» для ограничения доступа к службе SNMP с удаленных IP-адресов. Служба Windows SNMP

по умолчанию поддерживает несколько привилегий на чтение и запись, однако необходимо также дать службе SNMP права на чтение и создание для задач администрирования, таких как выход или отключение через Network Manager. При использовании Network Manager или другого управляющего ПО на основе SNMP только для мониторинга сервера (без удаленного управления), Citrix рекомендует настроить права только на чтение. Если консоль SNMP не используется, не устанавливайте компоненты SNMP на сервер. Для предотвращения несанкционированного доступа можно задать общие и выделенные консоли управления SNMP. Настройте агенты SNMP на прием ловушек только от известных консолей SNMP.

Настройка доверенного сервера. Эта функция определяет и обеспечивает отношения доверия в клиентских подключениях. Отношения доверия помогают повысить уверенность администраторов и пользователей клиентских машин в целостности данных на клиентских устройствах, а также предотвратить злонамеренное использование клиентских подключений. Когда эта функция включена, клиенты могут задавать требования к доверию и определять, доверяют ли они тому или иному серверному подключению. Дополнительные сведения об этой функции *см. в документе Clients for Windows Administrator's Guide.*

Защита хранилища данных

Один из самых важных аспектов обеспечения безопасности фермы серверов — защита хранилища данных. Она подразумевает не только защиту данных в БД хранилища, но и ограничение доступа к этим данным. Как правило:

- пользователи, которые имеют доступ к серверам фермы, не нуждаются в доступе к хранилищу данных и предоставлять его не следует;
- если подключение к хранилищу данных является прямым (т. е. без промежуточных серверов), все серверы фермы используют одно имя пользователя и пароль для доступа к хранилищу данных. Выберите пароль, который трудно подобрать. Храните имя пользователя и пароль в безопасном месте и давайте его администраторам только для установки Citrix XenApp.

Предупреждение. Входящий Интернет-трафик SNMP можно заблокировать, закрыв порты 161 и 162 для протокола UDP в межсетевом экране.

Более конкретные рекомендации Citrix по обеспечению безопасности хранилища данных зависят от БД, используемой для хранилища данных. В следующих разделах рассматриваются рекомендуемые меры безопасности для каждой базы данных, поддерживаемой Citrix XenApp.

Для повышенной безопасности можно изменить права учетной записи на db-reader и db_writer после первоначальной установки базы данных с правами db_owener. Изменение прав учетной записи с db_owener может вызвать проблемы установки новых пакетов обновления или версий Citrix XenApp.

Microsoft Access. Для хранилища данных Access именем пользователя по умолчанию будет «citrix», пароль — «citrix». Если пользователи имеют сетевой доступ к хранилищу данных, измените пароль с помощью команды dsmaint config и храните его в безопасном месте.

Microsoft SQL Server. Учетная запись, используемая для доступа к хранилищу данных Microsoft SQL Server, имеет роли public и db_owner на сервере и в базе данных. Учетная запись системного администратора для доступа к хранилищу данных не требуется. Не используйте эту учетную запись, так как это может стать причиной дополнительных рисков для безопасности.

Если Microsoft SQL Server использует смешанный режим безопасности (т. е. можно использовать проверку подлинности как Microsoft SQL Server, так и Windows), возможно

потребуется создание учетной записи Microsoft SQL Server только для доступа к хранилищу данных. Так как эта учетная запись будет иметь доступ только к хранилищу данных, риски безопасности для домена Windows в случае раскрытия пароля будут устранены.

Предупреждение. Если учетная запись для прямого доступа изменится, служба Citrix IMA Service не запустится на всех серверах, использующих эту учетную запись. Для того, чтобы изменить пароль Citrix IMA Service необходимо ввести команду dsmaint config на всех серверах, где это необходимо.

Предупреждение. Для сред с высоким уровнем безопасности Citrix рекомендует использовать только проверку подлинности Windows.

Microsoft SQL Server 2005 Express Edition. Проверка подлинности Windows поддерживается для баз данных Microsoft SQL Server 2005 Express Edition. По соображениям безопасности проверка подлинности Microsoft SQL Server не поддерживается. Дополнительные сведения см. в документации Microsoft. Как правило, используется имя пользователя и пароль учетной записи локального администратора. Если пользователи имеют доступ к серверу хранилища данных, измените пароль с помощью команды dsmaint config и храните его в безопасном месте.

Oracle. Если хранилище данных размещено в БД Oracle, дайте учетной записи, используемой для подключения к ферме серверов только права «connect» и «resource». Права учетной записи уровня системного администратора (system или sys) для доступа к хранилищу данных не требуются.

IBM DB2. Если хранилище данных размещено в БД IBM DB2, дайте учетной записи, используемой для подключения к ферме серверов следующие права:

- Connect database (подключение базы данных);
- Create tables (создание таблиц);
- Register functions to execute to database manager's process (регистрация функций для выполнения процесса диспетчера базы данных);
- Create schemas implicitly (неявное создание схем).

Права учетной записи уровня системного администратора (DB2Admin) для доступа к хранилищу данных не требуются.

Защита сетевой передачи данных

Сетевая передача данных между клиентом и сервером представляет риски безопасности в любой корпоративной среде. В следующих разделах рассматриваются компоненты безопасности, которые можно использовать для защиты сетевой передачи данных в ферме серверов. В зависимости от требований к безопасности в проект развертывания Citrix XenApp можно включить следующие компоненты для защиты сетевой передачи данных:

- шифрование средствами протокола ICA;
- Citrix SSL Relay;
- служба Secure Gateway;
- Secure Ticket Authority (служба STA)
- Межсетевые экраны

Использование средств шифрования протокола ICA

Протокол ICA предлагает встроенное шифрование на стороне клиента и сервера, добавляя дополнительный уровень защиты от раскрытия данных сеанса. Используйте шифрование ICA (Citrix SecureICA) для шифрования данных, передаваемых между сервером под управлением Citrix XenApp Server и клиентом. Шифрование ICA помогает предотвратить перехват данных. В отличие от шифрования SSL/TLS, шифрование ICA, если ис-

пользуется отдельно, не обеспечивает проверку подлинности сервера. Поэтому, теоретически, данные можно перехватить во время передачи по сетям общего пользования и перенаправить на поддельный сервер. Кроме того, шифрование ICA не включает проверку целостности данных. Шифрование ICA — только один из аспектов комплексной стратегии безопасности.

Уровень шифрования ICA для опубликованного приложения можно задать на странице Properties (свойства) приложения или с помощью политик Citrix. Кроме того, необходимо включить шифрование ICA на стороне клиента. См. документацию по клиенту, который планируется развернуть.

В целом шифрование ICA нужно использовать если:

- необходима безопасная внутренняя связь в рамках LAN или WAN; или есть потребность в безопасном внутреннем доступе в Интранет;
- необходима безопасная связь с устройствами под управлением ОС Microsoft DOS или Win16;
- клиентское ПО работает на старых устройствах, которые невозможно модернизировать;
- риск «атаки изнутри» невысок.

Использование Secure Gateway

Для обеспечения шифрования SSL/TLS между безопасным шлюзовым сервером Интернета и клиентом с поддержкой SSL в сочетании с шифрованием данных HTTP, передаваемых между веб-обозревателем и веб-сервером, используется **Secure Gateway**. Secure Gateway упрощает передачу данных через межсетевые экраны и улучшает безопасность, обеспечивая единую точку входа и безопасный доступ к фермам серверов.

Secure Gateway следует использовать, если требуется:

- скрыть внутренние IP-адреса;
- обезопасить общий доступ к серверам фермы;
- двухфакторная аутентификация (в сочетании с Web Interface);

Использование Secure Gateway позволяет добиться следующих преимуществ:

- безопасный доступ к Интернету;
- устранение необходимости в публикации адресов каждого сервера Citrix XenApp;
- упрощение управления серверными сертификатами;
- единая точка шифрования и доступа к серверам.

Для создания шлюза, изолированного от компьютеров под управлением Citrix XenApp, используется Secure Gateway. Организация шлюза упрощает передачу данных через межсетевой экран, так как входящий и исходящий трафики ICA проходят через широко используемый порт. Secure Gateway обеспечивает повышенную масштабируемость. Однако, поскольку данные ICA шифруются только между клиентом и шлюзом, может потребоваться защита трафика между шлюзом и серверами Citrix XenApp, включая серверы, на которых работает служба Citrix XML Service. Дополнительные сведения о настройке Secure Gateway см. в документе Secure Gateway Administrator's Guide.

Использование службы Secure Ticket Authority

Служба Secure Ticket Authority (STA) выполняет выдачу билетов сеансов по запросам на подключение к ресурсам, опубликованным на сервере Citrix XenApp. На билетах сеанса основываются процедуры проверки подлинности и авторизации для доступа к опубликованным ресурсам. Служба STA устанавливается одновременно с установкой XenApp.

Если Citrix XenApp устанавливается на сервер со старой версией службы STA, она обновляется до текущей версии. Служба STA встроена в службу Citrix XML Service.

Настройка межсетевых экранов

В дополнение к обеспечению физической безопасности серверов, большинство организаций устанавливают средства сетевой защиты, такие как межсетевые экраны, для изоляции Citrix XenApp и веб-обозревателей от Интернета и сетей общего доступа. Для развертывания Citrix XenApp во внутренних сетях обеспечьте безопасность данных, передаваемых между клиентом и сервером, с помощью протоколов SSL/TLS и других мер безопасности.

Дополнительные сведения о настройке межсетевых экранов в серверной ферме *см. в документе Advanced Concepts Guide for Citrix Presentation Server (Руководство по использованию дополнительных решений для Citrix Presentation Server).*

Настройка TCP-портов

В таблице ниже перечислены порты TCP/IP, которые используются серверами, клиентами Citrix XenApp, службой IMA Service и другими службами фермы. Эти сведения могут помочь в настройке межсетевых экранов и устранении конфликтов портов с другим программным обеспечением.

Таблица 3.1

Таблица используемых TCP портов

Передача данных	*Порт по умолчанию*
Citrix XML Service	80
Access Management	135
Citrix SSL Relay	443
Сеансы ICA (от клиентов к серверам)	1494
Клиент—сервер (направленный UDP)	1604
Сервер—сервер	2512
Консоль XenApp—сервер	2513
Надежность сеанса «Session Reliability»	2598
Сервер—сервер Microsoft SQL или Oracle	139, 1433 или 443 для MS-SQL
Консоль License Management	8082
Сервер—сервер лицензий	27000

3.2.2. Настройка проверки подлинности пользователя

Обеспечение безопасности серверов подразумевает гарантии того, что доступ к серверам и ресурсам могут получить только пользователи, подлинность которых проверена.

Настройка аутентификация для Workspace Control

Если пользователи выполняют вход, используя смарт-карты или сквозную аутентификацию, необходимо установить отношения доверия между сервером Web Interface и всеми серверами фермы, к которым Web Interface обращается для доступа к опубликованным приложениям. Без отношений доверия команды Disconnect, Reconnect и Log Off

(«Workspace Control») пользователей, выполнивших вход с помощью смарт-карты или сквозной аутентификации, работать не будут.

Если при входе пользователи вводят учетные данные в Web Interface или Program Neighborhood Agent, отношения доверия не требуются.

Если вы настраиваете сервер доверять запросам, отправленным в адрес службы Citrix XML Service, необходимо рассмотреть следующие факторы:

- отношения доверия нужны, только если вы планируете внедрить Workspace Control и пользователи выполняют вход, используя смарт-карты или сквозную аутентификацию;
- включайте отношения доверия только на серверах, к которым Web Interface подключается напрямую. Эти серверы перечислены в консоли Web Interface;
- устанавливая отношения доверия, вы передаете аутентификацию пользователей серверу Web Interface. Чтобы избежать рисков для безопасности, используйте SSL Relay, IPSec, межсетевые экраны или любые другие технологии, позволяющие гарантировать, что со службой Citrix XML Service смогут взаимодействовать только доверенные серверы. Установка отношений доверия без IPSec, межсетевых экранов и других технологий защиты позволит любому сетевому устройству отключать и завершать клиентские сеансы;
- настройте SSL Relay, IPSec, межсетевые экраны и другие технологии для защиты среды и ограничения доступа к службе Citrix XML Service таким образом, что ее смогут использовать только серверы Web Interface. Например, если служба Citrix XML Service делит порт с IIS, можно использовать функцию ограничения IP-адреса в IIS для ограничения доступа к службе Citrix XML Service.

Настройка входа Kerberos

Клиенты Citrix XenApp для Windows предлагают расширенную безопасность для сквозной аутентификации. В этом случае применяется аутентификация Kerberos, а не отправка паролей через сеть. Kerberos — стандартный протокол аутентификации, встроенный в операционные системы Windows. Вход Kerberos предлагает заказчикам с высокими требованиями к безопасности удобство сквозной аутентификации в сочетании с симметричной криптографией и целостностью данных, обеспечиваемой стандартными решениями по сетевой безопасности.

Системные требования. Вход Kerberos требует Presentation Server 3.0 или выше и клиентское ПО Citrix Presentation Server для Windows версии 8.x или выше. Kerberos работает только между клиентами и серверами, которые принадлежат одному домену или доверенным доменам Windows. Кроме того, серверы должны быть доверенными для делегирования. Эту возможность можно включить в средстве управления «Пользователи и компьютеры» Active Directory.

Вход Kerberos недоступен, если в конфигурации терминальных служб заданы следующие функции:

- использовать обычную аутентификацию Windows;
- всегда использовать следующие сведения или всегда запрашивать пароль:
  - — если подключения проходят через Secure Gateway;
  - — если сервер Citrix XenApp требует входа по смарт-карте.

Kerberos требует, чтобы для фермы серверов было включено разрешение DNS-адресов средствами службы Citrix XML Service, или для Active Directory было включено обратное разрешение DNS.

Использование смарт-карты с Citrix XenApp

В среде Citrix XenApp можно использовать смарт-карты:

- аутентификации пользователей в сетях и компьютерах;
- защищенной передачи данных по сети;
- цифровой подписи содержимого.

Если вы используете смарт-карты для аутентификации в сети, пользователям также будет доступна аутентификация для доступа к приложениям и содержимому, опубликованному на серверах. При этом функциональность смарт-карты сохраняется и внутри этих приложений. Например, опубликованное приложение Microsoft Outlook может требовать вставки смарт-карты в устройство для чтения клиентского устройства для входа на сервер. После аутентификации пользователей для доступа к приложению они смогут добавлять цифровую подпись к сообщениям электронной почты с помощью сертификатов смарт-карты.

Компания Citrix тестировала смарт-карты, соответствующие стандарту ISO 7816 для карт с электрическими контактами (также известных как контактные карты), которые взаимодействуют с компьютерными системами через устройства для чтения смарт-карт. Устройство чтения подключается к компьютеру через последовательный порт, USB или PCMCIA.

Citrix поддерживает криптографические смарт-карты PC/SC, используемые для криптографических операций, таких как цифровые подписи и шифрование. Криптографические карты обеспечивают безопасное хранение закрытых ключей, которые, в частности, могут использоваться в системах на основе инфраструктуры PKI (Public Key Infrastructure). В таких картах криптографические функции выполняются в самой смарт-карте. Это означает, что закрытые ключи и цифровые сертификаты никогда не покидают карту.

Кроме того, Citrix поддерживает двухфакторную аутентификацию для повышенной безопасности. Помимо простого предъявления смарт-карты (один фактор) для выполнения операции требуется PIN-код (второй фактор), известный только пользователю. Это позволяет гарантировать, что лицо, использующее смарт-карту, является ее законным владельцем.

Смарт-карты можно также использовать в Web Interface для Citrix XenApp. Дополнительные сведения о настройке Web Interface для поддержки *см. в документе Web Interface Administrator's Guide (Руководство администратора Web Interface).*

Требования к смарт-картам

Ниже приводятся основные инструкции по использованию смарт-карт с Citrix XenApp.

Для сервера необходимы следующие компоненты:

- программное обеспечение PC/SC;
- программное обеспечение Cryptographic Service Provider (CSP).

Предупреждение. Citrix Presentation Server не поддерживает функциональные спецификации стандарта PKCS компании RSA Security Inc по персональным криптографически маркерам.

Компоненты, которые необходимо установить на устройстве с поддерживаемым клиентским ПО Citrix XenApp:

- программное обеспечение PC/SC;
- драйверы устройства для чтения смарт-карт;
- устройство для чтения смарт-карт.

Операционные системы клиента и сервера могут включать PC/SC, CSP и драйверы устройства для чтения смарт-карт. Сведения о том, поддерживаются ли эти компоненты или их необходимо заменить специализированным программным обеспечением, можно получить у поставщика смарт-карт.

Если вы используете сквозную аутентификации для передачи учетных записей от клиентского устройства Windows 2000 или Windows XP серверному сеансу смарт-карты, необходимо установить ПО CSP на клиентское устройство.

Смарт-карты можно использовать в качестве средства аутентификации для доступа к опубликованному приложению, а также для использования внутри приложений, поддерживающих функциональность смарт-карт. При установке Citrix XenApp по умолчанию поддерживается только первое.

Настройка политик Windows для смарт-карт

Microsoft Windows поддерживает два параметра политик безопасности для интерактивного входа в серверный сеанс. Клиентские сеансы Citrix XenApp могут использовать следующие политики:

- для входа в интерактивный сеанс необходима смарт-карта. Это — пользовательская политика, которая требует вставки смарт-карты для аутентификации;
- политика удаления смарт-карты. Это — компьютерная политика, которая включает три параметра, определяющие режим работы клиентского устройства при извлечении смарт-карты из устройства чтения:
  - нет (без эффекта);
  - блокировка рабочей станции (отключение всех пользовательских сеансов);
  - принудительный выход (выход из всех пользовательских сеансов).

Настройка клиента

Смарт-карты поддерживаются следующими клиентами:

- клиент Citrix Presentation Server для Windows;
- клиент для Linux;
- клиент для терминалов Windows.

Список использованной литературы

1. Рэнд Моримото, Майкл Ноэл, Омар Драуби, Росс Мистри, Крис Амарис, «Microsoft Windows Server 2008. Полное руководство». М.: Вильямс, 2008.
2. Джонатан Хассел «Администрирование Windows Server 2003». — «Русская редакция», «Питер», 2006.
3. Курт Хадсон «Официальный учебный курс Microsoft. Планирование, внедрение и поддержка инфраструктуры Microsoft Windows Server 2003 Active Directory 70-294. Практические занятия». — М.: «ЭКОМ Паблишерз», 2007.
4. Windows Server 2008. Официальный сайт. http://www.microsoft.com/Rus/windows-server/default.mspx
5. Пошаговые руководства для установки, настройки и использования систем Windows Server 2008. http://www.microsoft.com/rus/windows-server/tutorials/default.mspx
6. Windows Server TechCenter, http://technet.microsoft.com/ru-ru/windowsserver/default.aspx
7. Воронин А. Безопасный доступ к Oracle E-Business Suite OC Week, № 13/2006, http://www. aladdin.ru/catalog/etoken_products/suite/public_detail.php?ID=7648
8. Демченко К., Додохов А., Сабанов А. Русская версия «индийской защиты», или Защита данных в СУБД Oracle. журнал Byte, № 8, 2004, http://www.bytemag.ru/?ID=602973
9. Додохов А., Сабанов А. О дополнительных возможностях защиты данных в среде Oracle9i, BYTE, № 5/2005, http://www.aladdin.ru/catalog/etoken_products/oracle/public_detail.php?ID=7264
10. Краткий обзор Oracle E-Business Suite, http://www.oracle.com/global/ru/pdfs/brochure_ebs.pdf

11. Сабанов А. Безопасность баз данных. Что, от кого и как надо защищать. Connect, № 4/2006, http://www.aladdin.ru/catalog/etoken_products/oracle/public_detail.php?ID=7640
12. Сабанов А. О роли аутентификации при обеспечении защищенного удаленного доступа. Connect № 5, 2007. Технические подробности eToken SecurLogon для Oracle Application Server www.aladdin.ru/catalog/etoken_products/oas/tech_details.php
13. Технические подробности eToken SecurLogon для Oracle E-Business Suite, www.aladdin.ru/catalog/etoken_products/suite/tech_details.php
14. eToken SecurLogon для Oracle Application Server www.aladdin.ru/catalog/etoken_products/oas/
15. eToken SecurLogon для Oracle E-Business Suite, www.aladdin.ru/catalog/etoken_products/suite/
16. Oracle Advanced Security Administrator's Guide Release 2 (9.2)
17. Oracle Database 10g — Каталог программных продуктов http://www.oracle.com/global/ru/pdfs/index.html
18. Oracle Database 10g Release 2 (10.2) Documentation http://www.oracle.com/technology/documentation/database10gr2.html
19. Oracle E-Business Suite. Каталог. http://download.oracle.com/otndocs/ebs/oracle-ebs-catalogue-full.pdf
20. Oracle Fusion Middleware. Каталог продуктов. http://www.oracle.com/global/ru/pdfs/index.html
21. Citrix Product Development Team. Access Security for IT Administrators, McGraw Hill Osborne, 2007.
22. Fabian Kienle. Citrix MetaFrame Secure Access Manager, MITP, 2004.
23. MetaFrame Presentation Server Security Standards and Deployment Scenarios, Citrix Systems, 2004.
24. Citrix Advanced Concepts Guide, Vol. 3, Security, Citrix Systems, 2007.
25. Web Interface Administrator's Guide, Citrix Systems, 2006.
26. Secure Gateway for Windows Administrator's Guide, Citrix Systems, 2007.
27. eToken Integration Guide. eToken and Citrix MetaFrame Presentation Server version 4.0, Aladdin Knowledge Systems, 2006.
28. eToken OTP Authentication 2.0 for Citrix WI Administrator's Guide, Aladdin Knowledge Systems, 2007.

Источники

1. http://technet2.microsoft.com/windowsserver2008/en/servermanager/activedirectorycertificateservices.mspx» (Службы сертификации Active Directory AD CS)
2. http://technet2.microsoft.com/windowsserver2008/en/servermanager/activedirectorydomainservices.mspx (Службы доменов Active Directory AD DS)
3. http://technet2.microsoft.com/windowsserver2008/en/servermanager/activedirectoryfederationservices.mspx (Службы федерации Active Directory AD FS)
4. http://technet2.microsoft.com/windowsserver2008/en/servermanager/activedirectorylightweightdirectoryservices.mspx (Службы Active Directory облегченного доступа к каталогам AD LDS)
5. http://technet2.microsoft.com/windowsserver2008/en/servermanager/activedirectoryrightsmanagementservices.mspx (Службы управления правами Active Directory AD RMS)
6. http://technet2.microsoft.com/windowsserver2008/en/servermanager/applicationserver.mspx (Сервер приложений)
7. http://technet2.microsoft.com/windowsserver2008/en/servermanager/dhcpserver.mspx (DHCP-сервер)
8. http://technet2.microsoft.com/windowsserver2008/en/servermanager/dnsserver.mspx (DNS-сервер)
9. http://technet2.microsoft.com/windowsserver2008/en/servermanager/faxserver.mspx (Факс-сервер)
10. http://technet2.microsoft.com/windowsserver2008/en/servermanager/fileservicesmspx (Файловые службы)
11. http://go.microsoft.com/fwlink/?LinkId=101268 (Hyper-V)
12. http://technet2.microsoft.com/windowsserver2008/en/servermanager/networkpolicyandaccessservices.mspx (Службы сетевой политики и доступа)
13. http://technet2.microsoft.com/windowsserver2008/en/servermanager/printservices.mspx (Службы печати)
14. http://technet2.microsoft.com/windowsserver2008/en/servermanager/streamingmediaservices.mspx (Службы потокового мультимедиа)

15. http://technet2.microsoft.com/windowsserver2008/en/servermanager/terminalservices.mspx (Службы терминалов)
16. http://technet2.microsoft.com/windowsserver2008/en/servermanager/uddiservices.mspx (Службы UDDI)
17. http://technet2.microsoft.com/windowsserver2008/en/servermanager/webserver.mspx (Веб-сервер)
18. http://technet2.microsoft.com/windowsserver2008/en/servermanager/windowsdeploymentservices.mspx (Службы развертывания Windows)
19. http://download-uk.oracle.com/docs/cd/B28196_01/idmanage.1014/b15988/toc.htm (Oracle Identity Management 10.1.4/ Single Sign-On Administration Guide)
20. http://download-uk.oracle.com/docs/cd/B31017_01/web.1013/b28948/toc.htm (Oracle Application Server 10.1.3.1 / Oracle HTTP Server Administration Guide)
21. http://download-uk.oracle.com/docs/cd/B31017_01/web.1013/b28957/toc.htm (Oracle Application Server 10.1.3.1 / Oracle Containers for J2EE (OC4J) Security Guide)
22. http://download-uk.oracle.com/docs/cd/B40078_02/doc/bi.1013/b31765.pdf (Oracle BI Suite Enterprise Edition 10.1.3.2 / Infrastructure Installation and Configuration Guide)
23. http://download-uk.oracle.com/docs/cd/B40078_02/doc/bi.1013/b40017/toc.htm (Oracle BI Suite Enterprise Edition 10.1.3.2 / Publisher User Guide)
24. http://download-uk.oracle.com/docs/cd/B40078_02/doc/bi.1013/b31766.pdf (Oracle BI Suite Enterprise Edition 10.1.3.2 / Presentation Services Administrator Guide)
25. http://download-uk.oracle.com/docs/cd/B40078_02/doc/bi.1013/b40058.pdf (Oracle BI Suite Enterprise Edition 10.1.3.2 / Deployment Guide)
26. http://download-uk.oracle.com/docs/cd/B40078_02/doc/bi.1013/b32481/toc.htm (Oracle BI Suite Enterprise Edition 10.1.3.2 / Deploying Oracle Business Intelligence Publisher in J2EE Application Servers)
27. http://technet2.microsoft.com/windowsserver/en/library/32aacfe8-83af-4676-a45c-75483545a9781033.mspx?mfr=true Windows Server 2003 TechCenter, Security
28. http://technet2.microsoft.com/WindowsServer/en/library/a92d8eb9-f53d-4e86-ac9b-29fd6146977b1033.mspx?mfr=true Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure
29. http://technet2.microsoft.com/windowsserver/en/library/2cb5c8c9-cadc-44a9-bf39-856127f4c8271033.mspx?mfr=true How Terminal Services Works
30. http://www.aladdin.com/etoken/windows-logon.aspx eToken Network Logon and Smart Card Logon for Windows
31. http://www.aladdin.com/etoken/otp.aspx eToken One-Time Password (OTP)
32. http://www.aladdin.ru/catalog/etoken/tech_details/ eToken Aladdin Технические Подробности
33. http://www.citrix.com/English/SS/supportSecond.asp?slID=162512&ntref=hp_nav_US Citrix Security and Compliance Information
34. http://support.citrix.com/article/CTX113743 Web Interface Administrator's Guide
35. http://support.citrix.com/article/CTX111066 Configuring Web Interface 4.x to Use Smart Cards
36. http://support.citrix.com/article/CTX105749 Citrix Presentation Server Security Standards and Deployment Scenarios
37. http://support.citrix.com/article/CTX112223 Citrix Presentation Server 4.5 Administrator's Guide
38. http://support.citrix.com/article/CTX112429 Secure Gateway for Windows Administrator's Guide
39. http://support.citrix.com/article/CTX113599 Citrix SmartAuditor for Presentation Server 4.5
40. http://support.citrix.com/article/CTX113935 Citrix Password Manager Administrator's Guide
41. http://support.citrix.com/article/CTX112190 Clients for Windows Administrator's Guide-10.x EN
42. http://www.ietf.org/rfc.html Request for Comments Repository
43. http://www.ietf.org/rfc/rfc1509.txt?number=1509 Internet EFC 1509