УДК 004.7

Ф. Н. Юданов, **А. М. Федотов**, **Р. С. Сейткасым**

Новосибирский государственный университет
ул. Пирогова, 2, Новосибирск, 630090, Россия

Институт вычислительных технологий СО РАН
пр. Акад. Лаврентьева, 6, Новосибирск, 630090, Россия

E-mail: fedwiz@academ.org; fedotov@nsu.ru
seitrustem@mail.ru

ТЕХНОЛОГИИ ЕДИНОЙ АВТОРИЗАЦИИ И ОРГАНИЗАЦИИ ЕДИНОЙ ТОЧКИ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ СЕТИ

Дается анализ существующих технологий построения информационной инфраструктуры предприятия, реализующей концепцию единой точки доступа к информационным ресурсам. Рассматриваются вопросы реализации процедуры единой авторизации и аутентификации пользователей, а также анализируются технологические решения ведущих мировых компаний-разработчиков программного обеспечения, использующих перечисленные технологии в комплексе.

Ключевые слова: единая авторизация, управление информационными ресурсами, LDAP, Active Directory, IBM Tivoly, Oracle Identity Management.

Введение

При эксплуатации информационной инфраструктуры крупного современного предприятии на первое место выходит проблема интеграции распределенных источников данных и других сетевых информационных и вычислительных ресурсов. Одной из важнейших задач интеграции является проблема управления доступом к этим ресурсам.

Примерами таких ресурсов являются различные информационные системы, эксплуатируемые в организации, веб-сервисы, веб-сайты, базы данных, а также физические ресурсы: подключенные к сети компьютеры, принтеры, точки доступа Wi-Fi и т. д. [1].

Одной из центральных задач в данной области является задача внедрения процедуры единой авторизации на множестве ресурсов. Это множество чаще всего представляет собой совокупность информационных ресурсов конкретно взятой организации, хотя возможны случаи как совместного использования определенных ресурсов несколькими организациями, так и выделение подобного множества в глобальном интернет-пространстве.

Внедрение процедуры единой авторизации позволяет пользователю, будучи однажды авторизованным на одном из ресурсов, получить далее авторизованный доступ к любому другому ресурсу без необходимости вводить повторно имя пользователя и пароль.

В случае если выделен отдельный ресурс, на котором осуществляется авторизация пользователя, а все остальные ресурсы далее взаимодействуют с первым, автоматически проверяя с его помощью личность пользователя, имеет смысл говорить о таком ресурсе, как о единой точке доступа к информационным ресурсам сети.

Задачи, решаемые с помощью внедрения технологии единой авторизации

Сотрудник современной крупной организации в процессе своей деятельности вынужден работать с множеством информационных ресурсов, требующих авторизованного доступа.

Таким образом, в случае если данные ресурсы не связаны друг с другом, он вынужден регулярно проходить процедуру аутентификации на каждом из ресурсов отдельно. Для этого ему приходится либо помнить множество паролей, которые в этом случае, как правило, становятся предельно простыми, а значит уязвимыми к таким атакам, как подбор по словарю, либо вовсе использовать один и тот же пароль для всех ресурсов.

В последнем случае устойчивость к взлому каждого из ресурсов сводится к устойчивости слабейшего из них, т. е. если злоумышленнику удается перехватить пароль к некоторому ресурсу, переданный по нешифрованному соединению, он получает доступ к любому другому ресурсу независимо от того, насколько хорошо защищен последний.

Другая проблема, связанная с существованием множества несвязанных между собой учетных записей одного пользователя, заключается в возникновении значительной нагрузки на системных администраторов по поддержанию данных ресурсов. Так, добавление нового пользователя в системе ресурсов потребует от администратора отдельной работы на каждом из ресурсов. То же самое можно сказать о закрытии доступа уволенному сотруднику.

Таким образом, внедрение технологии единой авторизации на множестве ресурсов организации способствует решению следующих задач:

- оптимизации работы администраторов, связанной с управлением доступом к ресурсам;
- унификации правил предоставления доступа к разнородным ресурсам;
- повышению общего уровня информационной безопасности в системе ресурсов;
- уменьшению времени и усилий пользователей, требуемых для получения доступа к ресурсам.

Основные технологические понятия и сущности

Функционирующая реализация модели единой авторизации может быть разделена на несколько независимых и заменяемых компонентов, взаимодействующих друг с другом по специальным протоколам, которые будут описаны ниже. Необходимость обеспечения такой независимости продиктована, во-первых, гетерогенностью современных информационных ресурсов (напомним, что сюда включаются столь разнородные объекты, как веб-сайты и точки доступа Wi-Fi) и, во-вторых, вытекающим из данной гетерогенности объемом функционала системы. Каждый из компонентов, как правило, весьма сложен в реализации, сама же система целиком реализуема только путем интеграции всех описанных ниже независимых компонентов.

Прежде чем перечислить эти компоненты, хотелось бы формально разделить такие понятия, как идентификация, аутентификация и авторизация. Это разделение крайне важно постольку, поскольку выполнение данных функций может лежать на разных компонентах, что значительно повышает гибкость системы.

Идентификация (*identification*) – присвоение субъектам и объектам доступа идентификатора и / или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов [1].

Аутентификация (*authentication*) – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Авторизация (*Authorization*) – подтверждение прав пользователей при доступе к системе [2]. Иными словами, под авторизацией подразумевается непосредственно предоставление доступа (или отказ в доступе) пользователю к ресурсу.

Теперь перейдем непосредственно к описанию компонентов.

1. *Хранимый слой* (*persistent layer*) – одна или несколько баз данных, содержащих полную информацию о ресурсах, пользователях системы и об их правах в системе. Фактически данный модуль отвечает концепции централизованного хранилища данных на множестве информационных ресурсов. Хранимый слой может взаимодействовать с остальными модулями,

[1] Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.: http://www.fstec.ru/_spravs/_spc/doc_3_3_020.htm

[2] Руководящий документ. Руководство по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 г.: http://www.fstec.ru/_spravs/_spc/doc_3_3_020.htm

путем использования различных языков и протоколов, наиболее распространенными из которых являются SQL и LDAP.

2. *Провайдер идентификации* (*identity provider*) – модуль, осуществляющий процедуру идентификации и аутентификации пользователя. Данный модуль принимает запросы, содержащие некоторый набор авторизационных данных (credentials), и на основе этих данных подтверждает, соответствует ли личность пользователя заявленной. При этом для таких процедур, как проверка пароля, компонент обращается к хранимому слою, настройка связи с которым осуществляется заранее администратором. Как уже говорилось, логика работы провайдера идентификации независима от технологии реализации хранимого слоя. Крайне важным моментом является тот факт, что, однажды выполнив процедуру аутентификации пользователя, провайдер идентификации в дальнейшем хранит пользовательскую *сессию*, что позволяет ему при следующем запросе не требовать повторного введения авторизационных данных. Таким образом, дальнейшее взаимодействие компонентов системы единой авторизации проходит для пользователя незаметно.

3. *Сервис-провайдер* (*service provider*) – модуль, обеспечивающий автоматическую авторизацию пользователя на каждом из ресурсов. Он отправляет запрос провайдеру идентификации в момент, когда пользователь пытается обратиться к ресурсу, с целью подтверждения заявленной личности пользователя. Имеют право на существование модели, рассматривающие данный компонент как часть ресурса либо как внешнюю для него сущность. Так или иначе, сервис-провайдер тесно интегрирован с ресурсом (часто в виде модуля или плагина) и реализован непосредственно в расчете на конкретное программное обеспечение, функционирующее на ресурсе.

4. *Менеджер ролей* (*role manager*) – модуль, отвечающий за проверку прав пользователей по отношению к каждому из ресурсов. Важно, что данная логика проверки прав вынесена за пределы собственно ресурсов и полностью независима от каждого из ресурсов, а также от процедур аутентификации и авторизации. Фактически менеджер ролей занимается лишь обработкой запросов, требующих подтверждения наличия у заданного пользователя заданной роли. Хотя данная терминология подразумевает использование ролевой модели управления доступом, как наиболее применимой в подобной системе, вариант использования других моделей нисколько не исключает возможности включения в систему компонента со сходным функционалом.

Итак, как мы видим, описанный подход позволяет обеспечить независимость друг от друга, а значит и гибкость реализации для следующих процедур: поддержание и хранение данных о пользователях, в том числе авторизационных, аутентификация и поддержание сессии, авторизация на каждом из ресурсов, управление правами доступа пользователей.

Технологии, используемые для реализации концепции единой авторизации

1. LDAP. В настоящее время протокол LDAP является технологическим стандартом в области организации корпоративных хранилищ данных. Хранилище данных, реализованное с учетом поддержки протокола LDAP, называют каталогом (directory), а соответствующую СУБД – службой каталогов (directory service). Особенностями хранилищ данных на основе LDAP являются:

- ориентированность на чтение. Предполагается, что количество запросов на чтение данных существенно превышает количество запросов на модификацию;
- иерархичность структуры данных. Данные в каталоге LDAP представлены в виде дерева и адресуются путем указания пути к вершине от корня (в отличие от табличного представления, характерного для SQL-баз);
- ориентированность на распределенность и реплицируемость;
- отсутствие принципа транзакционности при обращении к базе;
- наличие стандартной схемы LDAP. Данная схема включает основные классы сущностей, необходимые для создания корпоративных хранилищ данных (такие как персона, отдел, единица оборудования и т. д.).

Протокол LDAP поддерживается основной частью современного серверного ПО, при этом наличие стандартной схемы позволяет минимизировать конфигурацию каждого конкретного продукта, используя унифицированные стандартные решения.

2. SAML. Использование протокола SAML является одним из наиболее распространенных технологических решений задачи организации единой аутентификации на web-ресурсах. Протокол специфицирует процедуру поддержания пользовательской сессии путем сохранения и дальнейшей проверки cookies в браузере пользователя. SAML является протоколом взаимодействия между провайдером идентификации и сервис-провайдером, который перенаправляет пользователя к провайдеру идентификации в том случае, если в его браузере не найдено необходимых авторизационных данных.

Фактически термины *identity provider* и *service provider* происходят именно из терминологии данного протокола, хотя используются данные сущности во многих других решениях.

Основным недостатком протокола SAML является его ограниченность областью веб-ресурсов, которая, несомненно, не исчерпывает всего множества информационных ресурсов, которыми обладает современное предприятие.

3. OpenID и Windows Live ID. Стандарты, схожие по форме реализации и задачам с SAML, используемые многими крупными веб-ресурсами. Согласно данным технологиям, сервис может взять на себя роль провайдера идентификации, выдав каждому пользователю идентификатор и подтверждая в дальнейшем, что пользователь действительно авторизован на сервисе под данным идентификатором. Так, крупнейшим OpenID-провайдером на текущий момент является сервис LiveJournal, и на ресурсах, поддерживающих авторизацию по OpenID, пользователю для прохождения авторизации достаточно указать имя своей учетной записи на LiveJournal.

Стандарт OpenID используется такими крупнейшими корпорациями, как AOL, BBC, Google, IBM, MySpace, PayPal, Yahoo! и др.

Windows Live ID является аналогичной и совместимой с OpenID технологией от Microsoft. Этот стандарт используется на различных сервисах Microsoft, таких как Hotmail, MSN, Xbox Live и др.

4. RADIUS (Remote Authentication in Dial-In User Service) является протоколом класса AAA (Authentication, authorization, accounting). Понятия аутентификации и авторизации уже были разобраны в данной статье, последний термин, accounting, подразумевает ведение статистики использования сетевых ресурсов. Протокол используется для организации авторизованного доступа в Интернет с помощью таких технологий, как VPN, Wi-Fi, DSL и т. д.

Таким образом, RADIUS на сегодняшний день является наиболее распространенной технологией для интеграции в систему единой авторизации таких ресурсов, как точки доступа Wi-Fi и VPN сервера. Протокол поддерживается подавляющим числом современного сетевого оборудования и ПО, в том числе некоторыми SAML-серверами. В качестве хранимого слоя для RADIUS-сервера может быть использована БД на основе LDAP или SQL.

5. Kerberos. Данный протокол разработан для организации безопасной аутентификации на множестве ресурсов, т. е. его использование минимизирует риски, связанные с перехватом пароля пользователя. Данная цель достигается путем использования серии шифров на секретных ключах пользователя, сервисов и служебных серверов Kerberos. Важной особенностью технологии является тот факт, что ни пользовательский пароль, ни даже его хэш, не передается по сети, а используется в качестве ключа для расшифровки ответа от сервера аутентификации (CA). После успешной аутентификации сервер предоставляет пользователю сессионный ключ для доступа к серверу выдачи билетов (Ticket Granting Server, TGS), который в свою очередь предоставляет пользователю сессию (билет) на доступ к нужному сервису.

Использование CA и TGT как третьей стороны позволяет осуществлять подтверждение личности не только клиента, но и сервиса. Каждая сессия при этом имеет жесткую привязку к IP клиентской машины и ограничена по времени.

Реализация протокола включена в большинство распространенных операционных систем, в том числе Microsoft Windows, Mac OS X, Red Hat Enterprise Linux, FreeBSD, Oracle Solaris и др.

Технологические решения от Microsoft:
Microsoft Windows, Active Directory, IIS, Microsoft Exchange Server

Компания Microsoft реализует решение задач управления информационными ресурсами сети и единой авторизации на множестве этих ресурсов, основанное на использовании протокола LDAP и интегрированное в операционные системы семейства Windows, начиная с Windows NT [3].

Центральным компонентом данной технологии является служба LDAP каталогов Active Directory. Основной логической единицей управления является домен как именованное подмножество ресурсов (в первую очередь компьютеров) в сети. В свою очередь, домены могут объединяться в такие структуры, как деревья доменов и лес доменов. Между доменами в данных структурах устанавливаются отношения доверия, которые, например, позволяют пользователям одного домена авторизоваться на ресурсах другого.

Для каждого домена назначается контроллер домена – компьютер, на котором размещается хранилище данных LDAP, содержащее информацию о ресурсах и пользователях домена. Для повышения надежности системы контроллером домена обычно назначают не одну, а несколько машин, в этом случае осуществляется репликация данных между контроллерами, т. е. данные разных контроллеров периодически синхронизируются. Кроме того, каждый из доменов хранит свою копию схемы данных каталогов LDAP и конфигурации (т. е. общей топологии) системы.

Для осуществления поиска по всему лесу доменов создается также один или несколько глобальных каталогов (GC), содержащих частичный набор атрибутов каждого объекта из леса (неполная реплика).

Кроме того, существует 5 типов операций, каждая из которых может быть назначена только одному конкретному контроллеру домена в пределах домена или даже всего леса доменов (в зависимости от операции). Это так называемые FSMO (Flexible single-master operations, операции с одним исполнителем). Контроллер, которому назначена такая операция, называется мастером операции (operation master):

1) мастер схемы (schema master) – отвечает за обработку изменений схемы каталогов;
2) мастер именования доменов (domain naming master) – отвечает за добавление и удаление доменов в лесу;
3) мастер относительных идентификаторов (relative ID master) – для конкретного домена отвечает за присвоение идентификаторов объектов в пределах домена;
4) эмулятор основного контроллера домена (PDC emulator) – нужен для совместимости с Windows NT (в более поздних версиях нет понятия основного контроллера, все контроллеры равноправны);
5) мастер инфраструктуры (infrastructure master) – отвечает за обновление данных контроллеров домена при изменении данных глобального каталога.

Другой формой структуризации данных Active Directory является разбиение на сайты, т. е. по принципу физической, а не логической структуры. При этом сайт может размещаться более чем на одном домене, а домен может размещать более одного сайта. Репликация между данными сайтов настраивается отдельно в терминах каналов и мостов связи.

Как мы можем заметить, Microsoft активно использует технологии репликации LDAP для поддержания целостности и доступности данных об обширном множестве распределенных ресурсов, сохраняя при этом производительность всей системы путем предоставления своего отдельного хранилища для каждой локальной подгруппы ресурсов (домена).

Итак, авторизация на множестве информационных ресурсов Windows – это фактически авторизация в домене, которую осуществляет контроллер домена. В случае наличия у данного домена доверительных отношений с другими пользователь также может авторизоваться на ресурсах этих доменов, при этом для аутентификации используется протокол Kerberos, пришедший на замену устаревшему протоколу NTLM от Microsoft.

Следующей единицей логического разбиения множества ресурсов является подразделение (oganizational unit), заимствованное Active Directory непосредственно из стандартной схемы

[3] Active Directory Archeticture: http://technet.microsoft.com/en-us/library/bb727030.aspx

LDAP. Для сайта, домена и подразделения могут быть настроены групповые политики, т. е. общие настройки, применяемые к каждому из компьютеров внутри контейнера. Такими настройками могут быть настройки прокси-сервера при подключении рабочих машин к Интернету, настройки удаленного рабочего стола и многое другое.

Существует и такая специфичная возможность, как подключение сетевой директории в качестве локальной при помощи групповой политики. Таким образом, пользователю могут быть доступны его файлы независимо от того, на каком из компьютеров домена он авторизовался. Также существует возможность настройки сценариев, выполняемых при подключении и отключении пользователя, которые пишутся на языках Jscript и VBScript и выполняются специальным компонентом Windows Script Host (WSH). Эта настройка также осуществляется с помощью групповых политик.

Доступ пользователей к различным ресурсам настраивается при помощи механизма ACL (Access Control Lists). Это обозначает, что для каждого объекта в каталоге хранится список пользователей или групп пользователей с указанием конкретного типа доступа (чтение, запись, удаление и т. д.), который разрешен данному пользователю в отношении данного объекта. Аналогично групповым политикам ACL наследуются дочерними элементами от родительских, при этом наследованием также можно управлять и, в случае необходимости, для того или иного объекта отключить. Фактически описанный подход функционально эквивалентен ролевой модели управления доступом.

Microsoft осуществляет тесную интеграцию Active Directory с различными серверными приложениями, такими как IIS (Web-сервер) и Microsoft Exchange Server (почтовый сервер). Это позволяет, например, проводить аутентификацию пользователей на web-ресурсах, базирующихся на IIS, при помощи встроенной аутентификации Windows (т. е. через Active Directory). То же самое можно сказать и о доступе к почтовым ящикам Microsoft Exchange. Подобный подход позволяет значительно приблизиться к реализации концепции единой авторизации на множестве ресурсов сети.

Резюмируя вышесказанное, можно сделать следующие выводы: решение от Microsoft является комплексным и обширным по функциональности, представляет собой мощный инструмент для администрирования сетевых ресурсов предприятия. Его особенностью является центрированность решения вокруг операционной системы Windows, которая берет на себя основную часть функциональности, связанной с управлением сетевыми ресурсами. Фактически сама операционная система тесно интегрирована со слоем хранения и содержит в себе логику взаимодействия с этим слоем. Это же является и основным недостатком подхода, который становится неприменим, если множество сетевых ресурсов содержит ресурсы, не связанные с Windows. И хотя существуют технологические решения, обеспечивающие интеграцию Active Directory, например с UNIX-системами, применение таких решений накладывает существенные ограничения и в конечном счете лишает преимуществ комплексного подхода.

Тесная интегрированность компонентов в решении Microsoft не позволяет провести их четкого функционального разделения, описанного ранее в данной статье, что существенно сказывается на гибкости системы и также может быть отнесено к недостаткам данного подхода.

Технологические решения от IBM: IBM Tivoly

Все компоненты решения IBM, связанного с организацией единой точки доступа к ресурсам сети, входят в более широкий программный комплекс управления информационной инфраструктурой предприятия IBM Tivoly. Данный комплекс содержит множество различных программных систем, обеспечивающих структурирование, интеграцию и управление разнородными информационными ресурсами предприятия [4].

Компонентами IBM Tivoly, отвечающими за управление данными о персонах в системе, доступом к ресурсам и авторизацией, являются:

- IBM Tivoly Directory Server;

[4] Решения IBM Tivoly для управления информационной инфраструктурой. www.ibm.com/software/ru/tivoli/

- IBM Tivoly Directory Integrator;
- IBM Tivoly Identity Manager;
- IBM Tivoly Federated Identity Manager;
- IBM Tivoly Access Manager for Enterprise Single Sign-on;
- IBM Tivoly Access Manager for e-business;
- IBM Tivoly Access Manager for Business Integration;
- IBM Tivoly Access Manager for Operating Systems;
- IBM Tivoly Risk Manager.

Как можно заметить, аналогично решению Microsoft центральным компонентом является служба каталогов LDAP. В случае IBM это IBM Tivoly Directory Server, реализованный на основе СУБД IMB DB2. Данный сервер поддерживает широкий спектр операционных систем и, в том числе, является встроенным в такие системы, как IBM OS/400, z/OS и AIX.

Кроме того, существует возможность интеграции нескольких LDAP каталогов (не обязательно от IBM), а также других разнородных хранилищ идентификационных данных с помощью компонента IBM Directory Integrator. Данный компонент выполняет синхронизацию данных в локальных хранилищах, а также поддержание единого централизованного метакаталога.

Далее выполнение задач управления пользовательскими учетными записями берет на себя компонент IBM Tivoly Identity Manager (концепция Identity Manager (Provider) уже была ранее описана в этой статье). Идейной особенностью данного компонента является попытка максимального снижения нагрузки на системных администраторов путем предоставления пользователям возможности самообслуживания (например, в задачах управления паролями), а также возможности для администратора делегировать часть своих полномочий другим сотрудникам.

Помимо базовой версии менеджера идентификации, IMB Tivoly предоставляет также федеративную версию, позволяющую кооперировать процедуры управления пользователями и авторизации на информационных ресурсах с другими компаниями. При этом возможно как предоставление своих сервисов пользователям компании-партнера без регистрации их в своих базах данных, так и получение доступа к дружественным ресурсам без дополнительной регистрации пользователей на стороне партнера. Это достигается путем использования таких технологий, как SAML и WS-Security.

Управление правами доступа пользователей, а также выполнение процедур аутентификации и авторизации пользователей берет на себя семейство компонентов IBM Tivoly Access Manager.

Основным из них является IBM Tivoly Access Manager for Enterprise Single Sign-on, основанный на комплексе технологий Passlogix и решающих с их помощью задачу организации единообразного доступа к информационным ресурсам корпоративной сети. Данный компонент взаимодействует с множеством типов ресурсов, среди которых приложения на основе Windows, Java, Web и т. д. С другой стороны, компонент поддерживает различные методики аутентификации пользователей, в том числе биометрические сенсоры и смарт-карты. После обработки различных типов запросов аутентификации компонент далее делегирует проверку данных пользователей к Identity Manager.

Существуют также три более специфичных вида Access Manager.

1. IBM Tivoly Access Manager for Operating Systems – для управления доступом к компьютерам с операционными системами UNIX и Linux.

2. IBM Tivoly Access Manager for Business Integration – для управления доступом в приложениях, интегрированных с помощью технологий промежуточного слоя IBM WebSphere. Фактически осуществляется управление доступом к очередям сообщений IBM WebSphere MQ, с помощью которых реализовано взаимодействие приложений в WebSphere.

3. IBM Tivoly Access Manager for e-business – компонент, осуществляющий управление доступом к ресурсам корпоративной сети извне данной сети, т. е. из Интернета. Компонент позволяет построить инфраструктуру электронного бизнеса при помощи Web-приложений J2EE, а также управлять доступом к данной инфраструктуре через HTTP-прокси-сервер, расположенный в специальной «демилитаризированной зоне» между двумя брандмаурэми.

Все четрые типа Access Manager управляются единообразно и централизованно через компонент, называемый Access Manager Management Server.

Кроме этого система управления доступом в IBM Tivoly включает компоненты мониторинга, диагностики нарушений безопасности и автоматического реагирования на угрозы.

Исходя из вышесказанного можно заметить, что в противоположность Microsoft, которая строит свои решения путем интеграции собственных продуктов, игнорируя при этом остальные, IBM Tivoly ставит своей задачей интегрировать максимально широкий спектр ресурсов, опираясь при этом на универсальные стандарты (например, J2EE), однако же в случае необходимости выполняя и «штучное» подключение тех или иных видов ресурсов. Технологии же IBM в общей системе выполняют роль промежуточного слоя, унифицируя процедуры управления разнородными ресурсами, при этом сильная интеграция продуктов IBM между собой также имеет место быть.

Что касается структуры компонентов IBM Tivoly, можно заметить, что она весьма близка к той, что была описана в данной статье выше, с поправкой на тот факт, что некоторые компоненты берут на себя разные аспекты функциональности, например компоненты Access Manager помимо функций сервис-провайдера также берут на себя управление правами пользования и частично аутентификацией. Это следует объяснять желанием IBM добиться максимальной гибкости конфигурации компонентов, например, обеспечения возможности использовать Access Manager автономно, без Identity Manager. Тем не менее соответствие идеологии построения системы IBM Tivoly той идеологии, которая описана в данной статье, очевидно.

Технологические решения от Oracle: Oracle Identity Management

Решение от Oracle включает более 20 компонентов, зачастую дублирующих друг друга по функциональности. Такое дублирование связано с ребрендингом значительного количества разработок Sun после приобретения данной компании фирмой «Oracle» [5]. Компоненты объединены в следующие основные пакеты:

- Oracle Directory Services;
- Oracle Identity Governance;
- Oracle Access Management;
- Oracle Enterprise Single Sign-On;
- Oracle Enterprise Gateway.

Перечисленные компоненты объединяются под названием Oracle Identity Management и являются частью глобального решения по информатизации предприятия Oracle Fusion Middleware. Последний продукт можно считать аналогом IBM Tivoly.

Как и в разработках от Microsoft и IBM, основой решения Oracle является служба каталогов LDAP. В данном случае на выбор предоставляется несколько программных продуктов, в том числе Oracle Virtual Directory – инструмент для создания «виртуального» хранилища, служащего интерфейсом к данным нескольких разнородных источников.

Следующим слоем является пакет Oracle Identity Governance, построенный на Oracle Identity Manager – инструменте управления данными о пользователях, в том числе правами пользователей в терминах ролевой модели управления доступом.

Oracle Access Management решает задачи управления доступом к различным и разнородным приложениям, сервисам (в том числе JavaEE, Web и SaaS) и данным предприятия. На уровне этого пакета также осуществляется организация федеративного доступа к ресурсам (т. е. доступа пользователями нескольких провайдеров идентификации, возможно принадлежащих различным предприятиям).

[5] Oracle Identity Management: http://www.oracle.com/us/products/middleware/identity-management/overview/index.html

Хотя Oracle Access Management непосредственно является инструментом организации единого доступа к ресурсам (Single Sign-On), пакет Oracle Enterprise Single Sign-On расширяет возможности в этом направлении, предлагая концепцию, в соответствии с которой пользователь вводит пароль единственный раз при авторизации в операционной системе своего рабочего компьютера. После этого в процессе работы он не замечает никаких других процедур авторизации в используемых им приложениях и информационных ресурсах, так как выполнение этих процедур берет на себя Oracle Enterprise Single Sign-On. При этом реальный доступ к ресурсам может быть защищен длинными и сложными для подбора паролями, управление которыми осуществляется при помощи указанного продукта. Также поддерживается возможность аутентификации с помощью смарт-карт, биометрия и т. д.

Последний компонент, Oracle Enterprise Gateway, служит для организации доступа к ресурсам предприятия извне (аналогично IBM Tivoly Access Manager for e-business в IBM Tivoly), являясь инструментом создания «демилитаризованной зоны». При этом осуществляется интеграция с Oracle Identity Manager и Oracle Access Manager, что позволяет полностью включить данный аспект организации доступа к ресурсам в схему управления доступом Oracle Identity Management.

Подводя итог, можно заметить существенное сходство технологических подходов IBM и Oracle, что неудивительно ввиду совпадения решаемой ими задачи – задачи интеграции и управления разнородными информационными ресурсами предприятия. Различия в данном случае могут быть найдены в нюансах терминологии, в распределении функциональности между компонентами, в структуре взаимодействия компонентов и объединения их в пакеты, а также в других нефункциональных особенностях (например, стоимости соответствующего ПО).

Заключение

В статье была описана верхнеуровневая архитектура системы единой авторизации на множестве информационных ресурсов сети. Был перечислен набор компонентов данной системы со строгим указанием функциональности каждого из них, а также схем взаимодействия между ними. Далее были рассмотрены наиболее распространенные в настоящее время технологии, позволяющие реализовать указанную функциональность.

Наконец, были рассмотрены технологические решения крупнейших компаний-разработчиков ПО в данной области, показано соответствие этих решений описанной архитектуре (а также точки расхождения с ней), приведены примеры использования упомянутых технологий.

Отметим, что на примере трех рассмотренных решений мы наблюдаем два принципиально разных подхода к построению систем единой авторизации. Один из них подразумевает построение множества ресурсов сети на основе тесно интегрированных продуктов одного разработчика. Второй – интеграцию разнородных компонентов через некоторый промежуточный слой.

Первый вариант значительно дешевле в плане затрат на внедрение: мы фактически получаем готовое комплексное решение «из коробки». Второй вариант универсален, мы практически не ограничены в выборе технологий для реализации самих ресурсов, в том числе можем интегрировать в систему и сегменты, целиком построенные первым способом. Однако за эту универсальность мы платим серьезным усложнением общей системы, которая вынуждена учитывать множество частных случаев и при этом использовать методики единообразного управления частными разнородными ресурсами.

Реалии же построения подобных систем управления оказываются таковы, что, как правило, эти системы внедряются уже на очень сильно развитой инфраструктуре разнородных ресурсов, и выбор универсального подхода оказывается необходимым. Однако же, если система управления строится одновременно с инфраструктурой и появляется возможность построения общей системы на основе интегрированного множества продуктов, преимущества первого способа могут оказаться решающими.

Список литературы

1. *Жижимов О. Л., Федотов А. М., Юданов Ф. Н.* Модель управления информационными ресурсами организации // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2010. Т. 8, вып. 4. С. 81–95.

Материал поступил в редакцию 18.07.2012

F. N. Yudanov, A. M. Fedotov, R. S. Seitkasym

SINGLE SIGN-ON AND COMMON NETWORK RESOURCES ACCESS POINT TECHNOLOGIES

The article contains analysis of present technologies of building enterprise informational infrastructure implementing common network resources access point concept. The main questions covered in article are the details of single sign-on procedure implementation and review of top software developing companies' solutions that use single sign-on technologies in complex.

Keywords: single sign-on, information resources control, LDAP, Active Directory, IBM Tivoly, Oracle Identity Management.