электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.624

Сервис синхронизации учетных записей пользователей в рамках сервис-ориентированной архитектуры

***Сирота А.О.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Программное обеспечение ЭВМ и информационные технологии»
andrewio@ya.ru

Научный руководитель: Остриков С.П., к.т.н, Управление информатизации - ВЦ
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
ostrikov@bmstu.ru

Введение

Успешная деятельность современного Университета невозможна без широкого внедрения информационных технологий. Процесс построения единой информационной среды вуза, реализуемой с применением сервис-ориентированной архитектуры (СОА), делает актуальной задачу построения единой системы аутентификации, авторизации и учета ресурсов, которые потребляют пользователи (accounting). Это позволит уйти от локальных хранилищ пользователей к единому, и сделать задачу аутентификации пользователей в существующих и вновь вводимых информационных систем универсальной.

За последние несколько лет в МГТУ им. Н.Э. Баумана успешно проводятся работы по построению информационной среды Университета. Для хранения информации учетных данных и прав пользователей в информационных системах был сформирован кадровый справочник МГТУ им. Баумана в виде LDAP-структуры, размещенной в Microsoft Active Directory [1]. Справочник синхронизирован с информационной системой управления кадрами. Кроме того, из информационной системы «Электронный Университет» в кадровый справочник помещена информация о студентах и аспирантах. Проведены работы по формированию достаточного перечня типов серверов аутентификации. Это CAS-сервер, RADIUS-сервер, LDAD-запросы к единой базе учетных данных пользователей, аутентификация в домене Windows. Иными словами, сформирована инфраструктура для внедрения в Университете единой службы аутентификации пользователей. Единая служба аутентификации подразумевает наличие

единого пространства учетных данных пользователей наряду с широким выбором предлагаемых механизмов аутентификации. [1]

Следующим этапом в построении единой информационной среды Университета является перевод действующих информационных систем на аутентификацию пользователей в единой службе аутентификации. Успех данного этапа обеспечит принципиально новый уровень интеграции информационных систем вуза.

Однако, при внедрении в Университете единой службы аутентификации нельзя не учитывать накопленный опыт в управлении учетными данными пользователей в действующих информационных системах. Особенно, это важно в случае с информационными системами, с помощью которых уже многие годы обеспечивается массовый доступ пользователей к наиболее востребованным ИТ-сервисам Университета (корпоративная электронная почта, беспроводный интернет, и др.). Перевод многочисленных пользователей Университета на вновь созданные учетные записи, даже для решения такой важной задачи как построение единой службы аутентификации, есть неоправданное насилие над пользователями. Пользователи этих, критически важных для университета информационных систем, не должны почувствовать дискомфорт.

Решением является разработка и внедрение программного продукта, позволяющего осуществить мягкую (без существенного изменения существующих ИС) интеграцию систем управления пользователями в критически важных для Университета информационных системах с единой службой аутентификации. В качестве критически важной информационной системы, рассматривается автоматизированная система расчетов LANBilling, с помощью которой многие годы успешно регистрируются пользователи Университета и осуществляются услуги электронной почты, беспроводного Интернета, удаленного доступа к корпоративным приложениям.

В работе решаются следующие задачи:

- Проведен анализ инфологической и даталогической моделей базы данных автоматизированной системы расчетов LANBilling;
- Проведен анализ интеграционных возможностей автоматизированной системы расчетов LANBilling;
- Проведен анализ LDAP-структуры кадрового справочника МГТУ им. Баумана, размещенного в AD;
- Проведен анализ методов доступа на чтение и запись к LDAP-структуре кадрового справочника МГТУ им. Баумана, размещенного в AD и выбран наиболее эффективный;

- Предложена процедура первичной синхронизации учетных записей пользователей, уже зарегистрированных в автоматизированной системе расчетов LANBilling с учетными записями пользователей в кадровом справочнике МГТУ им. Баумана размещенном в AD;
- Предложена процедура синхронизации учетных записей пользователей на этапе их первичной регистрации в автоматизированной системе расчетов LANBilling с учетными записями пользователей в кадровом справочнике МГТУ им. Баумана размещенном в AD;
- Предложена процедура синхронизации учетных записей пользователей на этапе внесения изменений в регистрационные данные в автоматизированной системе расчетов LANBilling с учетными записями пользователей в кадровом справочнике МГТУ им. Баумана размещенном в AD;
- Разработана информационная модель и предложена архитектура программного продукта;
- Оценка работоспособности системы при ожидаемом уровне нагрузок;
- Внедрение предложенного программного продукта в информационную инфраструктуру МГТУ им. Н.Э. Баумана.

Среди множества существующих в университете систем управления пользователями наибольший интерес для анализа представляют две.

Первая, это единая служба управления пользователями, сопряженная с кадровой системой - служба Microsoft Active Directory (далее AD), появившаяся в МГТУ в последние годы. Несомненным преимуществом данной системы управления пользователями является ее полнота. В AD содержится информация обо всех работающих сотрудниках университета. Система оперативно отслеживает все изменения в кадровой структуре университета.

Наряду с преимуществами, данная система управления пользователями имеет существенные недостатки. Так, в данной системе управления пользователями учетная запись в AD (логин), пароль и электронная почта сотрудника формируются формальным образом (генерируются в соответствии с заданным алгоритмом). [1, 2]

Вторая - это система управления пользователями реализованная на основе программного продукта «Автоматизированная система расчетов LANBilling». Данная система функционирует в университете уже несколько лет и на ее основе в университете реализуются такие массовые ИТ услуги как: доступ к беспроводному Интернету (Wi-Fi), корпоративная электронная почта, удаленный доступ к корпоративным приложениям

университета, биллинг др. Основным недостатком данной системы управления пользователями является ее изолированность от кадрового справочника университета. Это приводит к тому, что уволенные сотрудники остаются в системе как пользователи. Но данная система управления пользователями имеет и достоинства. Регистрация пользователей в системе происходит на основании их письменного заявления. Следовательно, логин, пароль и адрес электронной почты согласованы с пользователями и уже реально используются ими при получении наиболее востребованных ИТ услуг. Кроме того, LANBilling – единственная система аудита действий пользователей в университете. LANBilling – система типа AAA (от англ. Authentication, Authorization, Accounting), то есть она осуществляет:

- Аутентификацию (сопоставление персоны существующей учётной записи в системе безопасности);
- Авторизацию (сопоставление учётной записи в системе (и персоны, прошедшей аутентификацию) и определённых полномочий);
- Учет (слежение за потреблением ресурсов (преимущественно сетевых) пользователем).

Потребность в синхронизации данных систем управления пользователями, цель данной работы, ставит вопрос об определении достаточного набора атрибутов пользователей, которые можно будет использовать на этапе первичной синхронизации.

Уникальность пользователя определяется по уникальному идентификатор UUID в системе AD и GUID (разновидность UUID) в системе LANBilling. [3, 11]

Основное назначение UUID - это позволить распределённым системам уникально идентифицировать информацию без центра координации. Таким образом, любой может создать UUID и использовать его для идентификации чего-либо с приемлемым уровнем уверенности, что данный идентификатор непреднамеренно никогда не будет использован для чего-то ещё. Поэтому информация, помеченная с помощью UUID, может быть помещена позже в общую базу данных, без необходимости разрешения конфликта имен. [11]

UUID может быть преднамеренно использован повторно, для идентификации той же самой сущности в различных контекстах, что и было реализовано в МГТУ им Н.Э. Баумана между системами AD и LANBilling.

Таким образом, на основании GUID и UUID можно провести идентификацию пользователей одной системы в другой, и осуществить синхронизацию учетных записей: данные из LANBilling поступят в AD.

Наиболее критическими данными для этой цели являются:

- Логин;
- Пароль;
- Электронная почта;
- UUID.

Одна часть пользователей работает с учетными записями AD (для определенных корпоративных приложений), другая – с учетными записями LANBilling (люди получают доступ к Wi-Fi и т.д.). В связи с этим первичная синхронизация должна осуществляться поэтапно, чтобы пользователи, которые работают с учетными записями AD, были бы уведомлены о смене какого-либо параметра.

Таким, образом необходимо предусмотреть, чтобы синхронизация осуществлялась не по всем полям сразу, а лишь по требуемым. И в случае, когда для конкретного пользователя уже была проведена синхронизация по некоторым полям, то не проводить синхронизацию по этим полям. Если же в процессе синхронизации конкретного пользователя не удалось синхронизировать по какой-либо причине, то необходимо предусмотреть синхронизацию его критических данных в индивидуальном порядке.

Отсюда возникает необходимость введения понятия «статуса синхронизации», то есть некоего контролирующего механизма, обеспечивающего целостность синхронизации.

Также необходимо, чтобы инструмент синхронизации не был привязан к определенной платформе и операционной системе. Для обеспечения этого условия достаточно, чтобы инструмент синхронизации был доступен из браузера и использовал один из серверных скриптовых языков.

Сервис синхронизации предполагает следующие прецеденты использования:

- Поиск пользователя в системе AD;
- Поиск пользователя в системе LANBilling с выводом наличия признаков синхронизации с системой AD (статус синхронизации);
- Регистрация нового пользователя в системе LANBilling, существующего в системе AD;
- Изменение по желанию информации о пользователе и обновление информации в системах AD и LANBilling;
- Массовую синхронизацию по одному из критических параметров (логин, пароль, почта) пользователей, существующих в обоих системах.

Структурная схема сервиса синхронизации представлена на рисунке 1.

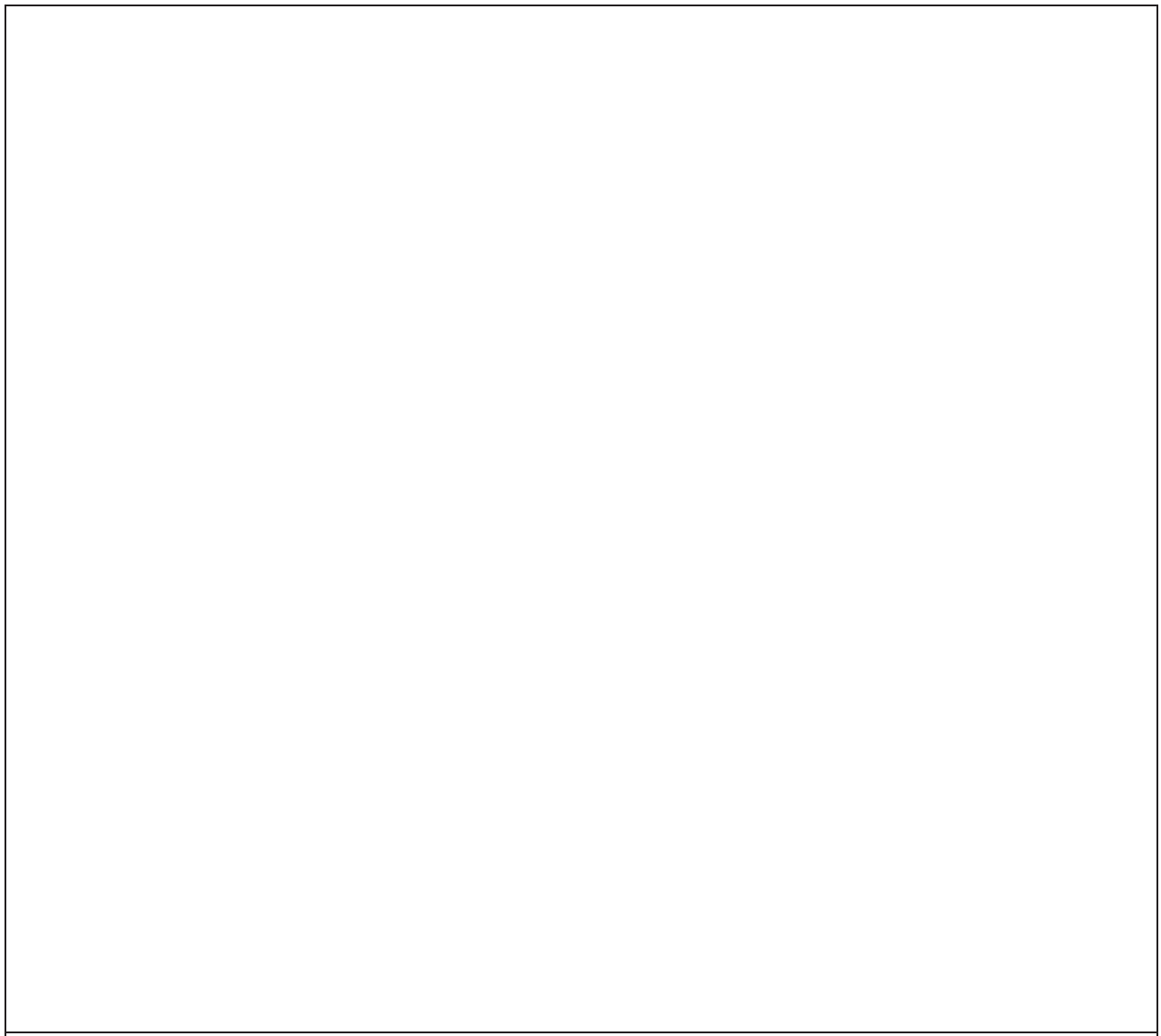

Рис. 1. Структурная схема сервиса синхронизации

Доступ к данным осуществляется следующим образом:

- Для внесения изменений в базу данных системы LANBilling целесообразно посредством SOAP-протокола работать с WSDL-сервисом, который она предоставляет;
- Запросы к системе AD целесообразно формировать в виде LDAP-запросов.

Алгоритм работы сервиса представляется двумя независимыми процедурами:

- Процедура первичной синхронизации учетных записей пользователей, уже зарегистрированных в автоматизированной системы расчетов LANBilling с учетными записями пользователей в кадровом справочнике МГТУ им. Баумана, размещенном в AD, и первичной регистрации пользователей LANBilling с AD;
- Процедура массовой синхронизации учетных записей пользователей.

При выполнении процедуры массовой синхронизации целесообразно не обрабатывать пользователей, которые уже синхронизированы по конкретному полю, чтобы снизить нагрузку на сервис.

При выборочном обновлении полей конкретного пользователя целесообразно иметь возможность видеть, какие поля уже затронула массовая синхронизация.

Таким образом, важным параметром в работе сервиса синхронизации является статус синхронизации. Поле, которым описывается статус синхронизации, присутствует в AD у каждого пользователя под именем Pager. Поле Pager было выбрано с связи с его незадействованностью, а также в целях не реорганизации структуры учетной записи пользователя в AD.

Поле Pager имеет строковый тип и имеет следующий "условный формат: "XXX". Каждый элемент "X" отвечает за синхронизацию конкретного параметра:

- Первый "X" - логин;
- Второй "X" - пароль;
- Третий "X" - почта.

Элемент "X" в качестве значения может принимать единицу, если параметр синхронизирован, и ноль – иначе.

Таким образом, в случае полной синхронизации поле Pager будет соответствовать строке "111".

Для наглядного описания работы сервиса синхронизации используются диаграмма последовательностей в UML-нотации, представленные на рис.2 и на рис.3.

Рассмотрим подробнее диаграмму последовательностей регистрации и обновления пользователя (рис.2).

Пользователь системы (или пользователь сервиса синхронизации) для поиска пользователя системы AD должен ввести в форму сервиса синхронизации относительное различающееся имя или CN (от англ. Common Name), которое в большинстве случаев в настоящей системе AD представлено в формате «Фамилия Имя Отчество». После чего сервис синхронизации отправляет запрос на поиск информации к системе AD, которая в свою очередь должна возвратить список пользователей, чьи CN совпадают с введенными

данными, с сопутствующей информацией. После чего, в случае нахождения совпадения, пользователь системы выбирает конкретного пользователя. Далее сервису синхронизации необходимо проверить, имеется ли такой же пользователь в системе LANBilling посредством направления запроса на поиск информации к системе LANBilling, которая в ответ должна вернуть информацию о существовании пользователя в системе.

Если пользователь не существует в LANBilling, то пользователь системы по желанию может зарегистрировать его, при этом обновив данные в AD (возможно выполнить при успешной регистрации). Результат регистрации и обновления представляется пользователю системы.

Если пользователь существует в LANBilling, то пользователь системы по желанию может изменить его данные, при этом данные обновятся как в системе LANBilling, так и в AD. Результат обновления представляется пользователю системы.

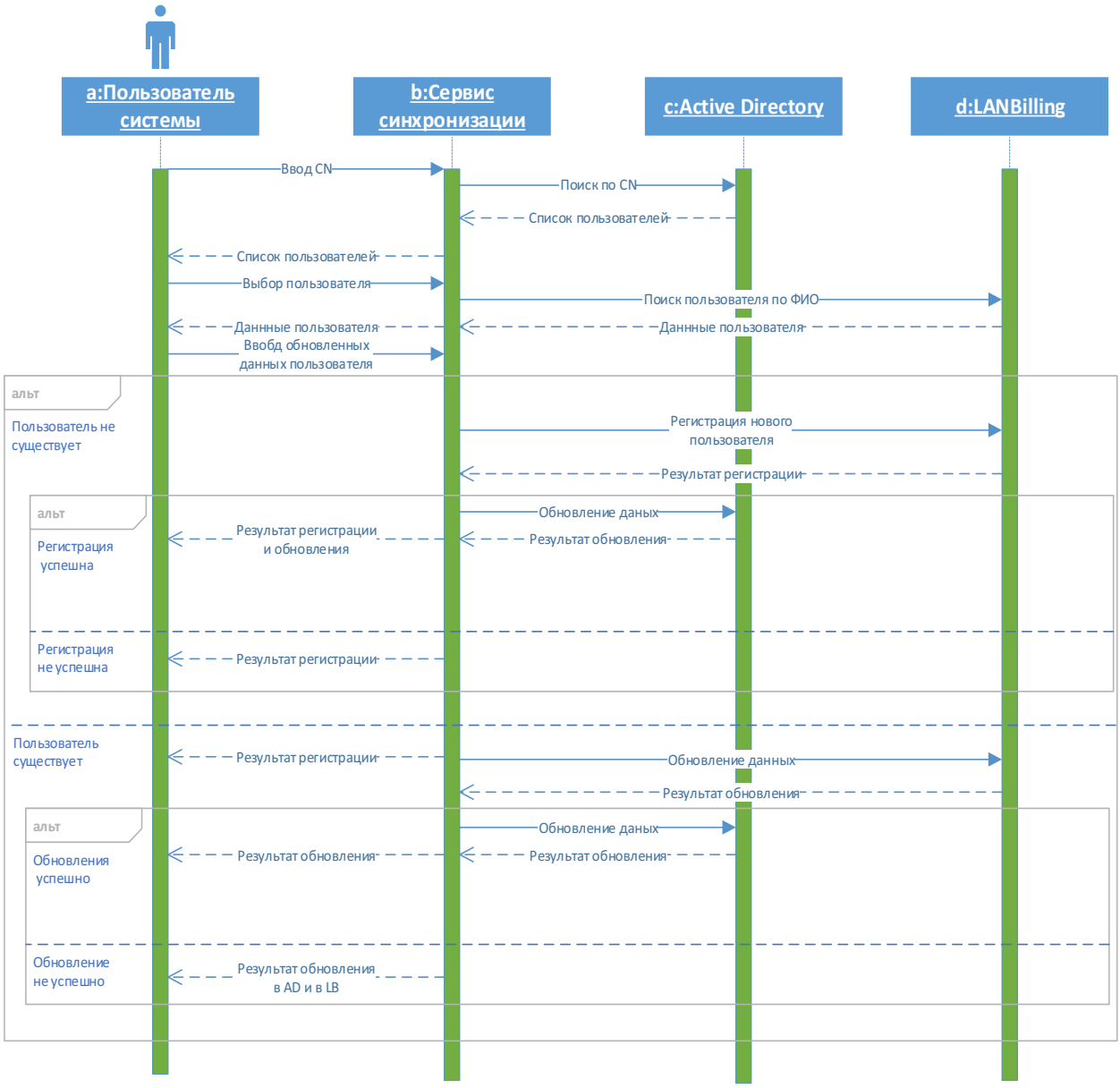

Рис. 2. Диаграмма последовательностей регистрации и обновления пользователя

Рассмотрим подробнее диаграмму массовой синхронизации(рис.3). Пользователю предлагается выбрать одно из критических полей, по которому требуется произвести синхронизацию. После чего происходит последовательная выборка пользователей сервисом синхронизации из LANBilling. Каждый пользователь проверяется на существование в AD на основе UUID.

В случае, если таковой имеется в системе AD, то данные синхронизируемого поля копируются из LANBilling и записываются в аналогичное поле в системе AD. Если последнее действие завершается с ошибкой, то об этом узнает пользователь системы. Он

также информируется о том, на каком именно пользователе системы AD произошла ошибка. Успешные обновления проходят в фоновом режиме.

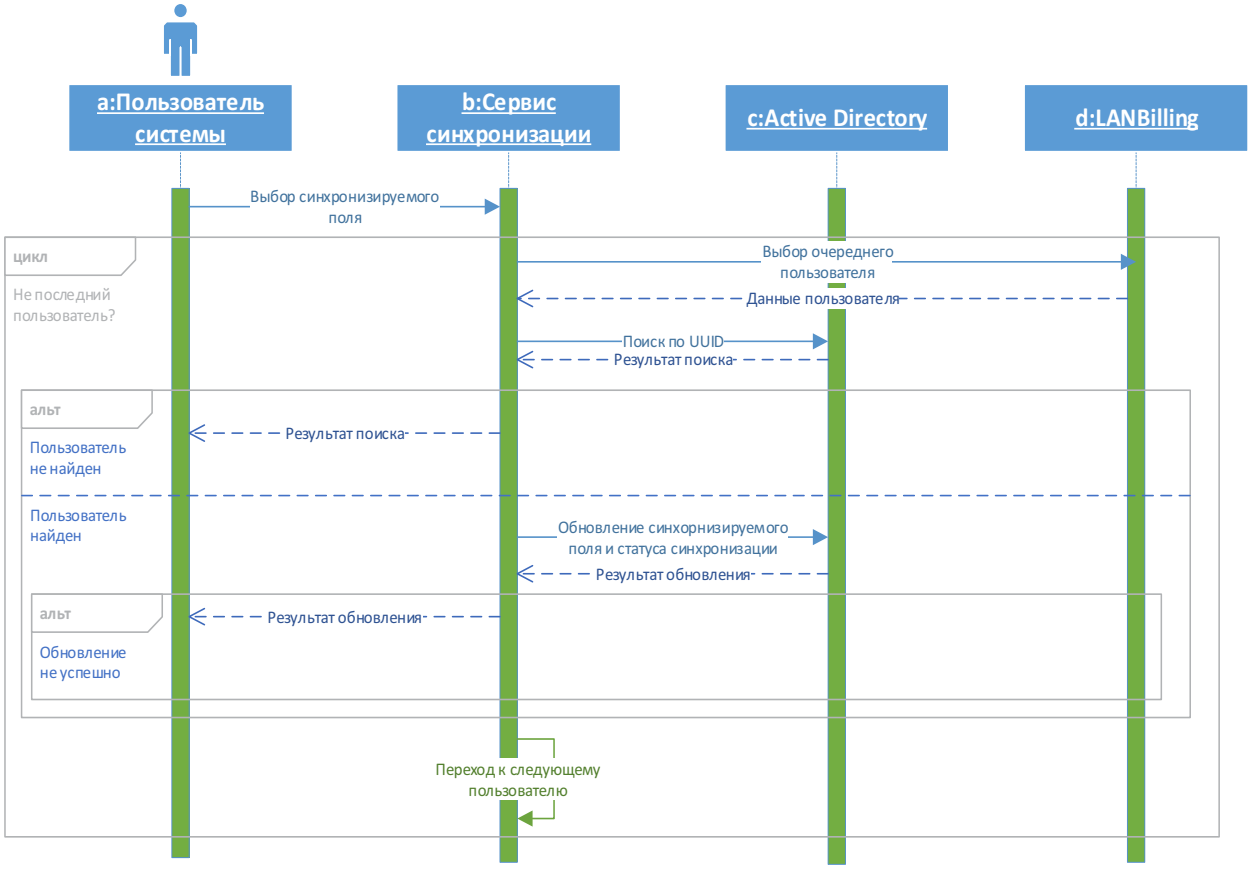

Рис. 3. Диаграмма последовательностей массовой синхронизации

Нагрузочное тестирование

Для проведения нагрузочного тестирования был использован Apache JMeter — инструмент для проведения нагрузочного тестирования, разрабатываемый Apache Software Foundation. Предполагается, что во время сеанса синхронизации, будет происходить фоновая нагрузка на сервер - например, авторизация 100 пользователей в один момент времени.

Настройки плана тестирования представлены на рис. 4 и рис. 5.

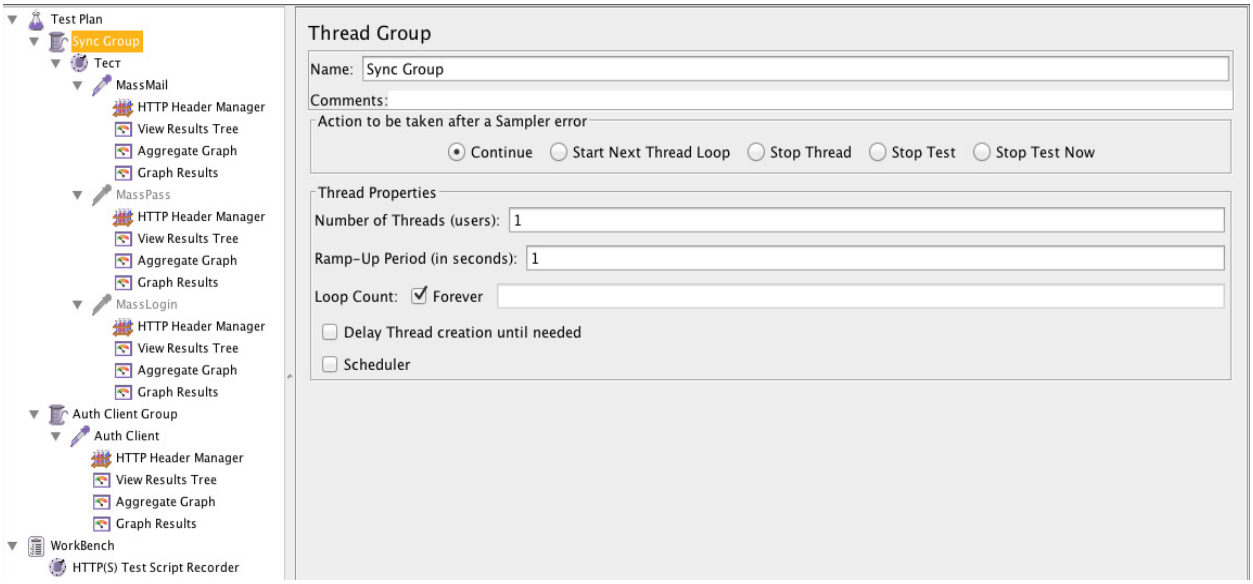

Рис. 4. План тестирования. Поток 1 - Синхронизация

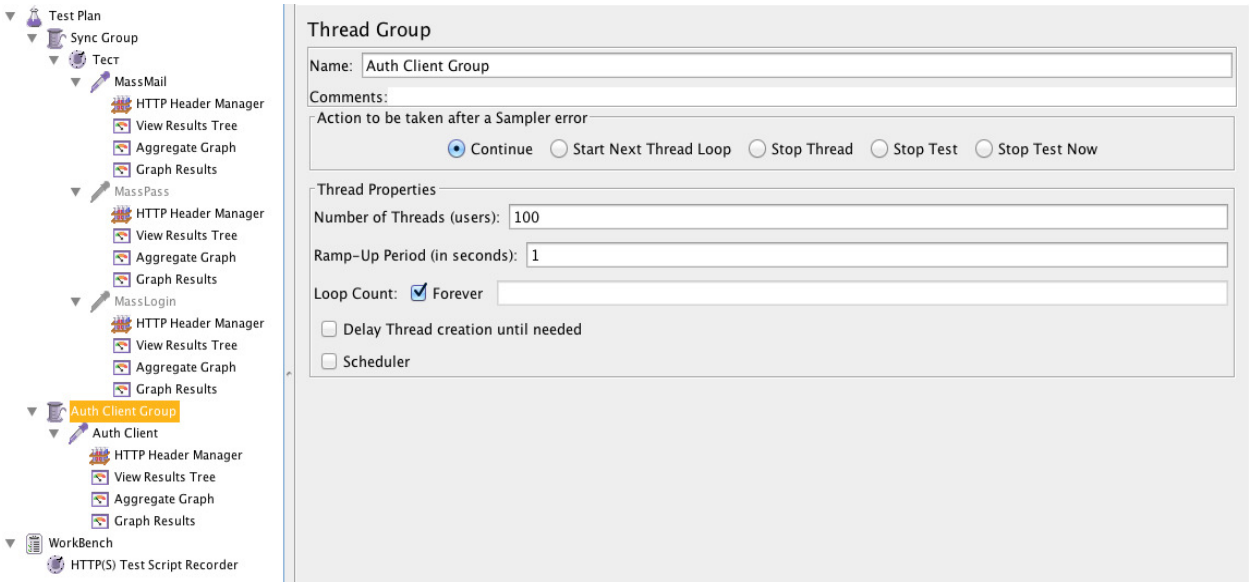

Рис. 5. План тестирования. Поток 2 – Авторизация

После проведения тестирования по синхронизации электронной почты 1000 пользователей получаются следующие результаты.

Как видно из рис. 6, 26 массовых синхронизаций электронной почты при указанной фоновой нагрузке прошли без ошибок. При этом среднее время выполнение синхронизации составляет около 83 секунд. Таким образом можно предположить (как видно из рисунка), что за 1 час можно синхронизировать (по параметру «электронная почта») в среднем около 43300 пользователей.

Label	# Samples	Average	Median	90% Line	Min	Max	Error %	Throughput
MassMail	26	83159	81837	93124	57201	109338	0,00%	43,3/hour
TOTAL	26	83159	81837	93124	57201	109338	0,00%	43,3/hour

Рис. 6. Тестирование массовой синхронизации электронной почты

На графике по авторизации (рис. 8) видно, что производительность (Throughput) не сильно меняется со временем (она стабильна). При этом среднее время ответа после авторизации равно 4,85 секунды.

Это означает, что при заданном плане тестирования не происходит снижения производительности, и роста задержек при выполнении запросов к LANBilling.

Label	# Samples	Average	Median	90% Line	Min	Max	Error %	Throughput
Auth Client	44224	4856	4210	5439	0	2027965	1,02%	18,8/sec
TOTAL	44224	4856	4210	5439	0	2027965	1,02%	18,8/sec

Рис. 7. Тестирование – фоновая нагрузка авторизации

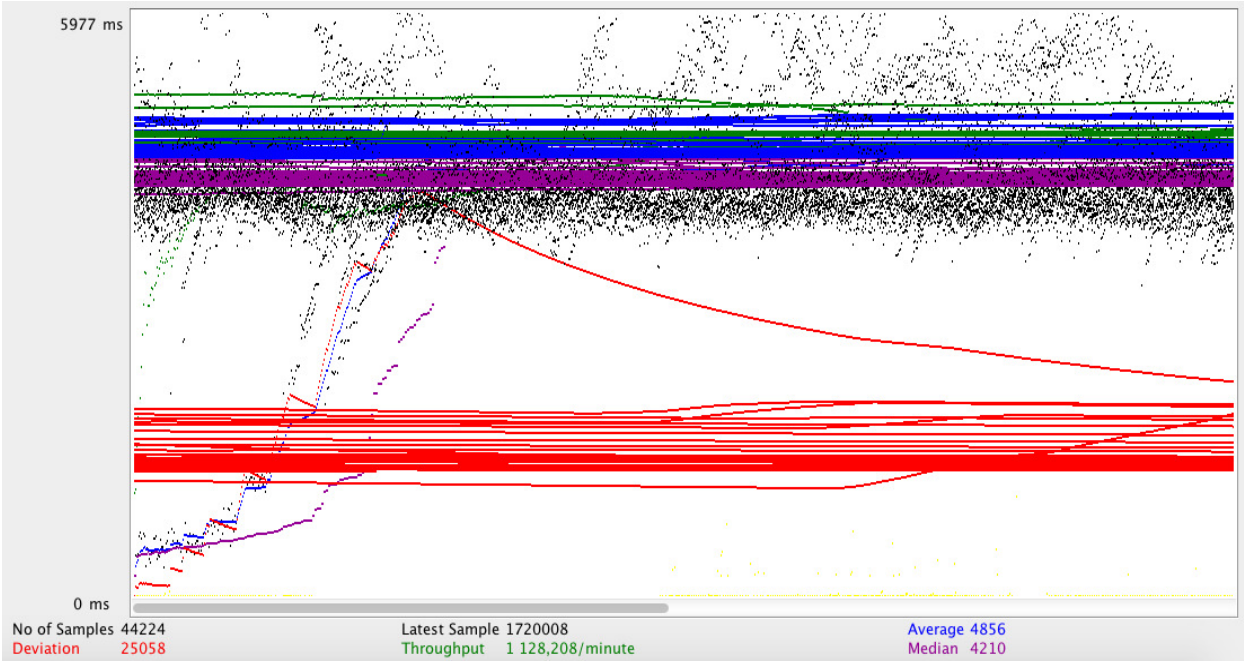

Рис. 8. График процесса авторизации пользователей в LANBilling

Данные по результатам тестирования синхронизации паролей и логинов представлены ниже. Как видно, сервер не генерирует отказы и синхронизация просиходит без ошибок. Таким образом, заявленная фоновая нагрузка не оказывает негативного влияния на процесс синхронизации.

По времени выполнения самая затратная операция – синхронизация по логину.

Label	# Samples	Average	Median	90% Line	Min	Max	Error %	Throughput
MassPass	11	145053	137626	176999	120595	217798	0,00%	24,8/hour
TOTAL	11	145053	137626	176999	120595	217798	0,00%	24,8/hour

Рис. 9. Тестирование массовой синхронизации паролей

Label	# Samples	Average	Median	90% Line	Min	Max	Error %	Throughput
MassLogin	12	135655	128399	162631	118324	170551	0,00%	26,5/hour
TOTAL	12	135655	128399	162631	118324	170551	0,00%	26,5/hour

Рис. 10. Тестирование массовой синхронизации логинов

Для исследования процесса синхронизации со стороны Active Directory был использован инструмент *Performance Monitor*. Эта утилита поставляется вместе с ОС Windows Server, и позволяет предоставлять результаты измеряемых метрик в виде графиков или отчета. Преимуществом этого инструмента является то, что он надежно интегрируется с операционными системами Windows и поэтому отображает достоверные значения различных аспектов производительности. Performance Monitor предоставляет множество объектов производительности, и каждый объект производительности имеет несколько счетчиков.

Были использованы следующие счетчики:

- **ADs \LDAP Searches/sec** – число операций поиска в секунду, выполняемых для запросов по протоколу *LDAP*. Является хорошим индикатором интенсивности использования контроллера домена. При оптимальной структуре службы каталогов метрика должна иметь одинаковое значение для всех контроллеров домена. Увеличение значения метрики указывает на то, что в сети появилось новое приложение, работающее со службой каталогов, или возросло количество клиентских компьютеров.
- **DS Directory Writes/Sec** – число операций записи в каталог *AD* в секунду
- **DS Directory Reads/Sec** – число операций чтения из каталога *AD* в секунду

Произведенные ниже измерения производились на виртуальной машине под управлением Windows Server 2008.

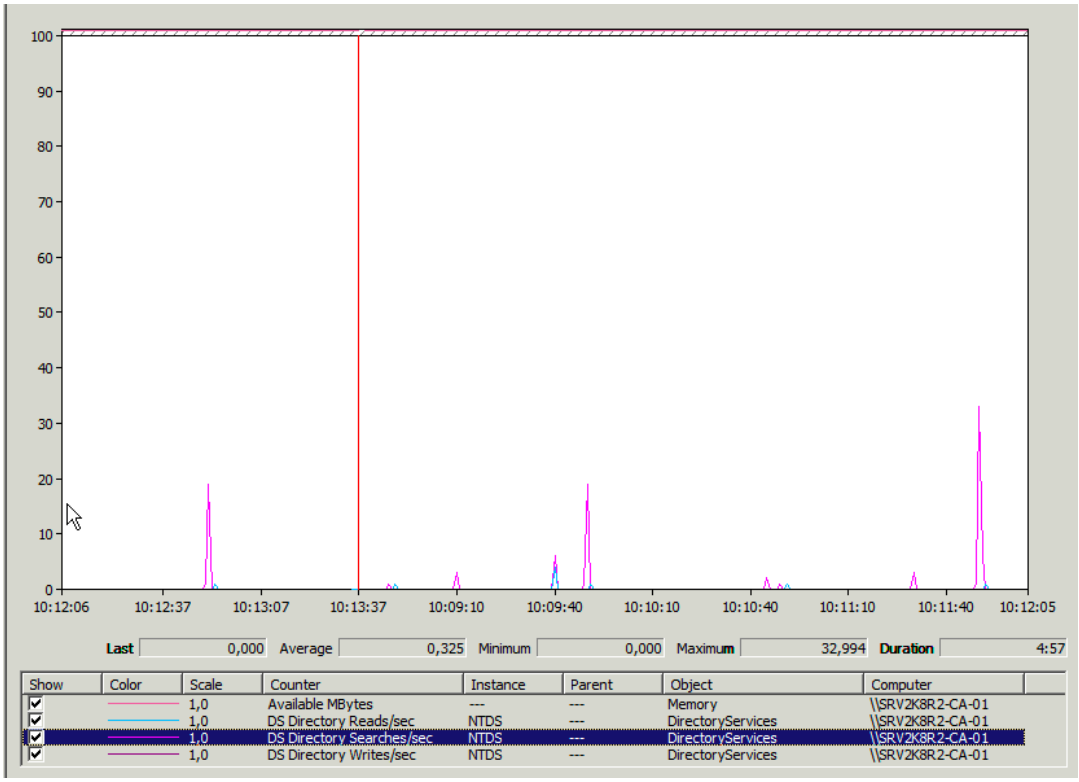

Рис. 11. Состояние сервера, когда синхронизация не запускалась

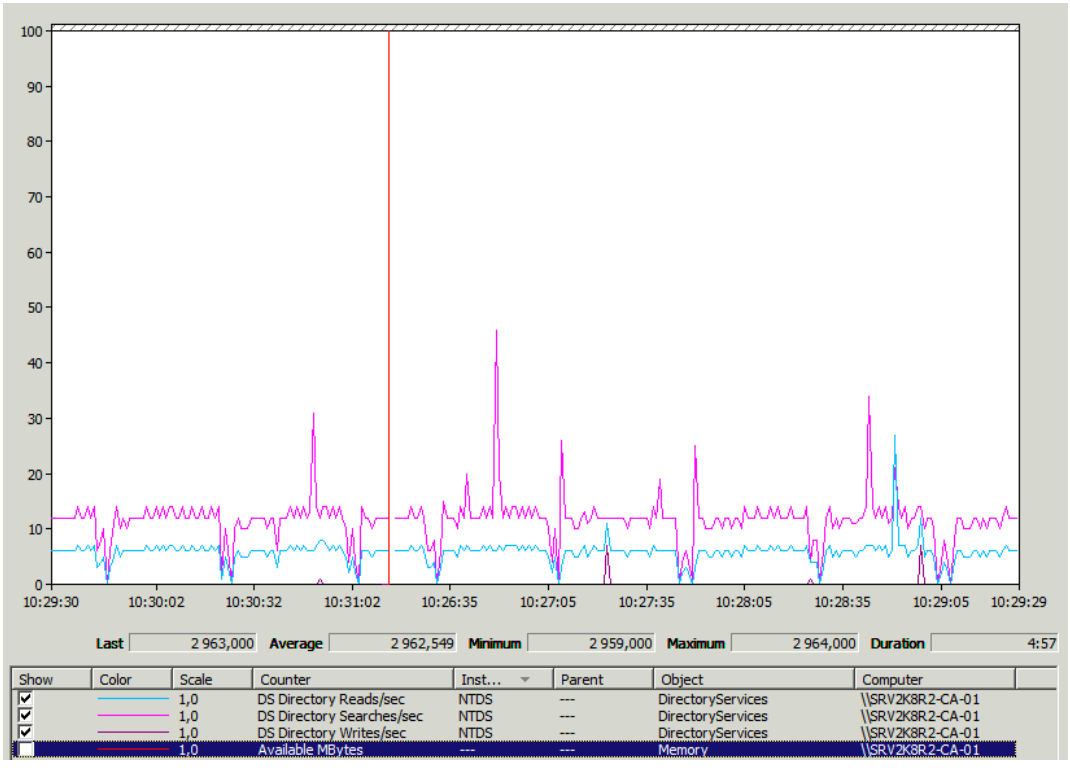

Рис. 12. Состояние сервера при запущенной массовой синхронизации

Как видно, из графика сервер справляется с нагрузкой, отказы не генерируются.

Выводы

Разработанный программный продукт позволяет осуществить мягкую (без существенного изменения существующих ИС) интеграцию систем управления пользователями в критически важных для Университета информационных системах с единой службой аутентификации.

- Интеграция LANBilling и Active Directory с помощью разработанного сервиса приведет к унификации логинов и паролей для учетных записей этих систем;
- Реализована первичная синхронизации по определенному полю (логину, пароле или почту), при этом актуальные данные поля поставляются системой LANBilling и записываются в системе AD;
- Реализована регистрация пользователя системы AD в системе LANBilling, если в ней такового не имеется;
- Реализовано возможность обновления пользователя в обоих системах;
- При большом количестве параметров и независимости их обновления требуется наличие специального поля, отвечающего за синхронизацию каждого из них;
- Состояние этого поля указывает какое поле в действительности синхронизировано, а какое нет;
- Интеграционный сервис написан на языке PHP, используя модуль LDAP для работы с Active Directory и модуль SOAP для работы с LANBilling
- Интерфейс сервиса реализован с помощью технологий CSS & HTML
- Синхронизация по логину - самая затратная операция (26,5 синхронизаций/час);
- Нагрузочное тестирование показало работоспособность решения при ожидаемом уровне нагрузок.

Список литературы

1. Рыбальченко М.А. Разработка единой системы управления пользователями в корпоративных приложениях Университета // Молодежный научно-технический вестник. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 4. Режим доступа: http://sntbul.bmstu.ru/doc/551855.html (дата обращения 18.02.2014);
2. Рыбальченко М. А. Архитектура единой службы аутентификации, авторизации и учета пользователей информационных ресурсов университета // Молодежный научно-технический вестник. МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 1. Режим доступа: http://sntbul.bmstu.ru/doc/681183.html (дата обращения 15.02.2014);
3. Русский TechNet. Режим доступа: http://technet.microsoft.com/ru-ru/library/cc782657(v=ws.10).aspx (дата обращения 20.02.2014);
4. Про LDAP по-русски. Режим доступа: http://pro-ldap.ru/index.html (дата обращения 20.02.2014);
5. Библиотека MSDN. Режим доступа: http://msdn.microsoft.com/library (дата обращения 25.02.2014);
6. Руководство по PHP. Режим доступа: http://www.php.net/manual/ru/index.php (дата обращения 02.02.2014);
7. Практическое использование SOAP в PHP5. Режим доступа: http://phpclub.ru/detail/article/soap (дата обращения 20.02.2014);
8. Документация LANBilling 2.0. Режим доступа: http://www.lanbilling.ru/documentations (дата обращения 20.02.2014);
9. Подразделение JMeter сообщества открытого ПО Apache Foundation Режим доступа: http://jmeter.apache.org/usermanual/index.html (дата обращения 20.02.2014).