

Интеграция со службами каталогов при разработке корпоративных порталов на платформе LAMP

Автор: [Олег Елифантьев](#)

Об авторе: старший программист компании Cetera Labs (www.cetera.ru).
Email: o.elifantiev@cetera.ru

Решаемая бизнес-задача / сфера применения

Веб-разработчики с завидной регулярностью получают заказы на создание корпоративных порталов. Под порталами в данном случае понимаются внутренние сайты предприятий, предоставляющие информацию и сервисы для собственных сотрудников и наиболее близких партнеров.

Подавляющее большинство крупных предприятий уже активно использует единую авторизацию на основе служб каталогов¹, доступ к которым осуществляется по Lightweight Directory Access Protocol (LDAP)².

Совершенно естественно, что заказчики заинтересованы в интеграции разрабатываемого портала со службами каталогов, а разработчикам выгодно использовать внешнюю систему авторизации с точки зрения сокращения объема работ в проекте. И хотя в ряд коробочных продуктов класса "Система управления информацией" встроена интеграция со службами каталогов, разработчикам, тем не менее, приходится решать различные технические и организационные вопросы.

Краткое описание проекта

Проект, который реализовывала наша компания в начале 2008 года, представляет собой функционально насыщенный корпоративный информационный портал холдинга, включающего в себя несколько территориально распределенных компаний. Подразделения холдинга большей частью объединены службой каталогов Microsoft Active Directory (AD)³.

Платформа для реализации проекта: Linux, Apache, PHP, MySQL, Cetera CMS⁴

Основные причины использования авторизации на основе AD в данном проекте:

- Обеспечение единого центра управления пользователями (собственно, AD) для системных администраторов компании.
- Упрощение доступа к portalу сотрудников компании, для которых необходимость ввода лишнего пароля могла стать критической для начала использования portalа.
- Большое количество сотрудников компании (несколько тысяч человек), что делает практически невозможным ввод перечня сотрудников в БД portalа и распределение персонала по дереву компаний и отделов и телефонному справочнику, реализованному в рамках portalа.

Используемые технологии

Две основные задачи - импорт данных из AD и дальнейшая авторизация пользователей, просматривающих страницы portalа. Импорт данных из AD осуществляется через LDAP. LDAP позволяет получить доступ к информации домена - списку пользователей, групп, компьютеров домена и т.д.

Авторизация пользователя производится средствами Apache, а точнее его модуля mod_ntlm (доступен для версий Apache 1.3.x, для 2.2.x используется модуль mod_auth_sspi)⁵. Mod_ntlm авторизует пользователя на этапе обращения к странице, и, если пользователь проходит авторизацию, его данные (имена домена и пользователя) передаются в переменных сервера (для PHP это \$_SERVER)

Описание полей AD

В рамках данного проекта требовалось получить следующую информацию о пользователе из AD:

- полное имя (фамилия, имя, отчество)
- доменное имя
- email
- должность
- принадлежность к компании/отделу (относительно корпоративной структуры заказчика)

Имя пользователя в домене (его логин) хранится в поле SAMAccountName. Title, Department и Company описывают должность, отдел и компанию. Email хранится в поле Mail, полное имя пользователя содержится в поле Name.

Импорт сотрудников

Всякая запись в каталоге LDAP состоит из одного или нескольких атрибутов и обладает уникальным именем (DN — англ. Distinguished Name). Имя может выглядеть, например, следующим образом: «cn=Иван Петров, ou=Сотрудники, dc=example, dc=com». Уникальное имя состоит из одного или нескольких относительных уникальных имен (RDN — англ. Relative Distinguished Name), разделённых запятой. Относительное уникальное имя имеет вид ИмяАтрибута=значение. На одном уровне каталога не может существовать двух записей с одинаковыми относительными уникальными именами. В силу такой структуры имени записи в каталоге LDAP можно легко представить в виде дерева.

Регистрация

Авторизация

В каталоге проекта: 1 370 веб-студий, 115 CMS, 7 529 сайтов.

Для выполнения поиска по структуре службы каталога требуется указать путь к корневому элементу, относительно которого будет осуществлен поиск. Также можно указать фильтр, состоящий из перечисления имен атрибутов записи и их значений в формате ИмяАтрибута=Значение.

Предположим, что требуется осуществить импорт сотрудников домена COMPANY.RU. Для этого путь поиска будет, например, такой:

```
cn=Users, dc=COMPANY, dc=RU
```

cn=Users указывает на т.н. контейнер под название Users.

При выполнении такого поиска без дополнительной фильтрации в результатах могут присутствовать другие элементы помимо самих пользователей. Например, данные о группах. Для получения в результатах поиска лишь данных о пользователях укажем фильтр:

```
ObjectCategory=Person.
```

В некоторых случаях пользователи в AD могут размещаться в т.н. Organizational Units. В таком случае используем путь поиска:

```
ou=Users-and-computers, dc=COMPANY, dc=RU.
```

Такой путь подразумевает, что данные об учетных записях находятся в Organizational Unit под названием Users-and-computers.

В процессе импорта может возникнуть потребность определения активности учетной записи пользователя.

При импорте может быть интересен атрибут учетной записи UserAccountControl ⁶, в котором сохраняются в двоичном виде различные свойства учетной записи. Интересным может быть признак ACCOUNTDISABLE (0x0002). Если данный флаг установлен в атрибуте UserAccountControl, учетная запись считается заблокированной.

Для поиска всех активных пользователей потребуется модифицировать фильтр. Он будет таким:

```
(&(objectcategory=Person)(!(UserAccountControl:1.2.840.113556.1.4.804:=2)))
```

1.2.840.113556.1.4.804 - т.н. OID (Object Identifier), данный OID применяется для отбора объектов, выбранный атрибут которых содержит либо все, либо любой из указанных в фильтре битов. Приведенный выше OID признает совпадение, если в атрибуте присутствует любой из указанных битов. 2 - это значение флага ACCOUNTDISABLE. Данный фильтр целиком можно расшифровать так: Атрибут objectcategory равен Person и в атрибуте UserAccountControl не присутствует бит 2 (0x0002)

Пример кода на PHP

```
<?
/**
 * Данный код подключается к AD и получает список всех незаблокированных сотрудников
 * контейнера Users из домена COMPANY.RU
 * Выводится имя сотрудника, его email, компания, отдел и должность в соответствии с данными,
 * полученными из AD
 */
$ds=ldap_connect("1.2.3.4");
if ($ds) {
    $r=ldap_bind($ds, 'COMPANY\admin', 'adminPassword');
    $sr=ldap_search($ds,
        "cn=Users, dc=COMPANY, dc=RU",
        '(&(objectcategory=Person)(!(UserAccountControl:1.2.840.113556.1.4.804:=2)))');

    echo "Number of entires returned is " . ldap_count_entries($ds, $sr) . "<br />";

    $info = ldap_get_entries($ds, $sr);
    // $info содержит результаты запроса...

    for ($i=0; $i<$info["count"]; $i++) {
        echo "Name: {$info[$i]['name'][0]}<br />\n";
        echo "Email: {$info[$i]['mail'][0]}<br />\n";
        echo "Company: {$info[$i]['company'][0]}<br />\n";
        echo "Department: {$info[$i]['department'][0]}<br />\n";
        echo "Title: {$info[$i]['title'][0]}<br />\n";
    }

    ldap_close($ds);
}
```

```

Регистрация      Авторизация      В каталоге проекта: 1 370 веб-студий, 115 CMS, 7 529 сайтов.
} else {
    echo "Unable to connect to LDAP server";
}
?>

```

Дополнительная информация по работе с LDAP в PHP может быть получена в документации ²

Проблемы и решения

Отсутствие в службе каталогов информации о сотрудниках, достаточной для отображения на портале (полные имена, адреса Email, названия подразделений, хобби, поля корпоративной социальной сети и т.д.).

Почти всегда в службе каталогов не содержится вся информация, необходимая для работы портала. Могут отсутствовать как "банальные" данные, например, номер телефона, так и нетипичные для службы каталогов сведения типа "перечень мест предыдущей работы для нужд корпоративной социальной сети". При этом необходимость этих данных для портала сложно недооценивать.

Нашим решением проблемы является хранение учётных записей в службе каталогов, а расширенной информации - в открытой БД портала. Предполагается, что управление списком и ролями пользователей осуществляется в службе каталогов, а всё остальное - задачи портала.

Недостатком решения является необходимость связывания и синхронизации перечней пользователей в службе каталогов и в БД портала. Важнейшие преимущества:

- предоставление пользователям возможности самостоятельно дополнять информацию о себе в БД портала с последующей модулируемой загрузкой этих сведений в службу каталогов;
- возможность быстро настраивать набор полей в профиле пользователя портала без влияния на работу службы каталогов.

Отсутствие в службе каталогов достоверной информации о принадлежности сотрудника к той или иной компании холдинга или отделу

Стандартом де-факто для корпоративных порталов является отображение дерева компаний холдинга и отделов с автоматической привязкой к дереву сотрудников. При этом часто в службе каталогов сотрудники хранятся единым плоским списком с указанием компаний и отделов в каких-либо свойствах пользователей службы каталогов.

Наше решение:

1. Завести дерево компаний и отделов на портале средствами системы управления контентом, используя данные об организационной структуре, предоставленные заказчиком.
2. Импортировать сотрудников из службы каталогов со сверкой названий элементов дерева, заведенного в БД портала, с содержимым карточек пользователей службы каталогов.
3. Пользователей, для которых определить положение в дереве не удалось, импортировать во временную директорию.
4. По итогам импорта отображать протокол с нотификацией администраторов портала и службы каталогов о недостатках импорта и некачественных записях в службе каталогов.

Выводы

По итогам проекта мы считаем, что:

1. Использование AD и прочих служб каталогов в проектах по разработке корпоративных информационных порталов является оправданным и экономически обусловленным.
2. Заметных технических сложностей в реализации интеграции с AD при использовании технологий, описанных выше, не выявлено.
3. Успешное решение организационных сложностей целиком и полностью зависит от квалификации менеджеров проекта с обеих сторон и системных администраторов заказчика.

Дополнительная информация, источники

¹ http://en.wikipedia.org/wiki/Directory_service

² http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

³ http://ru.wikipedia.org/wiki/Active_Directory

⁴ <http://www.cetera.ru/products/cms/>

⁵ <http://www.gknw.net/development/apache/>

⁶ <http://support.microsoft.com/?kbid=305144>

⁷ <http://ru2.php.net/manual/ru/ref.ldap.php>

→| [посмотреть все статьи этого раздела](#)

Добавить комментарий

→| [авторизоваться](#) или →| [зарегистрироваться](#)

Ваше имя: