Решение задач доступа к ресурсам сайта и снижения нагрузки на сервер

Содержание

Введение

Данные рекомендации предназначены в первую очередь для пользователей, имеющих опыт работы с операционной средой Unix и обладающих достаточными знаниями для применения предложенных решений на сервере.

У вас есть задача: разместить на сервере ряд файлов большого размера и организовать ограниченный доступ пользователей к этим файлам. Однако, при попытке использовать скрипт **download_private.php** происходит перегрузка сервера по объему используемой оперативной памяти, что приводит к неустойчивой работе сервера (даже под управлением двухуровневой системой Front/Back end (NGINX + Apache). Создание же простой HTTP-авторизации является нецелесообразным, поскольку CMS Bitrix позволяет оперативно управлять правами доступа к файлам без использования дополнительных инструментов. Рекомендации, приведенные в данном документе, помогут вам найти верное решение в подобной ситуации.

Задача

Исходные данные

Предполагается, что некоторое количество файлов большого размера будет размещено на сервере. Доступ к этим файлам должен быть предоставлен широкому числу *авторизованных* в системе пользователей (т.е. пользователям, относящимся к определенной группе(ам).

Требования

Необходимо обеспечить приемлемую (низкую) нагрузку на сервер, а также предусмотреть невозможность скачивания файлов по прямой ссылке в обход процедуры авторизации.

Решение

Поставленная задача может быть решена с помощью специального скрипта **download_private.php**, поставляемого с CMS Bitrix.

Однако, узким местом такого решения является то, что весь поток запрашиваемых пользователем данных сначала считывается в память сервера, а только потом отдается пользователю (при этом неважно, выполняется ли запрос через прокси-сервер или напрямую). В результате оказывается занят большой объем памяти, а сервер не обладает безграничным ресурсом памяти!

В результате анализа сложившейся ситуации было принято решение о пересмотре процесса работы скрипта **download_private.php** и его переработке с учетом особенностей прокси-сервера NGINX 0.3.15.

 *Сразу хочу оговориться – я не представляю, каким образом вообще возможен запуск CMS Bitrix без системы Front/Back End. Если Ваш сервер до сих пор не имеет ее, то вы ходите по минному полю.*

Структура HTTP сайта

- **\download\private** - директория для хранения файлов, доступ к которым является ограниченным. Используется для управления правами доступа через File Manager, интегрированный в CMS Bitrix.
- **\public_private** - данная директория содержит обновленный скрипт **download_private.php** и файл перенаправления **.htaccess**, позволяющие генерировать предоставляемые пользователям ссылки-перенаправления на требуемые файлы.

Файловая структура сайта

- **/home/www/** - корневой каталог веб-сайта;
- **/home/www/download/private/** - папка хранения файлов, доступ к которым ограничен;
- **/home/www/denied/** - папка для хранения сообщения, показываемого пользователям в случае использования некорректной ссылки (например, при попытке получить доступ к файлу по прямой ссылке в обход процесса авторизации в системе).

Скрипт download_private.php

```
<?
function initialize_params($url)
{        if (strpos($url,"?")>0)
        {       $par = substr($url,strpos($url,"?")+1,strlen($url));
                $arr = explode("#",$par);
                $par = $arr[0];
                $arr1 = explode("&",$par);
                foreach ($arr1 as $pair)
                {
                        $arr2 = explode("=",$pair);
                        global $$arr2[0];
                        $$arr2[0] = $arr2[1];
```

```
                }
        }
}
// место размещения скрипта
$SELF_SCRIPT_DIR = "\/public_private";
// реальное место размещения файлов с ограниченным доступом
$PRIVATE_DIR = "/download/private ";
// папка для редиректа с защитой от прямого скачивания
$PRIVATE_WWW = "/private_download";

$DIR = dirname($_SERVER["REQUEST_URI"]);

$DIR_ASKED = preg_replace("/^({$SELF_SCRIPT_DIR}\/{0,1})/i","",$DIR);
if (!empty($DIR_ASKED)) $DIR_ASKED = "/" . $DIR_ASKED;

$sapi = php_sapi_name();
set_time_limit(0);
$arr1 = explode("?",$_SERVER["REQUEST_URI"]);
$arr2 = explode("#",$arr1[0]);
$URI = $arr2[0];
$file = str_replace("..", "", $file);
$file = substr($URI, strlen($DIR)+1);
$filename = urldecode($_SERVER["DOCUMENT_ROOT"].$PRIVATE_DIR.$DIR_ASKED."/".$file);

if(file_exists($filename))
{
require_once($_SERVER["DOCUMENT_ROOT"]."/bitrix/modules/main/include/prolog_before.p
hp");
        $FILE_PERM = $APPLICATION-
>GetFileAccessPermission($PRIVATE_DIR.$DIR_ASKED."/".$file, $USER-
>GetUserGroupArray());
        $FILE_PERM = (strlen($FILE_PERM)>0 ? $FILE_PERM : "D");
        if($FILE_PERM<"R")
        {

LocalRedirect($DIR."/auth.php?fname=".urlencode($file)."&DIR=".urlencode($DIR));
        }
        else
        {
                header("X-Accel-Redirect: {$PRIVATE_WWW}{$DIR_ASKED}/{$file}");
                die();
        }
}
else
{        include($_SERVER["DOCUMENT_ROOT"]."/404.php");
} ?>
```

Важно! *Обратите внимание на переменную* ***$SELF_SCRIPT_DIR****. Так как при работе с данной переменной используются регулярные выражения, то символы* ***^$/.[]?{}**** *должны отображаться с использованием обратного слэша, например* ***\?****.*

Комментарий Виталия Каплича, ведущего разработчика компании «Битрикс»:

В приведенном выше примере файла **download_privet.php** описывается вариант работы с переменной **$SELF_SCRIPT_DIR** с использованием регулярных выражений:

```
$SELF_SCRIPT_DIR = "\/public_private";
$DIR_ASKED = preg_replace("/^({$SELF_SCRIPT_DIR}\/{0,1})/i","",$DIR);
```

Однако, в данной ситуации лучше использовать способ, исключающий использование регулярных выражений, что позволит повысить скорость обработки запросов пользователей на доступ к файлам:

```
$SELF_SCRIPT_DIR = "/public_private";
$DIR_ASKED = substr(strtolower($DIR),
strlen(strtolower($SELF_SCRIPT_DIR))-1);
```

Также в файле **download_privet.php**, приведенном в качестве примера, не предусматривается учет событий в модуле Статистики, поэтому нет необходимости в использовании функции **initialize_params**.

Если же события должны учитываться в модуле Статистики, то в текст файла нужно добавить соответствующий код. Пример текста файла с использованием кода, отвечающего за учет событий в модуле Статистики, приводится ниже:

```
<?
function initialize_params($url)
{
        if (strpos($url,"?")>0)
        {
                $par = substr($url,strpos($url,"?")+1,strlen($url));
                $arr = explode("#",$par);
                $par = $arr[0];
                $arr1 = explode("&",$par);
                foreach ($arr1 as $pair)
                {
                        $arr2 = explode("=",$pair);
                        global $$arr2[0];
                        $$arr2[0] = $arr2[1];
                }
        }
}
// место размещения скрипта
$SELF_SCRIPT_DIR = "/public_private";

// реальное место размещения файлов с ограниченым доступом
```

```
$PRIVATE_DIR = "/download/private ";
// папка для редиректа с защитой от прямого скачивания
$PRIVATE_WWW = "/private_download";


$DIR = dirname($_SERVER["REQUEST_URI"]);


$DIR_ASKED = substr(strtolower($DIR), strlen(strtolower($SELF_SCRIPT_DIR))-1);
if (!empty($DIR_ASKED)) $DIR_ASKED = "/" . $DIR_ASKED;


$sapi = php_sapi_name();
set_time_limit(0);
$arr1 = explode("?",$_SERVER["REQUEST_URI"]);
$arr2 = explode("#",$arr1[0]);
$URI = $arr2[0];
$file = str_replace("..", "", $file);
$file = substr($URI, strlen($DIR)+1);
$filename =
urldecode($_SERVER["DOCUMENT_ROOT"].$PRIVATE_DIR.$DIR_ASKED."/".$file);


if(file_exists($filename))
{

require_once($_SERVER["DOCUMENT_ROOT"]."/bitrix/modules/main/include/prolog_before
.php");
        $FILE_PERM = $APPLICATION-
>GetFileAccessPermission($PRIVATE_DIR.$DIR_ASKED."/".$file, $USER-
>GetUserGroupArray());


        $FILE_PERM = (strlen($FILE_PERM)>0 ? $FILE_PERM : "D");
        if($FILE_PERM<"R")
        {

LocalRedirect($DIR."/auth.php?fname=".urlencode($file)."&DIR=".urlencode($DIR));
        }
        else
        {
                        if (CModule::IncludeModule("statistic"))
                        {
                                initialize_params($_SERVER["REQUEST_URI"]);
                                if (strlen($event1)<=0 && strlen($event2)<=0)
                                {
                                        $event1 = "download";
                                        $event2 = "private";
                                        $event3 = $file;
                                }
                                $e = $event1."/".$event2."/".$event3;
```

```
                                if (!in_array($e, $_SESSION["DOWNLOAD_EVENTS"])) //
проверим не скачивался ли в данной сессии
                                {
                                        $w = CStatEvent::GetByEvents($event1,
$event2);
                                        $wr = $w->Fetch();
                                        $z =
CStatEvent::GetEventsByGuest($_SESSION["SESS_GUEST_ID"], $wr["EVENT_ID"], $event3,
21600);
                                        if (!($zr=$z->Fetch())) // проверим не
скачивал ли посетитель за последние 6 часов
                                        {
                                                CStatistic::Set_Event($event1,
$event2, $event3);
                                                $_SESSION["DOWNLOAD_EVENTS"][] = $e;
                                        }
                                }
                        }
                header("X-Accel-Redirect: {$PRIVATE_WWW}{$DIR_ASKED}/{$file}");
                die();
        }
}
else
{
        include($_SERVER["DOCUMENT_ROOT"]."/404.php");
}
?>
```

Файл .htaccess

```
ErrorDocument 404 /public_private/download_private.php
```

Изменения в конфигурации NGINX (nginx.conf)

```
location /download/private/ {
     alias        /home/www/denied/;
}
location /private_download/ {
     alias        /home/www/download/private/;
     internal;
}
```

Описание данных изменений должно быть размещено до определения основного пути к серверу.

Принцип работы

Директива internal в настройках NGINX означает, что данный редирект выполняется только в том случае, если запрос на редирект приходит с локальной машины. В нашем случае эту директиву выполняет сервер Apache, установленный на той же машине, что и NGINX.

При попытке обратиться к файлу **/download/private/file.zip** напрямую будет выполнен редирект в папку **/home/www/denied/**. Так как данная папка не содержит файл **file.zip**, то получим **Ошибку 404**.

Поскольку запрос пришел «извне» (т.е. по прямой ссылке), то директива **alias** выполнена не будет и запрос будет перенаправлен в папку **/home/www/private_download/**, которая также не содержит требуемый файл. В результате получим **Ошибку 404**.

Дополнительные изменения в скрипте download_private.php

Обратите внимание на этот фрагмент скрипта:

```
$DIR_ASKED = preg_replace("/^({$SELF_SCRIPT_DIR}\/{0,1})/i","",$DIR);
if (!empty($DIR_ASKED)) $DIR_ASKED = "/" . $DIR_ASKED;
```

Так как больше нет потребности в создании внутренней папки **/files/**, вы сможете управлять структурой дерева каталогов в соответствии с вашими потребностями. Т.е. структура дерева каталогов для скачивания и хранения файлов с ограниченным доступом может быть любая. Например:

```
/download/private/docs/file.zip
/download/private/audio/file.mp3
…
```

Соответственно, публичные ссылки на файлы должны быть:

```
/public_private/docs/file.zip
/public_private/audio/file.mp3
…
```

Таким образом, вы можете создать единую папку для хранения приватных файлов. Выдача прав на доступ к файлам может осуществляться как с использованием средств CMS Bitrix, так и с помощью вашего собственного скрипта. Запрос на доступ к закрытым файлам обрабатывается сервером так же, как и запрос на показ обычной HTML страницы. Кроме того, событие доступа к закрытым файлам может регистрироваться в модуле **Статистики** системы Bitrix.

Примечания

Некоторые директивы NGINX имеют свойство меняться от версии к версии. Поэтому настоятельно рекомендуется перед внесением изменений в настройки NGINX обратиться к официальной документации по адресу:

http://sysoev.ru/nginx/docs/

Автор статьи и реализация решения: Алексей Штоль, CEO, MediaTwins s.r.o., Чешская Республика.

http://www.mediatwins.com

Автор идеи: Евгений Круглов, компания CIFNet Inc., USA

http://www.cifnet.com