



Dovecot - настройка ACL доступа для IMAP (доступ только на чтение)

Опубликовано muff в Пт, 2016-08-19 18:59



Довольно часто, при работе с почтой, используется протокол **IMAP (Interim Mail Access Protocol)**. Удобность этого протокола заключается в синхронизации, в отличие от протокола **POP3 (Post Office Protocol - Version 3)**.

Однако, если доступ ящику имеет несколько человек (например менеджеры компании), то могут возникнуть проблемы, как случайные, так и умышленные. Самая частая: удаление сообщений на одном клиенте влечёт за собой синхронное удаление на всех активных клиентах (в том числе и на сервере).

Попытаемся избежать возможных неприятностей, если есть вероятность данной ситуации... Отталкиваемся от того, что в качестве **MDA (Mail delivery agent)** используем [Dovecot \[1\]](#). Воспользуемся возможностями плагина **ACL (Access Control Lists)**.

Для подключения плагина необходимо внести изменения в конфигурационный файл **dovecot.conf**. Изменения касаются следующих пунктов файла конфигурации:

- protocol imap
- protocol lda
- plugin

Данные пункты необходимо будет отредактировать до следующего состояния (или дополнить, в случае необходимости):

```
protocol imap {# ?????? ?????????? (?????????? - ???????)mail_plugins = acl imap_acl}
protocol lda {# список плагинов (сепаратор - пробел)mail_plugins = acl}plugin {acl = vfile}
```

Чтобы изменения вступили в силу, необходимо перезапустить **dovecot**:

```
# sh /usr/local/etc/rc.d/dovecot restart
```

Плагин активирован... Следующий шаг - создание **acl** для ящика, права которого необходимо изменить. Для этого необходимо в корневом каталоге этого ящика создать файл **dovecot-acl**. Тоесть, если путь к ящику **/var/exim/domain/user**, то путь к **acl** будет **/var/exim/domain/user/dovecot-acl**.

Синтаксис файла **dovecot-acl** следующий:

```
<identifier> <ACLs> [:<named ACLs>]
```

Тоесть, чтобы разрешить доступ к ящику только на чтение, достаточно создать файл **dovecot-acl** следующего содержания:

```
owner lr
```

Пример многострочного файла **dovecot-acl**:



```
owner lrwstipekxa
anyone lr
```

Чтобы полностью разобраться с данным вопросом, разместим следующую информацию - допустимые значения идентификаторов и допустимые значения флагов.

Таблица идентификаторов

- group-override=group name
- user=user name
- owner
- group=group name
- authenticated
- anyone (или anonymous, что равнозначно anyone)

Таблица флагов

l	lookup	Ящик виден в списке
r	read	Ящик может быть открыт на чтение
w	write	Флаги и ключевые слова сообщения могут быть изменены, за исключением «Просмотрено» и «Удалено»
s	write-seen	Флаг сообщения «Просмотрено» (\Seen) может быть изменён
t	write-deleted	Флаг сообщения «Удалён» (\Deleted) может быть изменён
i	insert	Сообщения могут быть записаны или скопированы в ящик
p	post	Сообщения могут быть размещены через LDA, например через Sieve
e	expunge	Сообщения могут быть исключены
k	create	Ящики могут быть созданы или переименованы под управлением этого ящика (переименование требует прав на удаление)
x	delete	Ящик может быть удалён
a	admin	Административные права на ящик (изменение списков ACL)

Примечание: Кроме файла **dovecot-acl**, в каталоге может находится кэш-файл **dovecot-acl-list**, его нужно удалить после внесения изменений в файле **dovecot-acl**.

Проверяем работоспособность правил... Для ящика разрешен доступ только на чтение. При попытке удалить письмо (используя web-интерфейс **Roundcube**), получаем ошибку:



[2]

Источник (получено 2026-04-05 17:26):

<http://muff.kiev.ua/content/dovecot-nastroika-acl-dostupa-dlya-imap-dostup-tolko-na-chtenie>

Ссылки:

[1] <http://muff.kiev.ua/content/dovecot-vygrebaem-pochtu-iz-pochtovogo-yashchika>

[2] http://muff.kiev.ua/files/imagepicker/1/roundcube_dovecot_acl.png