Визитка

АЛЕКСЕЙ БОГОМОЛОВ, системный администратор (г. Иваново). Технические предпочтения – системы виртуализации и корпоративные коммуникации на базе MS Exchange и SharePoint

Microsoft Exchange 2010

Контроль за действиями администратора

Зачастую обслуживанием сервера занимаются несколько администраторов, и руководителю бывает трудно отследить их действия. Выяснить, кто и какие настройки выполнял на сервере, поможет функция ведения журнала аудита администратора

В сфере ИТ администратор – это тот человек, который обладает полным набором прав по отношению к вверенным ему серверам. Это означает, что он может изменять конфигурацию системы практически не контролируемо. У каждого сервера есть механизмы, позволяющие ограничить возможности рядовых администраторов, но тем не менее в любом случае остается человек, который обладает всей полнотой власти.

Делегирование прав в Microsoft Exchange Server 2010 реализовано на базе механизма Role Based Access Control (RBAC) [1]. В больших организациях RBAC значительно упрощает процесс разграничения полномочий администраторов, но не решает одной серьезной проблемы – контроля над их действиями.

Как быть, когда одни и те же рычаги управления делегированы сразу нескольким лицам? Как выявить администратора, некорректные действия которого привели к остановке сервиса, в том случае, когда никто не хочет брать на себя ответственность? Эти вопросы актуальны для больших и средних компаний, и ранее их решение было непростой задачей.

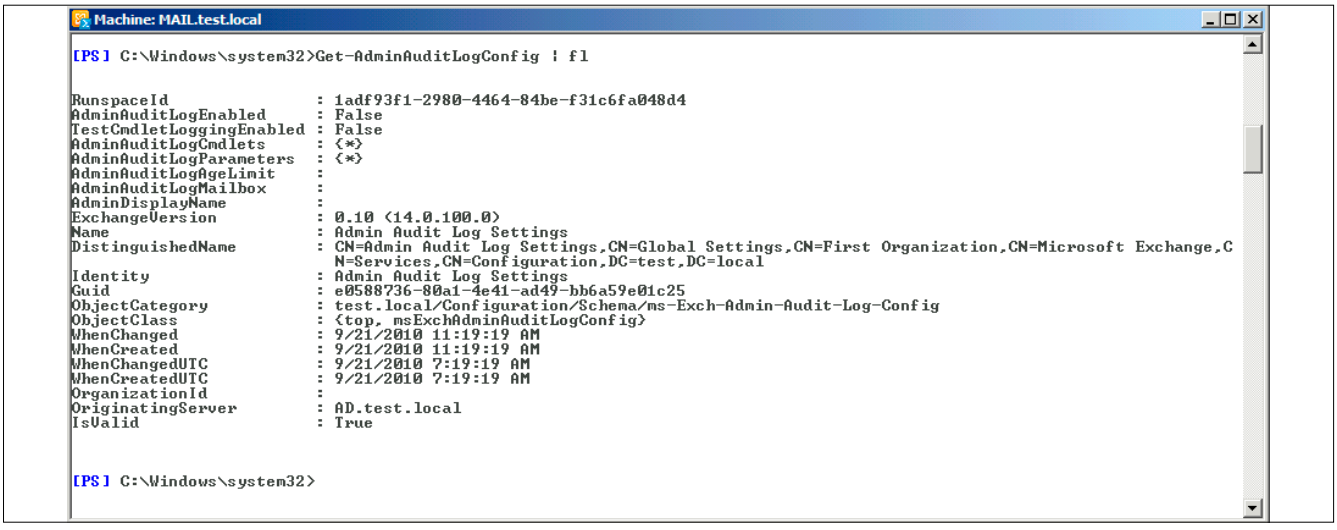
Агенты расширения командлетов

С приходом Microsoft Exchange Server 2010 ситуация значительно изменилась. В эту версию сервера был включен функционал агентов расширения командлетов (Cmdlet Extension Agents) [2].

Агенты расширения командлетов – это компоненты Microsoft Exchange Server 2010, которые активируются в момент выполнения определенного командлета.

Учитывая тот факт, что начиная с версии Microsoft Exchange Server 2007 абсолютно все действия в графической консоли (Exchange Management Console), командной консоли (Exchange Management Shell) либо в панели управления Exchange (Exchange Control Panel), реализуются через запуск определенных командлетов, то это именно

Рисунок 1. Текущие настройки ведения аудита



Ведение журнала аудита поможет администраторам расследовать произошедшие инциденты и выявить виновного

тот функционал, который поможет произвести журналирование (аудит) выполняемых действий.

Примечание: агенты расширения командлетов доступны во всех ролях Microsoft Exchange 2010, кроме роли пограничного транспорта (Edge), и не доступны в любых других продуктах компании Microsoft.

В рассматриваемом Microsoft Exchange 2010 интегрирован ряд агентов расширения, список и состояние активации которых можно получить с помощью командлета Get-CmdletExtentionAgent:

```
Get-CmdletExtentionAgent | ft Name, Priority, Enabled
```

Один из них – Admin Audit Log Agent – реализует функционал ведения аудита действий администратора на серверах Microsoft Exchange 2010.

По умолчанию агент Admin Audit Log Agent включен, однако сам аудит выключен. Активировать функцию журналирования можно командой:

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $True
```

Данная настройка реплицируется на все серверы организации согласно расписанию репликации, следовательно, должно пройти некоторое время до тех пор, пока аудит будет активирован на всех серверах.

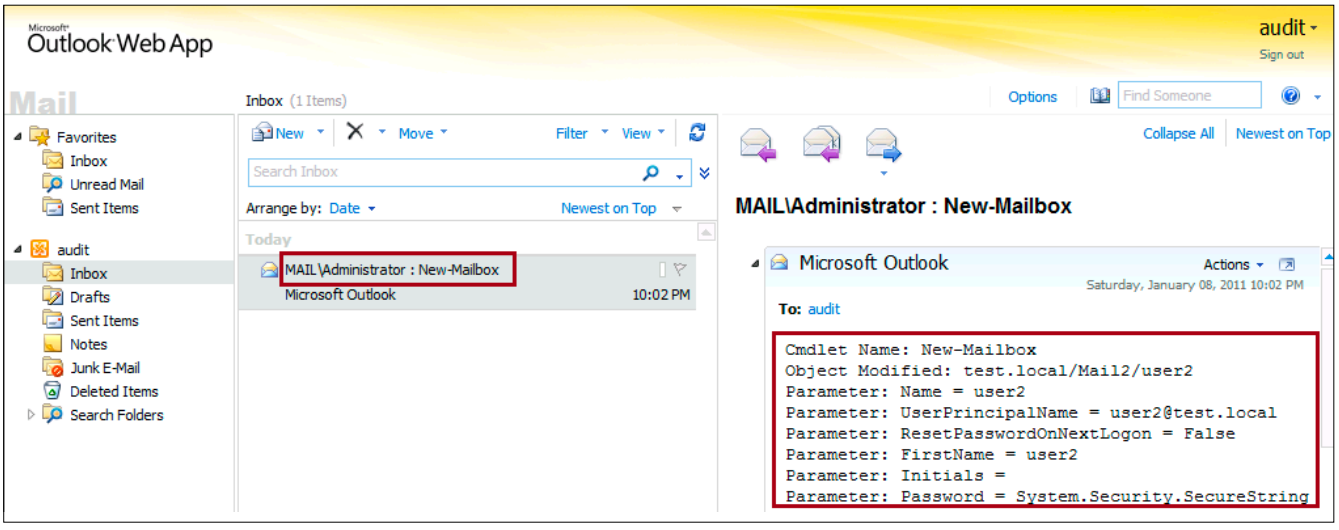
Включение аудита никак не влияет на сам агент Admin Audit Log Agent, соответственно если ранее агент был отключен, то активация только функции ведения журнала аудита администратора не принесет ожидаемого результата. Настройка параметров аудита

После того как функция аудита активирована, необходимо произвести ее настройку. Но для начала следует выяснить текущие параметры.

Вывести текущую конфигурацию нам поможет следующая команда:

```
Get-AdminAuditLogConfig | fl
```

Рисунок 2. Пример записи в ящике для аудита



Из вывода команды видно, что по умолчанию ведение журнала аудита администратора включено для всех командлетов (AdminAuditLogCmdlets) и для всех параметров (AdminAuditLogParameters), т.к. соответствующие значения равны звездочке (*).

Примечание: по умолчанию история использования Get-, Search- и Test-командлетов не сохраняется, поскольку они не выполняют никаких изменений в конфигурации сервера, а лишь производят чтение данных.

Примечание: ведение журнала аудита для Test-командлетов можно активировать командой

```
Set-AdminAuditLogConfig -TestCmdletLoggingEnabled $True
```

По умолчанию журнал аудита содержит много лишней информации, которая затрудняет его анализ. С помощью командлета Set-AdminAuditLogConfig можно указать набор командлетов (AdminAuditLogCmdlets) и параметров (AdminAuditLogParameters), для которых будет вестись аудит. Список командлетов и параметров необходимо перечислить через запятую, а для обозначения набора командлетов допускается использовать в качестве знака подстановки звездочку (*).

Например, для наблюдения только за операциями над почтовыми ящиками пользователей можно задействовать команду:

```
Set-AdminAuditLogConfig -AdminAuditLogCmdlets "*-Mailbox"
```

Хранение данных аудита

После конфигурирования параметров ведения журнала аудита администратора встает вопрос анализа собранных данных.

Функция ведения журнала аудита администратора на серверах Microsoft Exchange 2010 сохраняет записи журнала в специальный почтовый ящик в виде отдельных сообщений. Сообщения имеют заголовок и текстовую часть. В заголовке отображаются имя пользователя и наименование запущенного командлета. В текстовой части содержится подробная информация о работе команды: результат ее выполнения, набор свойств, которые были обработаны, и др. (см. рис. 2).

В Microsoft Exchange Server 2010 RTM администраторы вынуждены вручную создавать этот почтовый ящик на сервере и указывать его в качестве ящика для ведения журнала аудита с помощью следующего командлета Set-AdminAuditLogConfig:

```
Set-AdminAuditLogConfig -AdminAuditLogMailbox ↵
        "audit@test.local"
```

В версии Microsoft Exchange Server 2010 SP1 такая необходимость отпала. Здесь для ведения журнала аудита администратора используется выделенный системный почтовый ящик.

Примечание: важно знать, что в Microsoft Exchange Server 2010 SP1 выделенный системный почтовый ящик невозможно изменять или настраивать.

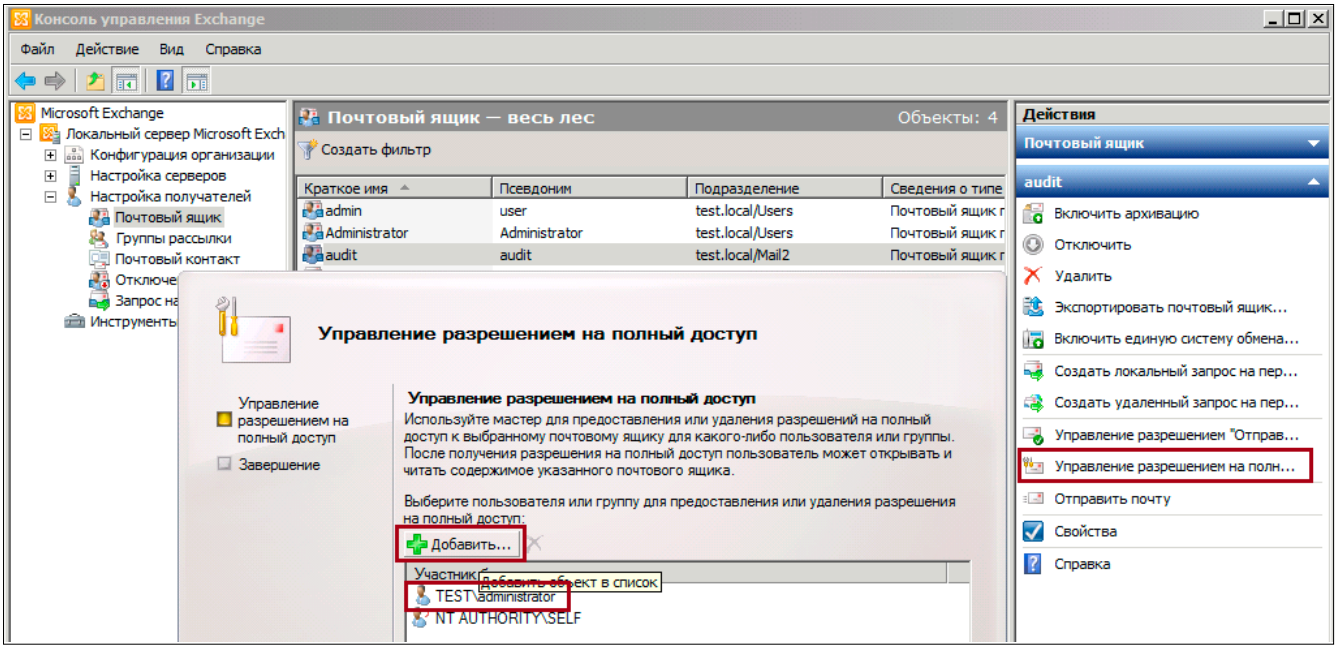
Важным параметром аудита является срок хранения записей. По умолчанию он составляет 90 дней. После истечения указанного периода соответствующие данные из журнала автоматически удаляются.

Срок хранения данных в журнале можно изменить с помощью командлета Set-AdminAuditLogConfig. В приведенном примере значение срока хранения данных увеличивается до полугода (180 дней):

```
Set-AdminAuditLogConfig -AdminAuditLogLimit 180.00:00:00
```

В результате проделанных выше манипуляций попытка выполнения любой команды в организации Exchange приведет к запуску агента расширения командлетов Admin Audit Log Agent, который проверит выполняемые командле-

Рисунок 3. Добавление права доступа к почтовому ящику через EMC



ты и их параметры на предмет наличия в свойствах AdminAuditLogCmdlets и AdminAuditLogParameters. В случае совпадения он сгенерирует сообщение в заданном почтовом ящике, которое будет храниться 180 дней.

Важно заметить, что для аудита используется единственный почтовый ящик. В случае его недоступности попытка запуска командлетов на всех серверах Exchange в организации будет заблокирована. При этом администратор увидит ошибку 5000 от msExchange Management Application с соответствующим текстовым описанием.

Примечание: для дополнительного документирования своих действий администратор искусственно может создать запись в журнале аудита, не выполняя никаких командлетов. Делается это следующим образом:

```
Write-AdminAuditLog -Comment "Любой текстовый комментарий ↵
       длиной до 500 символов"
```

Анализ журналов аудита

Мало настроить ведение журнала аудита администратора, необходимо также научиться его анализировать. Подход к анализу журнала аудита в Microsoft Exchange 2010 для версий RTM и SP1 имеет значительные отличия. Рассмотрим их подробнее.

Анализ журнала аудита в Exchange 2010 RTM

В версии сервера Microsoft Exchange 2010 RTM средств для анализа собранных данных не предусмотрено. Администратор должен предоставить себе право доступа к почтовому ящику, указанному в качестве ящика для ведения журнала аудита, и далее осуществлять поиск в нем, используя стандартные механизмы Microsoft Outlook либо Outlook Web App.

Для предоставления прав доступа к почтовому ящику необходимо воспользоваться графической консолью управления Microsoft Exchange 2010, активировав свойство «Управление разрешением на полный доступ» (см. рис. 3).

Анализ журнала аудита в Exchange 2010 SP1

С выходом первого сервис-пака для Microsoft Exchange 2010 подход к вопросу анализа журнала аудита изменился. Разработчики обеспечили два механизма анализа собранных данных:

- Набор специализированных отчетов, доступ к которым осуществляется через Exchange Control Panel (ECP) (см. рис.4).
- Командлет Search-AdminAuditLog для генерации своих собственных отчетов по средствам PowerShell.

Для создания отчета с помощью консоли управления Exchange (ECP) необходимо:

- открыть нужный шаблон;
- указать диапазон дат для поиска;
- условия поиска;
- запустить процесс генерации отчета;
- после чего просто его открыть.

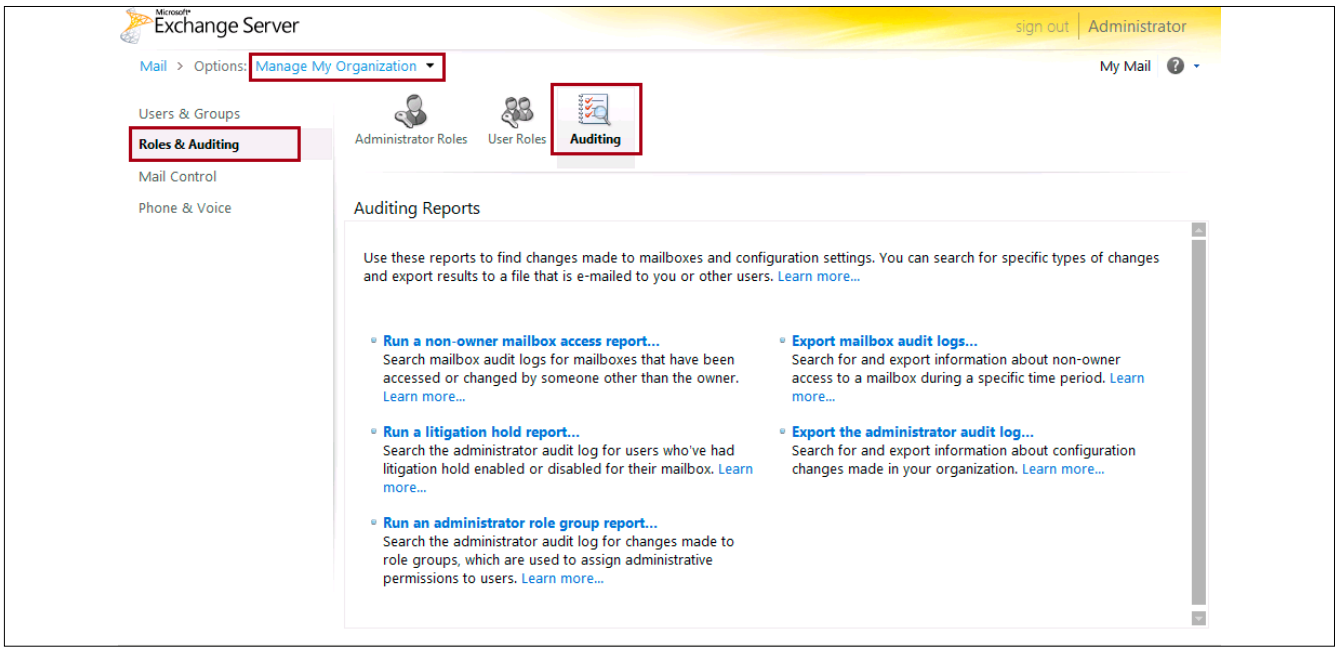
Примечание: для генерации подобных отчетов используется командлет Search-AdminAuditLog, работу с которым мы разберем немного подробнее далее.

Зачастую бывает недостаточно шаблонов, предложенных разработчиками. В такой ситуации вам сможет помочь командная консоль управления Exchange (EMS), в которой с помощью командлета Search-AdminAuditLog вы сможете реализовать практически любую необходимую логику. Подробное описание командлета Search-AdminAuditLog и его параметров можно найти в библиотеке TechNet пройдя по ссылке [3].

Давайте рассмотрим несколько практических примеров (см рис. 5).

Пример 1. Получение списка всех успешных действий, выполненных определенным пользователем.

Рисунок 4. Отчеты, доступные через ECP



```
Search-AdminAuditLog -UserIds Administrator -IsSuccess ↵
        $True | FT RunDate, Caller, CmdletName
```

Примечание: можно указать нескольких пользователей, перечислив их через запятую в параметре -UserIds.

Пример 2. Выполнить поиск администраторов, которые создавали почтовые ящики пользователей в диапазоне дат 01.01.2011 – 30.01.2011. Показать, какие почтовые ящики были созданы.

```
Search-AdminAuditLog -Cmdlets New-Mailbox ↵
        -StartDate 01/01/2011 -EndDate 01/30/2011 ↵
        -IsSuccess $true
```

Пример 3. Показать все командлеты, выполненные на сервере. Отсортировать в алфавитном порядке.

```
Search-AdminAuditLog | Sort CmdletName | ↵
        Group CmdletName | FT Count, Name -AutoSize
```

Созданные подобным образом отчеты достаточно информативны для администратора, но мало полезны с точки зрения руководителя.

Отчет будет выглядеть наглядно, если его представить руководителю в HTML-формате [4]. При этом к отчету можно будет применить различное текстовое форматирование и цветовые шаблоны.

Кроме этого, существует возможность автоматически отправить отчет по электронной почте, для чего используется командлет New-AdminAuditLogSearch.

Командлет New-AdminAuditLogSearch выполняет поиск в журнале аудита подобно командлету Search-AdminAuditLog.

Однако вместо вывода результатов поиска в командную консоль командлет New-AdminAuditLogSearch отправляет результаты поиска по электронной почте указанному получателю.

Результаты поиска включаются в сообщение электронной почты в качестве XML-вложения. Подробнее о его использовании прочитайте в библиотеке TechNet [5].

***

Ведение журнала аудита поможет администраторам сервера Microsoft Exchange 2010 расследовать произошедшие инциденты и выявить виновного. Однако это не означает, что журналирование поможет избежать ошибочных действий администраторов.

Гораздо правильнее будет грамотно настроить политику делегирования прав с учетом того, чтобы серьезные настройки мог выполнять только высококвалифицированный персонал. EOF

1. Role Based Access Control (RBAC) – новая модель управления доступом к Exchange 2010 – http://www.alexxhost.ru/2010/04/role-based-access-control-rbac-exchange.html.
2. Богомолов А. Microsoft Exchange 2010. Упрощаем обслуживание с помощью агентов сценариев. //«Системный администратор», №1-2, 2011 г. – С. 51-53.
3. Описание командлета Search-AdminAuditLog в Microsoft TechNet – http://technet.microsoft.com/ru-ru/library/ff459250.aspx.
4. HTML-отчеты в Exchange 2010 – http://www.alexxhost.ru/2010/12/html-exchange-2010.html.
5. Описание командлета New-AdminAuditLogSearch в Microsoft TechNet – http://technet.microsoft.com/en-us/library/ff459243.aspx.

Рисунок 5. Иллюстрация генерации отчетов в EMS