Работа со списками контроля доступа

В наш век высоких мощностей и быстрого развития Интернета несложно заметить, что, чем дальше, тем больше пользователи компьютеров начинают заботиться о безопасности и сохранности своих данных.

Пока на персональных компьютерах преобладала DOS, защита файлов сводилась к банальной установке пароля в BIOS на загрузку системы. Теперь все стало по-другому. На одном компьютере может работать зачастую 10 человек, а если к нему подключена сеть — то и сотни, а иногда и тысячи пользователей. Защитить данные в такой агрессивной среде средствами самой ОС — задача не простая, но вполне решаемая, если суметь грамотно настроить правила доступа пользователей к файлам. Именно для раздачи соответствующих прав доступа и была создана подсистема ACL, или Access Control Lists.

Исторически так сложилось, что во всех существующих операционных системах присутствует некоторая привилегированная группа администраторов. В Windows, например, она так и называется «Администраторы». В Unix- и Linux-системах данная группа носит имя «wheel». На рисунке вы можете видеть типичный пример групп и распределения пользователей в них. Как можно заметить на том же рисунке, изначально у нас есть три группы: «Администраторы», «Пользователи» и «Бухгалтеры». В первую группу входят весьма опытные и ответственные пользователи, умеющие обращаться с системой. »

» Во вторую попали те люди, которым необходима работа с электронной почтой, файловыми архивами и Microsoft Office. В третью группу мы определили всех бухгалтеров, которым по роду деятельности ежедневно необходимы программы семейства «1С:Предприятие», возможность доступа к материалам с данными о доходах и другим секретным документам компании. Каждый пользователь нашей системы кроме имени и принадлежности к группе обязательно должен иметь еще один атрибут — пароль. Помните, что сочетание пользователь/пароль всегда уникально, и создать на одном компьютере двух одинаковых пользователей невозможно.

Необходимые пояснения

Со всеми необходимыми для дальнейшей работы терминами мы разобрались, теперь можно переходить к основной теме нашей статьи — непосредственной работе с системой ACL, или, говоря по-русски, со списками контроля доступа. Как всем хорошо известно, с тех пор как персональные компьютеры стали действительно персональными, прошло всего 20 лет. Теперь в памяти машин часто содержатся весьма важные, а зачастую и совершенно секретные документы, доступ к которым может и должен быть ограничен. Именно по этой причине и стали появляться различные вариации систем контроля доступа пользователей.

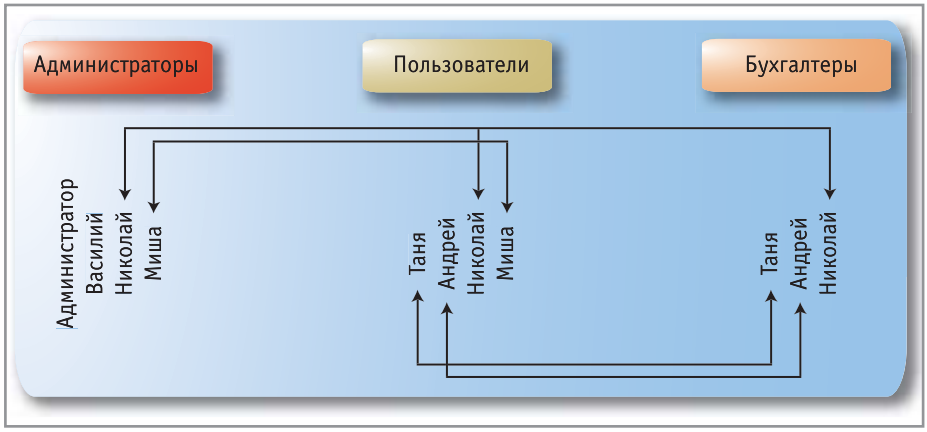
Рассмотрим систему работы ACL, взяв в качестве примера Windows 2000 (впрочем, нам подойдет любая версия Windows класса NT, то есть NT3, NT4, 2000, XP, 2003), установленную на файловую систему NTFS. У каждого файла или каталога на этой файловой системе есть так называемые права доступа (Access Rights). Разные операционные системы могут предоставлять различные параметры доступа к файлам. Например, в Windows 2000 по умолчанию существуют три параметра: разрешение на чтение, разрешение на запись и разрешение на запуск. Все остальные параметры представляют собой лишь различные комбинации трех предыдущих. Например, разрешение на модификацию файла — это сочетание разрешения на чтение и на запись. Разрешение на полный доступ — все три базовых составляющих вместе. В более сложных операционных системах, таких как Novell Netware или Linux, каждый файл закреплен за какими-либо конкретными пользователями и группами, так называемыми «owners» и «groups».

Подобная система разделения прав доступа впервые появилась в операционной системе Novell Netware. Компания-разработчик Novel даже сумела убедить институт стандартов, что данную систему контроля доступа необходимо включить в официальный международный стандарт POSIX. Именно поэтому теперь она носит гордое название POSIX ACL и поддерживается во всех POSIX-совместимых операционных системах, таких как Windows NT, Linux, FreeBSD, IRIX и, конечно же, во всех системах самой Novell.

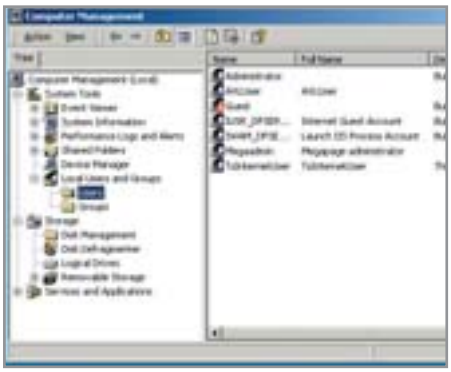
Назначение прав доступа

Проще всего рассматривать систему назначения прав доступа на какомлибо конкретном примере. Давайте попробуем смоделировать следующую ситуацию: на одном из серверов работают по очереди или одновременно (через службу терминального доступа) пять человек. Задачу можно сформулировать примерно так: двое пользователей (Таня и Ольга) должны иметь возможность работать с программой «1С:Предприятие», четверо (Таня, Андрей, Николай и Михаил) работают с различными документами MS Word, которые находятся в специальной папке C:\SharedDocs. Один человек (Константин) имеет полный доступ ко всем документам на диске, и никто кроме него не может обращаться к папке C:\TopSecret, в которой хранятся данные по зарплатам всех сотрудников компании.

Один из важнейших элементов при использовании ACL — правильное создание группы. В нашем случае оптимально будет использовать группы «Бухгалтеры», «Офис» и «Начальники». »



▲ Схема распределения пользователей по группам



▲ Начальный список пользователей нашей системы

▲ Добавление новых пользователей в существующую группу

▲ Назначение прав доступа для пользователя «Everyone»

» После детального рассмотрения становится совершенно ясно, что члены группы «Начальники» должны иметь полный доступ ко всем ресурсам, то есть по своим возможностям совершенно аналогичны группе «Администраторы». Соответственно, останется создать лишь две новые группы. План готов, приступим к его реализации:

- Нажмем правой клавишей мыши на иконке «My Computer» и выберем «Manage → Computer Management → Local Users and Groups».
- Открыв ветвь «Users», добавим в нее всех пятерых пользователей.
- Затем в ветвь «Groups» добавим две новые группы — «Бухгалтеры» и «Офис».
- Двойным щелчком откроем группу «Бухгалтеры» и с помощью появившегося диалогового окна добавим в нее пользователей «Таня» и «Ольга».
- Теперь откроем группу «Офис» и добавим в нее пользователей «Таня», «Андрей», «Николай» и «Михаил». Заметьте, что пользователь «Таня» фигурирует в обеих группах. Это совершенно нормально, один пользователь может состоять в 16 разных группах.
- Откроем группу «Администраторы» и внесем в нее Константина.

На этом предварительная подготовка закончена, можно приступить к раздаче прав пользователей.

Перейдем в папку, где установлена программа 1С, в нашем случае это C:\Program Files, и, нажав правой кнопкой на папке 1С, перейдем на закладку «Security». Щелкнув по кнопке «Add», добавим в фильтр группу «Бухгалтеры» и группу «Everyone». Последняя группа нужна для того, чтобы иметь возможность запретить всем кроме бухгалтеров обращаться к данным в папке. Нажав на группу «Everyone», щелкните на галочке «Full Control» в колонке «Deny». Таким образом вы закроете доступ к этой папке для любого пользователя, кроме тех, которые состоят в группах «Администраторы». Теперь, щелкнув на группе «Бухгалтеры», дадим им полный доступ к этому каталогу, нажав на галочку «Full Control» в колонке «Allow». Теперь никто кроме членов группы «Администраторы» или «Бухгалтеры» не сможет обращаться к файлам в каталоге C:\Program Files\1C, что нам и требовалось реализовать.

Осталось повторить подобную операцию над папками C:\SharedDocs и C:\TopSecret, запретив доступ к ним для всех пользователей. Аналогично предыдущему действию укажите, что группа «Офис» имеет полный доступ к папке C:\SharedDocs. Отметьте для себя, что мы не назначаем прав доступа на папку C:\TopSecret, потому что пользователь «Константин» состоит в группе «Администраторы» и поэтому имеет доступ ко всем файлам на диске.

Наследование правил доступа

Системы ACL для каталогов и файлов существенным образом отличаются. Дело в том, что для каталогов введена отдельная категория, называемая Default ACLs, то есть списки контроля доступа по умолчанию. Эта система позволяет неявно указать ACL для вновь создаваемых в каталоге файлов. Если представить себе файловую систему в виде дерева, где в качестве корня каталог C:\, то можно объяснить систему списков по умолчанию примерно так: «Назначенный на ветку список по умолчанию наследуется всеми ветками и листьями этой ветки, кроме случаев, когда пользо- »

Немного теории

Принцип работы современных ОС

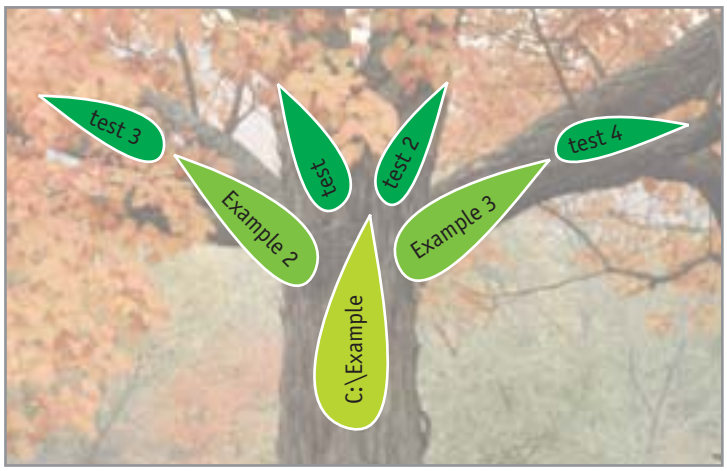
Все современные многозадачные операционные системы стоят на трех китах — процессах, файлах и пользователях. Объяснить их значение человеку, не сведущему в высоких технологиях, можно примерно так: процессы — это выполняемые системой программы, файлы — упорядоченная совокупность данных, содержащаяся на диске или в памяти, а пользователи — обычные люди, которые работают на данном компьютере.

Строго говоря, дать определение слову «пользователь» в компьютерном его понимании довольно сложно. Если провести аналогию между компьютером и реальной жизнью, то окажется, что операционная система считает пользователем не человека, а его паспорт, так называемую «учетную запись». Кроме реальных пользователей в системе существуют некоторые специальные учетные записи, от имени которых, например, могут работать некоторые системные сервисы. Однако компьютером они воспринимаются так же, как и реальные люди. Как и в жизни, в операционных системах существует некоторая структура, позволяющая объединять пользователей (точнее, их учетные записи) в группы. Деление на группы позволяет удобно и своевременно определять права на доступ сразу для большого количества пользователей.

» ватель переназначил список по умолчанию для подветки». То есть список доступа по умолчанию наследуется всеми файлами в этом каталоге, а также во всех его подкаталогах.

Для примера — создадим каталог C:\Example. Внутрь этого каталога поместим файлы test1 и test2 и каталоги Example2 и Example3. Внутрь последних добавим еще по одному файлу — test3 и test4. Получим примерно такое дерево, как вы видите на рисунке. Для проверки создадим еще одного пользователя, например «Полуэкт». Теперь попробуем изменить права доступа для каталога C:\Example. Как видите, сделать это не так-то просто — дело в том, что на сам корневой каталог C:\ после инсталляции системы установлены разрешающие права по умолчанию для группы «Everyone». Чтобы избавиться от этого неудобства, в нашем случае достаточно снять галочку «Allow inheritable permissions from parent propogate to this object», то есть указать системе, что этот каталог не наследует от предка (каталога C:\) права по умолчанию. Теперь запретим пользователям «Everyone» (то есть всем пользователям системы) записывать в этот каталог, сняв галочку «Write» в ряду «Allow». Обратите внимание, что права на каталоги Example2 и Example3 изменились соответственно, то есть были унаследованы от каталога Example. Это очень удобное свойство, но пользоваться им надо крайне аккуратно. Ведь если запретить для всех запись в каталог C:\, то с большой вероятностью операционная система перестанет работать адекватно. Самый известный пример — запретить чтение файлов из системного каталога «Fonts», после чего Windows приходит в состояние полной неработоспособности. Оно и понятно, ведь результатом этого является ситуация, когда пользователь «System», от имени которого происходит обработка шрифтов, не в состоянии прочитать ни одного системного шрифта.

Но вернемся к нашим экспериментам с каталогами. Представим реальную задачу — разрешить пользователю «Полуэкт» записывать данные только в файл test2. Для этого нам придется наложить поверх правил, которые файл унаследует от родительского каталога,



Так называемая «древовидная» схема представления каталогов, в которой каждый каталог может выглядеть в виде ветки

еще одно правило. Добавив пользователя «Полуэкт», разрешите ему полный доступ к файлу через пункт «Full Control» в колонке «Allow». Это было легко, не правда ли?

Чуть более сложная задача — разрешить нашему пользователю создавать новые файлы в каталоге Example3, но запретить записывать в находящийся в этом каталоге файл test4. Сделать это можно следующим образом: разрешим каталогу Example3 наследовать свойства от родительского каталога, но добавим еще одно правило: пользователю «Полуэкт» разрешим полный доступ к этому каталогу. Однако файл test4 вместе с остальным содержимым каталога Example3 по-прежнему доступен для записи. Чтобы избежать этого, снимите галочку «Allow inheritable permissions from parent propogate to this object» и назначьте новые права на файл — всем пользователям нужно разрешить читать этот файл, но запретить запись в него.

Итог

Как видите, все достаточно просто, и надо лишь немного потренироваться, чтобы не запутаться в схеме работы ACL. Однако простота может быть обманчивой, ведь мы рассматривали лишь небольшие системы каталогов, не более чем из 5–10 элементов. Попробуйте представить, каких объемов достигает суммарный список доступа на дисковой системе с 10–20 тысячами правил и насколько сложно ими управлять.

Возможно, что когда-то, в далеком будущем, на смену системе ACL придет что-то новое, так же как устаревшую систему Unix ACL постепенно вытеснила современная реализация POSIX ACL. Но пока что можно с уверенностью сказать: нынешняя система контроля доступа к ресурсам позволяет сделать все, что необходимо системному администратору для обеспечения защиты файлов и каталогов. Мы рассмотрели лишь базовые операции, не углубляясь в подробности и не распространяя внимание на такие аспекты, как мандатный доступ к файлам, разделение прав системного администратора и специалиста по безопасности, потому что все это уже не столь важно. Главное — помнить, что использование правильно назначенных списков доступа, щедро приправленных антивирусом, системой резервного копирования и обильно политых здравым смыслом, убережет вас от потери и утечки любых данных. ■ ■ ■ **Григорий Бакунов**

Это важно знать

Работа ACL в Linux

В современных дистрибутивах Linux настройка правил ACL не сложнее, чем в Windows. Файловые менеджеры Nautilus и Konqueror прекрасно справляются с установкой прав доступа к файлам и каталогам, однако надо учитывать, что Linux по умолчанию использует более старую и более простую систему ACL — так называемую Unix ACL.

В ней, как и в Netware, каждый файл и каталог имеет своего владельца, а права на доступ разбиты на три части: доступ для пользователя-владельца, доступ для группы-владельца и доступ для остальных пользователей. Эта система более сложна в использовании, и при переходе с Windows некоторые администраторы испытывают легкий дискомфорт.