Application Pool Identities в IIS

windowsnotes.ru/iis/application-pool-identities-v-iis

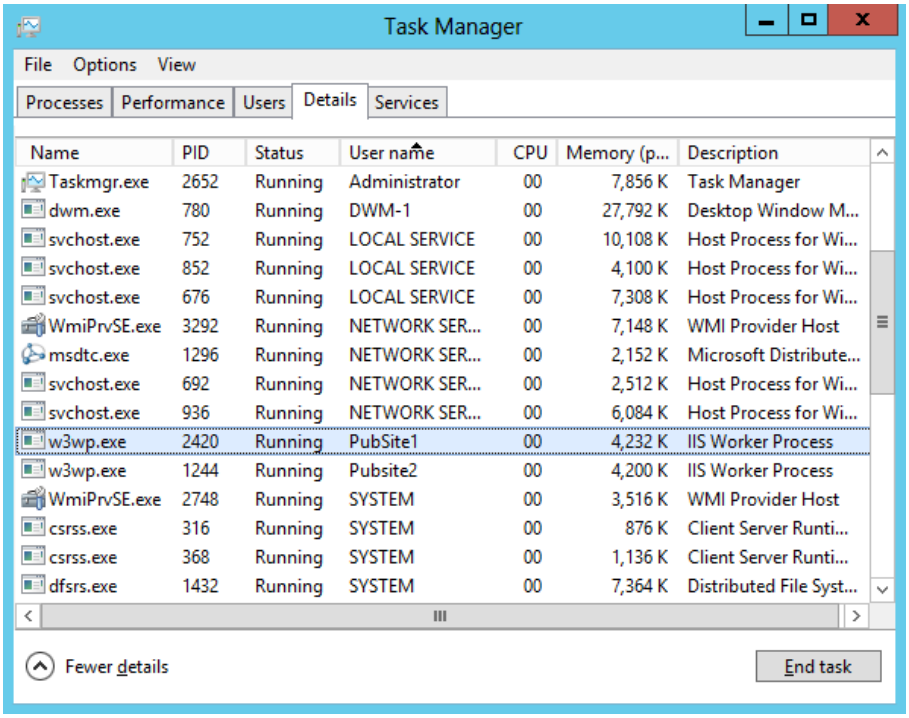
5 июля 2013 г.

Каждый пул приложений в IIS использует свой собственный рабочий процесс (IIS Worker Process). Удостоверение пула приложений (Application Pool Identities) представляет из себя имя учетной записи, под которой выполняется рабочий процесс этого пула.

В IIS 6.0 и IIS 7.0 пул приложений по умолчанию работал под встроенной системной учетной записью **NetworkService**. Эта запись не требует пароля и имеет на локальном компьютере ограниченные права, что является хорошей практикой с точки зрения безопасности. Однако под этой учетной записью могут одновременно работать разные системные службы Windows, и при использовании одного и того же идентификатора одни службы могут воздействовать на работу других.

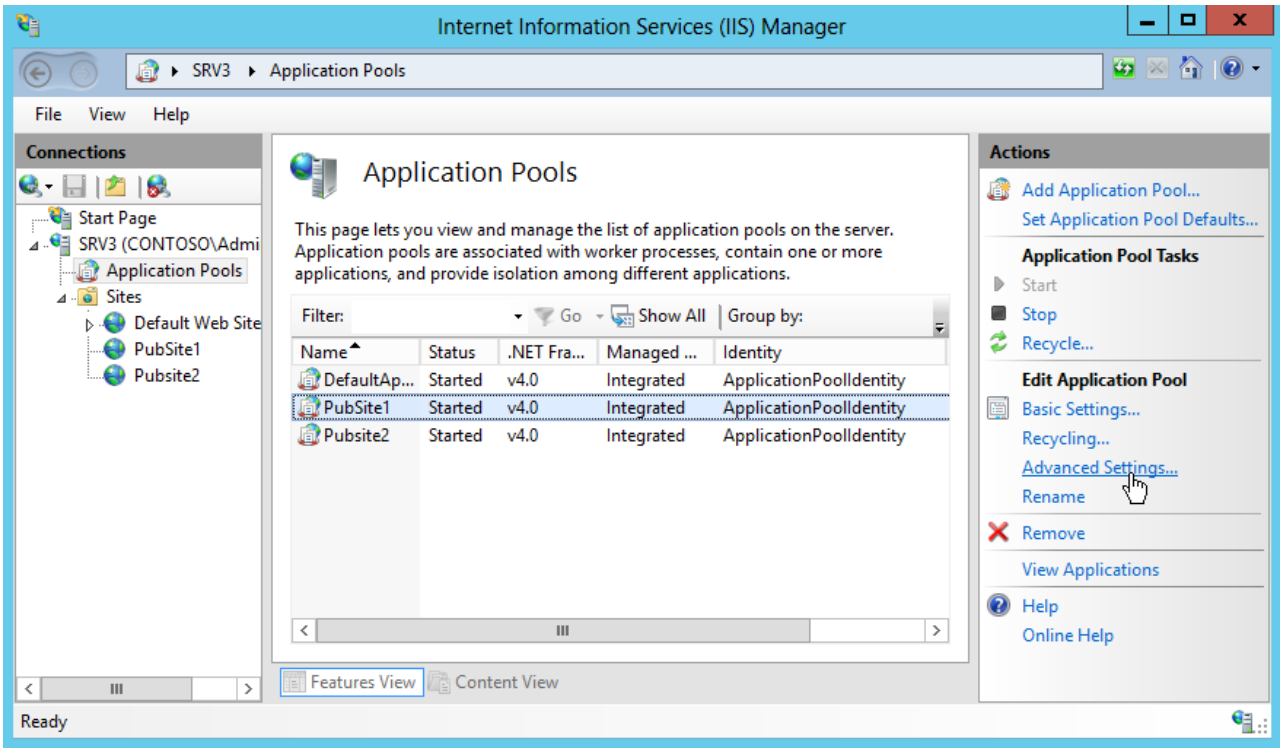
Начиная с Windows Server 2008 SP2 для того, чтобы изолировать рабочие процессы IIS от других системных служб, можно использовать виртуальные учетные записи (Virtual Accounts). Они позволяют запускать рабочий процесс для каждого пула приложений под собственной уникальной учетной записью **ApplicationPoolIdentity**. Эта учетная запись не требует управления и создается автоматически при создании каждого нового пула. Также она не имеет практически никаких привилегий в системе и не использует профиль пользователя, что повышает безопасность веб-сервера.

Для примера возьмем Application Pool с именем PubSite1. Открываем Task Manager и находим рабочий процесс IIS (w3wp.exe), выполняющийся от имени PubSite1. Как видите, имя учетной записи совпадает с именем пула приложений. Дело в том, что начиная с IIS 7.5 для каждого вновь созданного пула приложений по умолчанию создается виртуальная учетная запись с именем этого пула, и его рабочий процесс запускается из под этой записи.



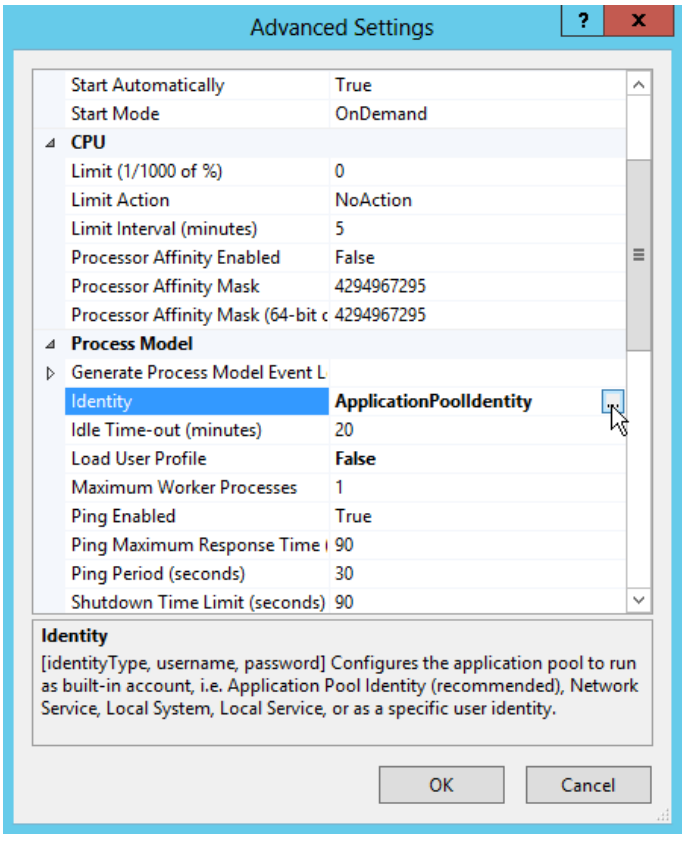
Настройка типа удостоверения пула приложений

При необходимости тип идентификации пула приложений можно изменить. Для этого запускаем IIS Manager, переходим в раздел Application Pools, выбираем нужный пул и открываем его свойства (Advanced Settings).



В свойствах выбираем пункт Identity.

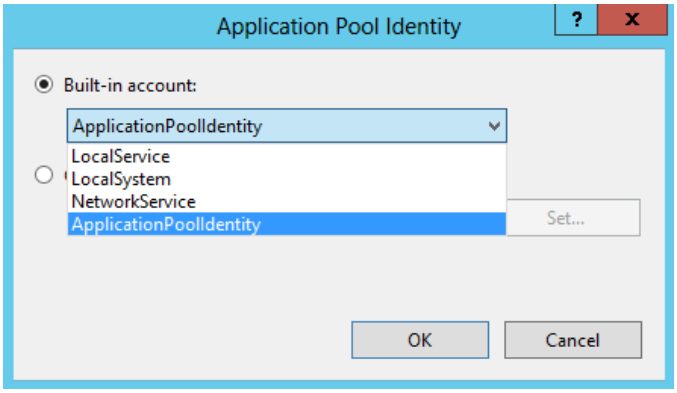
Здесь мы указываем учетную запись, от имени которой будет работать данный пул приложений:



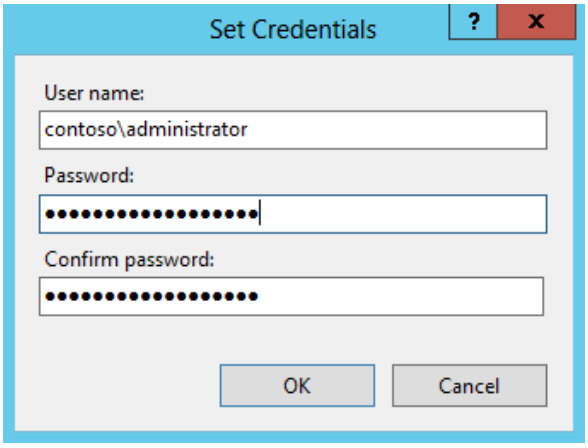
• ApplicationPoolIdentity — учетная запись удостоверения пула приложений. Создается автоматически при запуске пула приложений и имеет самые минимальные права на локальном компьютере. Это наиболее безопасный вариант, начиная с IIS 7.5 используется по умолчанию;
• LocalService – встроенная учетная запись, которая имеет ограниченные права на локальном компьютере. Примерно то же самое, что и NetworkService, но ограничена только локальным компьютером;
• LocalSystem – системная учетная запись, имеющая неограниченные права на локальном компьютере. Наименее безопасный вариант, по

возможности не рекомендуется ее использовать;
• NetworkService — учетная запись, которая имеет ограниченные права на локальном компьютере, а также может использоваться для доступа к ресурсам в сети Active Directory на основании учетной записи компьютера.

Кроме того, в качестве удостоверения можно использовать и обычную учетную запись пользователя. Для этого надо выбрать Custom Account, нажать кнопку Set и ввести имя пользователя и пароль. Можно указать любого доменного или локального пользователя.



Примечание. При использовании учетной записи пользователя надо отслеживать срок действия пароля и своевременно менять его.



То же самое можно сделать с помощью утилиты командной строки **appcmd.** Чтобы указать учетную запись, которая будет использоваться для пула приложений, используется следующий синтаксис:

appcmd set config /section:applicationpools /[name="имя пула приложений"].processModel.identityType:SpecificUser|NetworkService|LocalService|LocalSystem

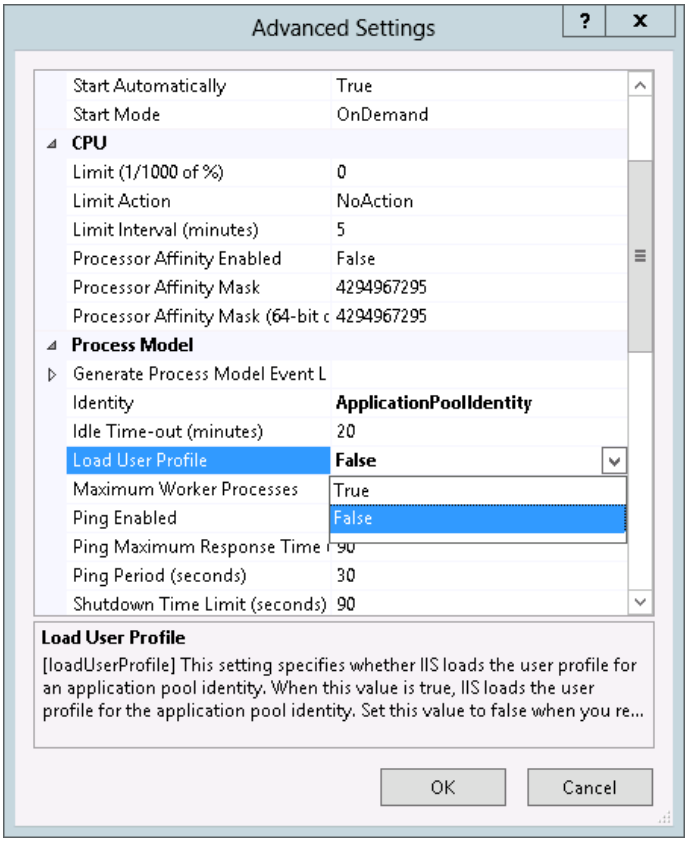
Для примера изменим тип удостоверения для пула приложений PubSite1 на NetworkService:

appcmd set config /section:applicationpools /[name="PubSite1"].processModel.identityType:NetworkService

Профиль пользователя

По умолчанию IIS не использует профиль пользователя, но некоторые приложения могут потребовать использование профиля, например для хранения временных файлов. Профиль для учетной записи NetworkService создается системой и всегда доступен. Стандартные пулы приложений (DefaultAppPool, Classic .NET AppPool и т.п.) также имеют профиль пользователя на диске, однако при использовании ApplicationPoolIdentity профиль не создается автоматически.

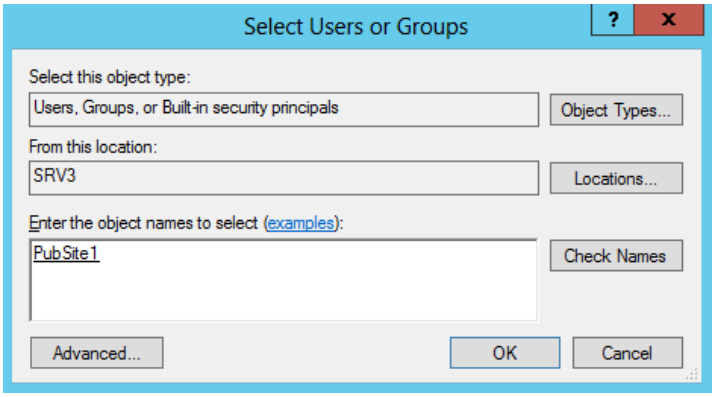
Если вы хотите настроить ApplicationPoolIdentity на использование пользовательского профиля, то надо зайти в расширенные свойства пула и перевести параметр **Load User Profile** в состояние **True**.



Настройка доступа к ресурсам

Иногда веб-приложению может потребоваться доступ к определенной папке или файлу на диске. Чтобы добавить ApplicationPoolIdentity в Access Control List (ACL):

• Запускаем Windows Explorer;
• Выбираем нужный файл или директорию, кликаем по ней правой клавишей мыши и выбираем пункт Свойства (Properties);
• Переходим на вкладку Безопасность (Security),
• Кликаем по кнопке Изменить (Edit), затем Добавить (Add);
• В поле Размещение (Locations) выбираем локальную машину;
• Вводим имя пользователя в виде **"IIS AppPool\имя пула приложений"**. Так для пула приложений PubSite1 имя пользователя будет выглядеть **"IIS AppPool\PubSite1"**;
• Проверяем имя клавишей Проверить имена (Check Names) и жмем OK.



Также при желании можно воспользоваться утилитой командной строки ICACLS. Для примера дадим права на изменение для PubSite1:

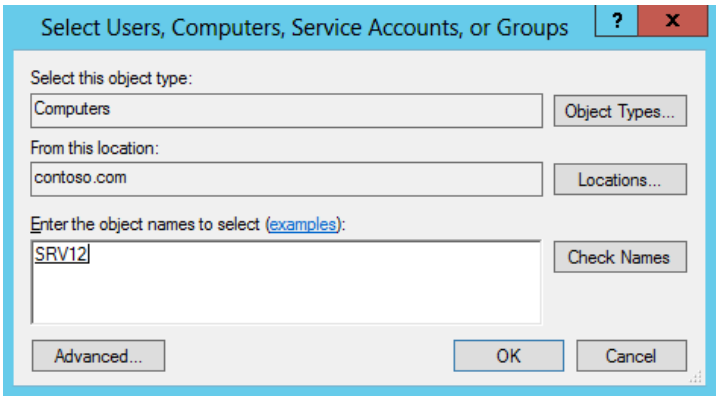
ICACLS C:\Web\Pubsite1 /grant "IIS AppPool\PubSite1":M

Список разрешений выглядит следующим образом:

D – удаление;
F – полный доступ;
M – изменение;
RX – чтение и выполнение;
R – чтение;
W – запись.

Если ресурс находится в сети, то для доступа к нему лучше всего использовать учетную запись NetworkService. Рабочий процесс, запущенный под этим аккаунтом, для доступа к ресурсам использует учетные данные компьютера, сгенерированные при добавлении компьютера в домен. Для того, чтобы дать процессу доступ к сетевому ресурсу, в качестве пользователя указываем компьютер:

• Выбираем тип объекта (Object Type) Computers;
• В поле Размещение (Locations) выбираем домен;
• Вводим имя пользователя в виде **domainname\machinename$**, например **contoso\SRV12$**;
• Проверяем имя и жмем ОК.



Очень удобный способ предоставлять доступ к сетевым ресурсам типа файловых шар или баз данных SQL Server. Однако работает он только при наличии домена AD.