Настройка Kerberos авторизации на сайте IIS

08.06.2022 itpro (https://winitpro.ru/index.php/author/itpro/)

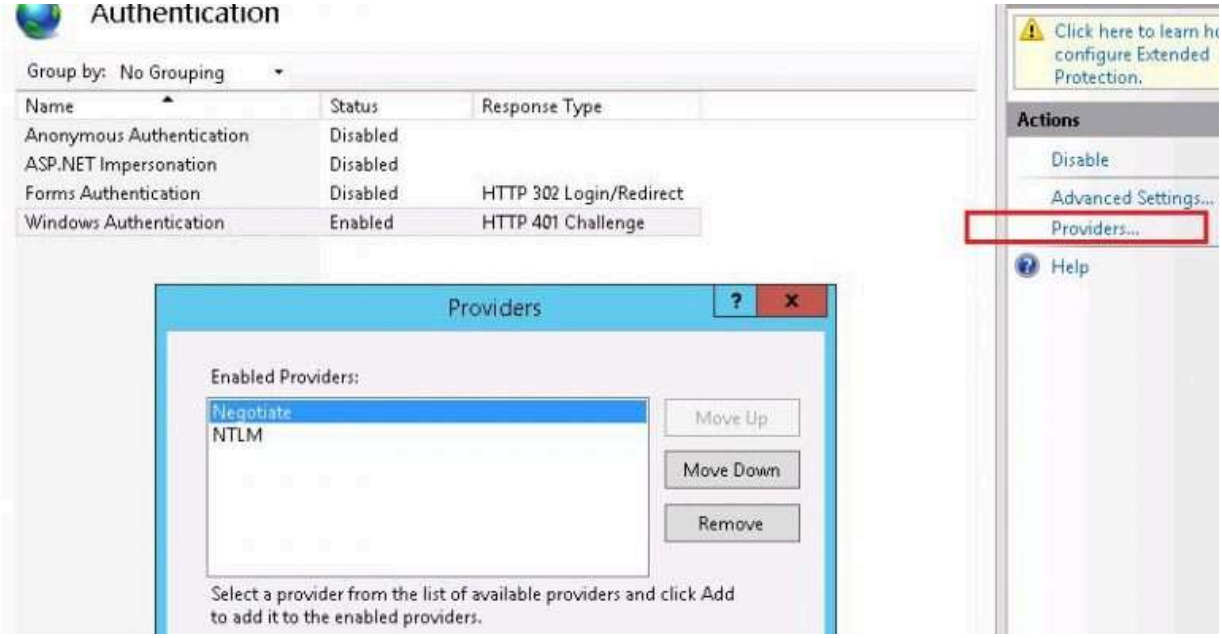
Windows Server 2012 R2 (https://winitpro.ru/index.php/category/windows-server-2012-r2/)

комментариев 26 (https://winitpro.ru/index.php/2016/05/18/nastrojka-kerberos-avtorizacii-na-sajte-iis/#comments)

Пошаговая инструкция по настройке на веб-сайте IIS на Windows Server 2012 R2 прозрачной авторизации доменных пользователей в режиме SSO (Single Sign-On) по протоколу Kerberos.

На веб сервере запустите консоль IIS Manager, выберите нужный сайт и откройте раздел **Authentication**. Как вы видите, по умолчанию разрешена только анонимная аутентификация (**Anonymous Authentication**). Отключаем ее и включаем **Windows Authentication** (IIS всегда сначала пытается выполнить анонимную аутентификацию).

(https://winitpro.ru/wp-content/uploads/2016/05/iis-windows-authentication.jpg)Открываем список провайдеров, доступных для Windows аутентификации (**Providers**). По умолчанию доступны два провайдера: **Negotiate** и **NTLM**. Negotiate – это контейнер, который в качестве первого метода проверки подлинности использует Kerberos, если эта аутентификация не удается, используется NTLM. Необходимо, чтобы в списке провайдеров метод **Negotiate** стоял первым.

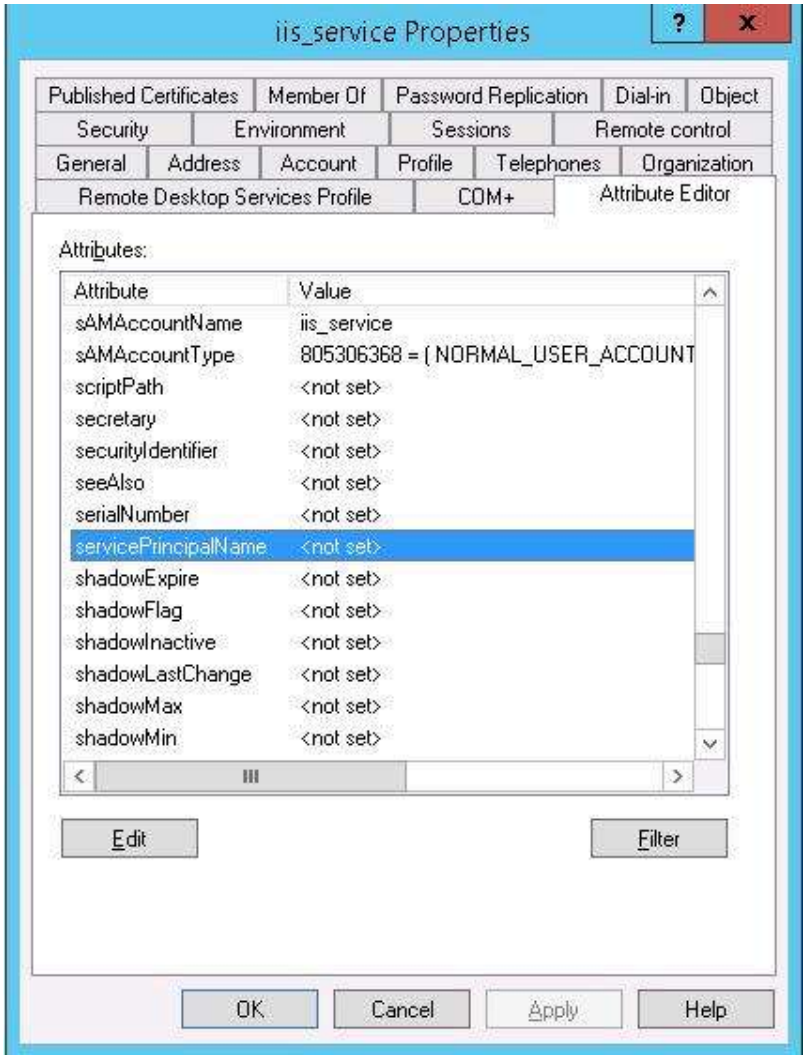


(https://winitpro.ru/wp-content/uploads/2016/05/negotiate-provider.jpg)

Следующий этап – регистрация **Service Principal Name (SPN)** записей для имени сайта, к которому будут обращаться пользователи. В том случае, если сайт IIS должен быть доступен только по имени сервера, на котором он расположен (http://server-name или http://server-name.contoso.com), создавать дополнительные SPN записи не нужно (SPN записи уже имеются в учетной записи сервера в AD). При использовании адреса сайта, отличного от имени хоста, или при построении веб-фермы с балансировкой, придется привязывать дополнительные записи SPN к учётной записи сервера или пользователя.

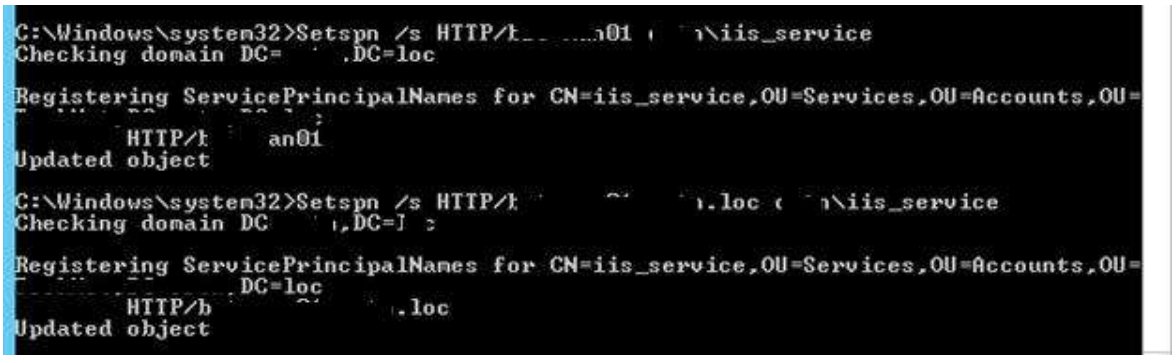
Предположим, у нас имеется ферма IIS серверов. В этом случае оптимально создать отдельную учетную запись в AD и привязать SPN записи к ней. Из-под этой же учетной записи будут запускать целевой Application Pool нашего сайта.

Создадим доменную учетную запись **iis_service**. Убедимся, что SPN записи для этого объекта не назначены (атрибут servicePrincipalName пустой).



(https://winitpro.ru/wp-content/uploads/2016/05/servicePrincipalName-empty.jpg)Предположим, что сайт должен отвечать по адресам _http://webportal and _http://webportal.contoso.loc. Мы должны прописать эти адреса в SPN атрибут служебной учетной записи

```
Setspn /s HTTP/webportal contoso\iis_service
Setspn /s HTTP/webportal.contoso.loc contoso\iis_service
```



(https://winitpro.ru/wp-content/uploads/2016/05/Setspn-s-HTTP.jpg)Таким образом, мы разрешим этой учетной записи расшифровывать тикеты Kerberos при обращении пользователей к данным адресам и аутентифицировать сессии.

Проверить настройки SPN у учетной записи можно так:

```
setspn /l iis_service
```

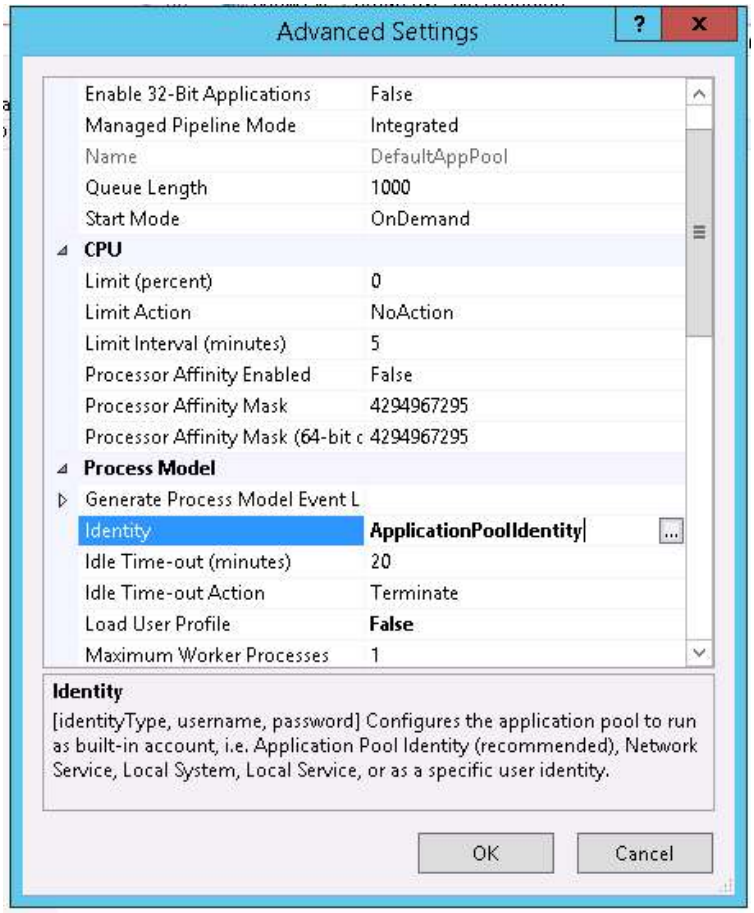
(https://winitpro.ru/wp-content/uploads/2016/05/setspn-l-iis_service.jpg)

> **Совет**. Kerberos не будет работать корректно при наличии дублирующих SPN у разных записей домена. С помощью следующей команды, убедитесь, что дубликатов SPN в домене нет: `setspn -x`

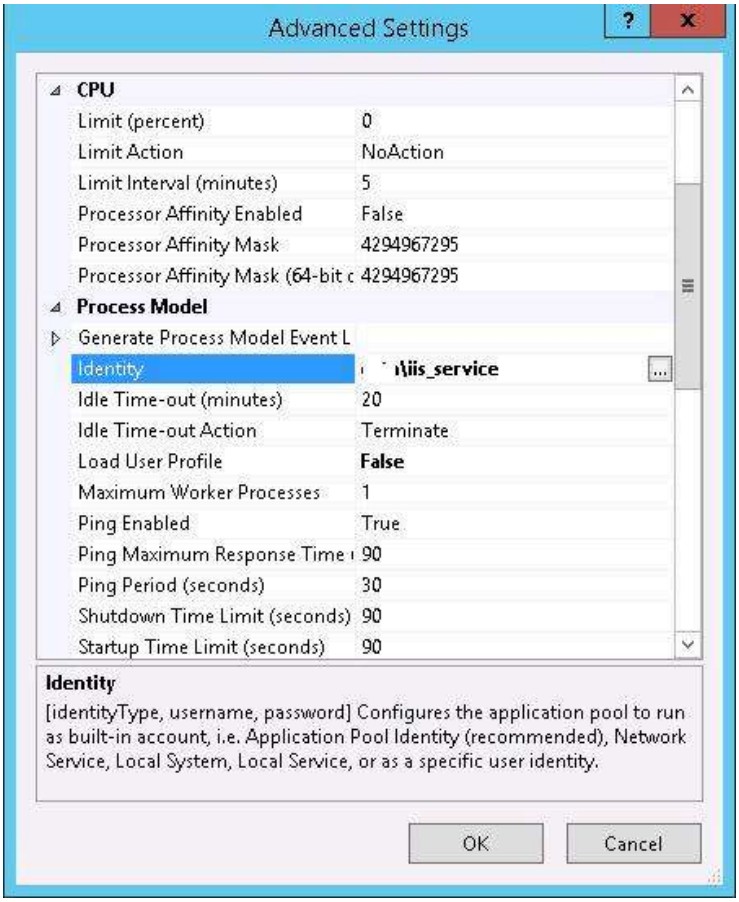
Следующий этап – настройка в IIS Application Pool для запуска из-под созданной сервисной учетной записи.

Выберите Application Pool сайта (в нашем примере это DefaultAppPool).

(https://winitpro.ru/wp-content/uploads/2016/05/DefaultAppPool.jpg)Откройте раздел настроек **Advanced Settings** и перейдите к параметру **Identity.**



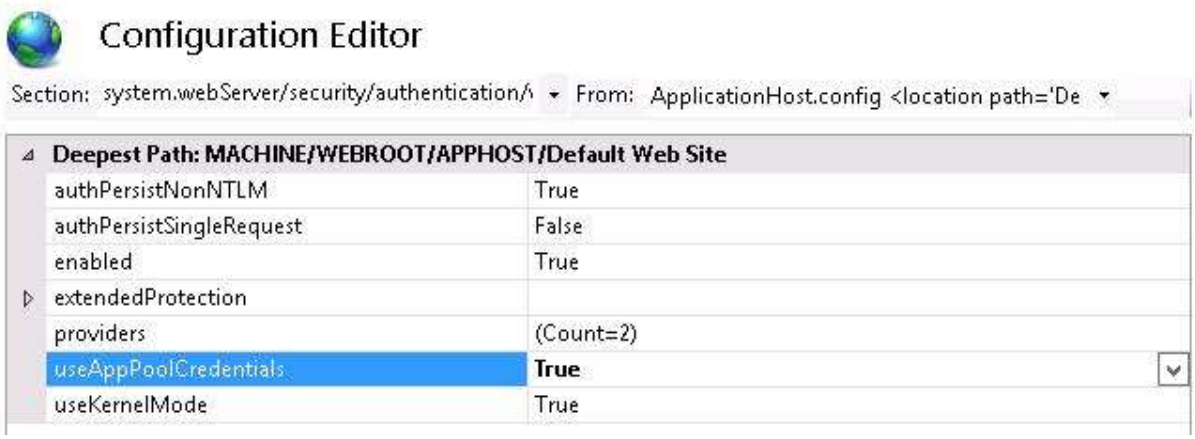
(https://winitpro.ru/wp-content/uploads/2016/05/iis-pool-advanced-settings.png)Измените его с **ApplicationPoolIdentity** на **contoso\iis_service**.



(https://winitpro.ru/wp-content/uploads/2016/05/iis-pool-identity.jpg)

Затем в консоли IIS Manager перейдите на свой сайт и выберите секцию **Configuration Editor**.

В выпадающем меню перейдите в раздел **system.webServer > security > authentication > windowsAuthentication**



(https://winitpro.ru/wp-content/uploads/2016/05/useAppPoolCredentials.jpg)

Измените **useAppPoolCredentials** на **True**.

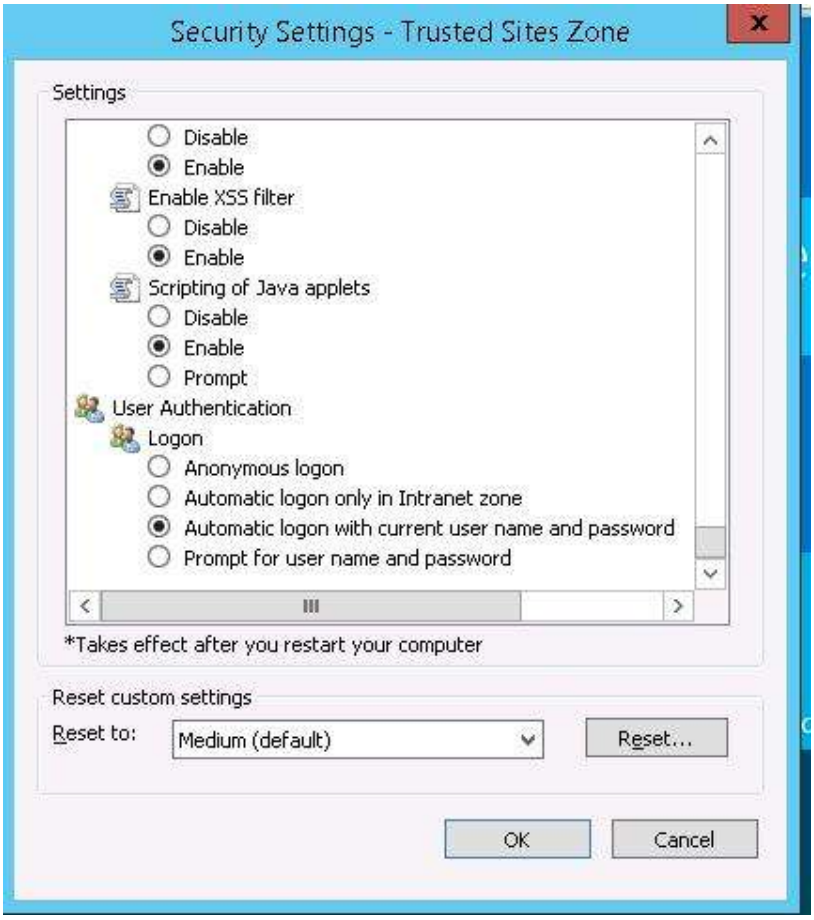
Тем самым мы разрешим IIS использовать доменную учетку для расшифровки билетов Kerberos (https://winitpro.ru/index.php/2015/05/14/razmer-bileta-kerberos-i-problemy-ego-rosta/) от клиентов.

Перезапустим IIS командой:

```
iisreset
```

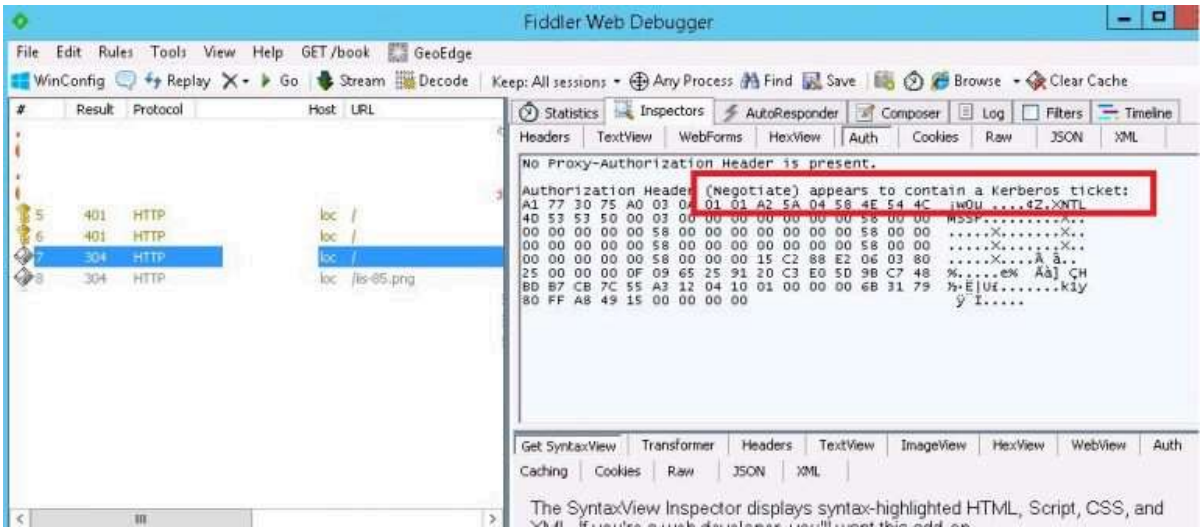
(https://winitpro.ru/wp-content/uploads/2016/05/iisreset.jpg)Аналогичную настройку нужно выполнить на всех серверах веб-фермы.

Протестируем работу Kerberos авторизации, открыв в браузере клиента (браузер нужно предварительно настроить для использования Kerberos (https://winitpro.ru/index.php/2018/01/22/nastrojka-kerberos-autentifikacii-v-razlichnyx-brauzerax/)) адрес _http://webportal.contoso.loc

> **Примечание**. В моем примере, на IE11 сразу авторизоваться не получилось. Пришлось добавить адрес в доверенные и в настройках Trusted Zones Sites выставить значение параметра User Authentication -> Logon на **Automatic logon with current user name and password**
>
> 
>
>
> (https://winitpro.ru/wp-content/uploads/2016/05/User-Authentication-Automatic-logon-with-current-user-name-and-password.jpg)

Убедится, что для авторизации на сайте используется Kerberos можно с помощью инспектирования HTTP трафика утилитой Fiddler.

Запускаем Fiddler, в браузере открываем целевой сайт. В левом окне находим строку обращения к сайте. Справа переходим на вкладку Inspectors. Строка **Authorization Header (Negotiate) appears to contain a Kerberos ticket**, говорит о том, что для авторизации на IIS сайте использовался протокол Kerberos.



(https://winitpro.ru/wp-content/uploads/2016/05/iis-kerberos-authorization.jpg)

Предыдущая статья (https://winitpro.ru/index.php/2016/05/16/polzunok-user-account-control-i-nastrojki-gruppovyx-politik/)

Следующая статья (https://winitpro.ru/index.php/2016/05/20/obnovlenie-chlenstva-v-gruppax-ad-bez-perezagruzki-perelogina/)

Читайте далее в разделе Windows Server 2012 R2 (https://winitpro.ru/index.php/category/windows-server-2012-r2/)

Аудит удаления файлов в сетевой папке на Windows Server (https://winitpro.ru/index.php/2016/05/04/prostaya-sistema-audita-udaleniya-fajlov-i-papok-dlya-windows-server/)

FTP over SSL (FTPS) в Windows Server 2012 R2 (https://winitpro.ru/index.php/2016/03/14/ftp-over-ssl-ftps-v-windows-server-2012-r2/)

Использование TSADMIN.msc и TSCONFIG.msc для управления RDS в Windows Server 2019/2016/2012R2 (https://winitpro.ru/index.php/2016/03/02/zapusk-osnastok-tsadmin-msc-i-tsconfig-msc-v-windows-server-2012-r2/)

FAQ по KMS активации продуктов Microsoft (Windows и Office)

Аудит удаления файлов в сетевой папке на Windows Server