

Настройка Kerberos авторизации на сайте IIS

winitpro.ru/index.php/2016/05/18/nastrojka-kerberos-avtorizacii-na-sajte-iis

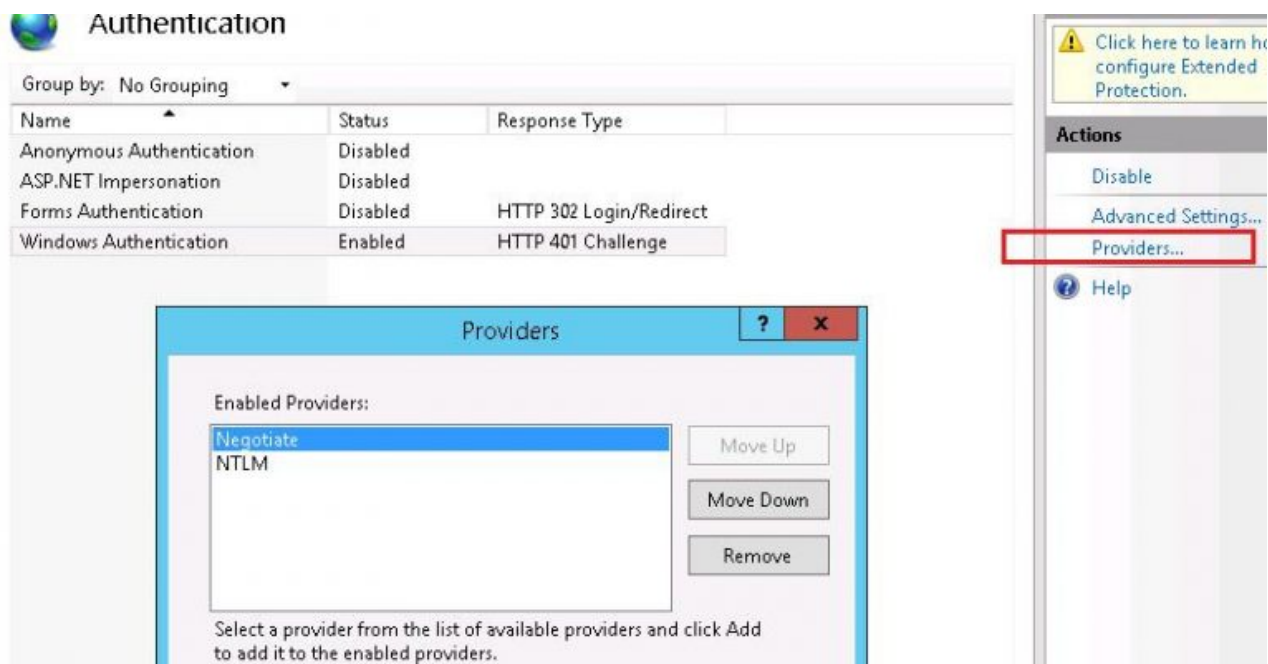
itpro

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).



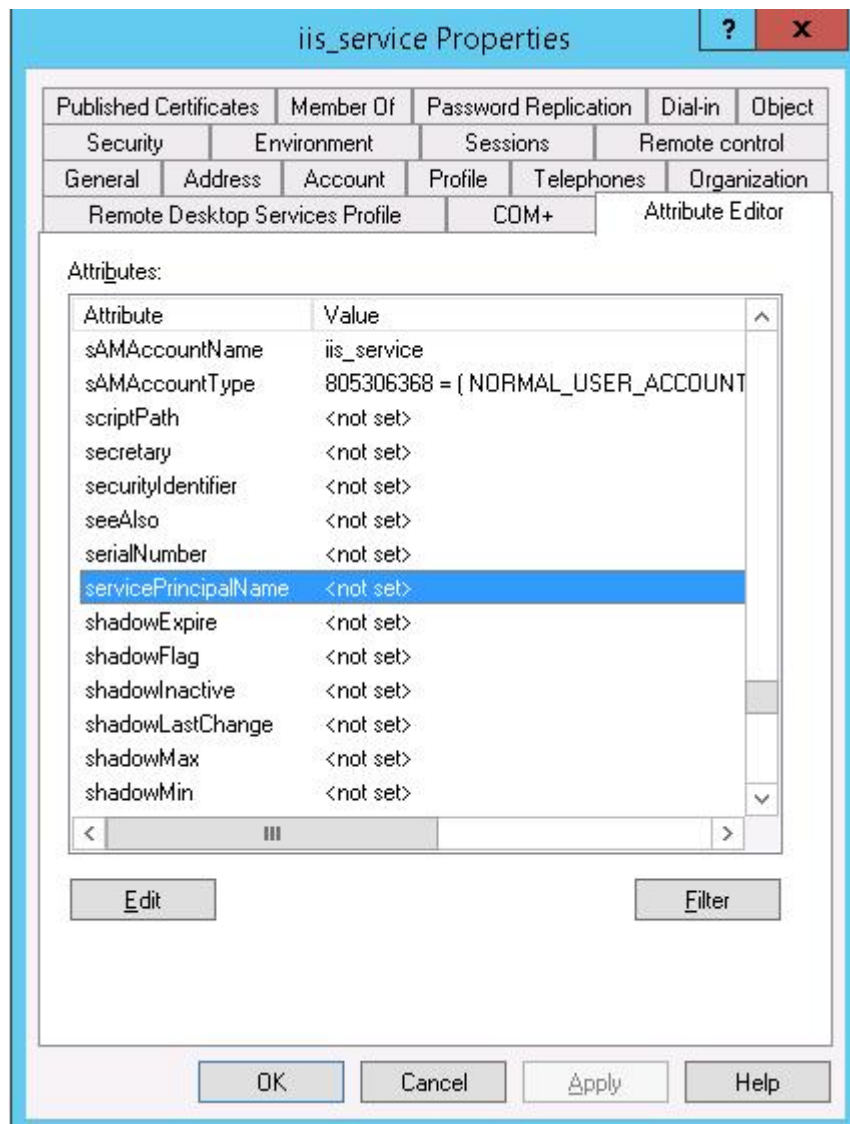
Открываем список провайдеров, доступных для Windows аутентификации (**Providers**). По умолчанию доступны два провайдера: **Negotiate** и **NTLM**. Negotiate – это контейнер, который в качестве первого метода проверки подлинности использует Kerberos, если эта аутентификация не удастся, используется NTLM. Необходимо, чтобы в списке провайдеров метод **Negotiate** стоял первым.



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).



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
```

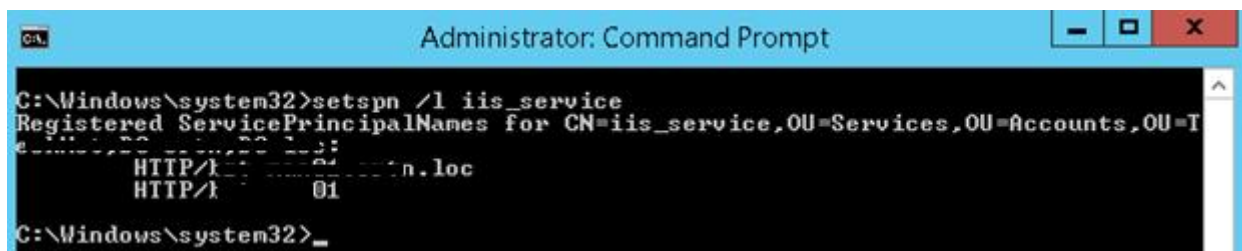
```
C:\Windows\system32>Setspn /s HTTP/webportal contoso\iis_service
Checking domain DC=contoso,DC=loc
Registering ServicePrincipalNames for CN=iis_service,OU=Services,OU=Accounts,OU=
HTTP/webportal
Updated object

C:\Windows\system32>Setspn /s HTTP/webportal.contoso.loc contoso\iis_service
Checking domain DC=contoso,DC=loc
Registering ServicePrincipalNames for CN=iis_service,OU=Services,OU=Accounts,OU=
DC=loc
HTTP/webportal.contoso.loc
Updated object
```

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
```



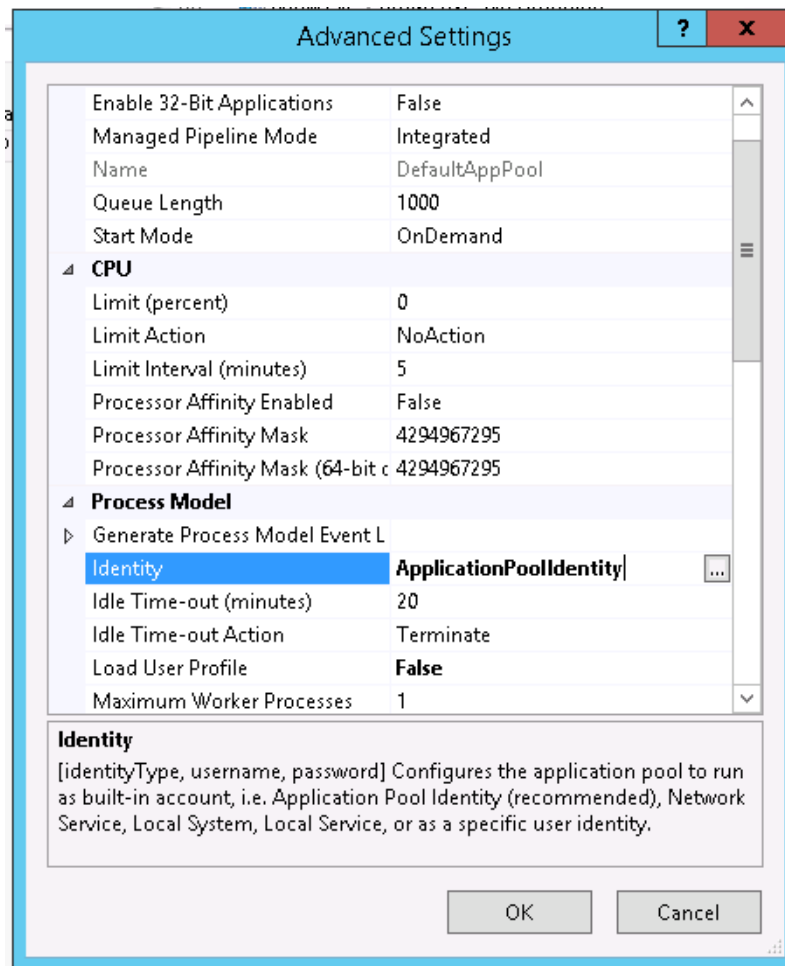
Совет. Kerberos не будет работать корректно при наличии дублирующих SPN у разных записей домена. С помощью следующей команды, убедитесь, что дубликатов SPN в домене нет: `setspn -x`

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

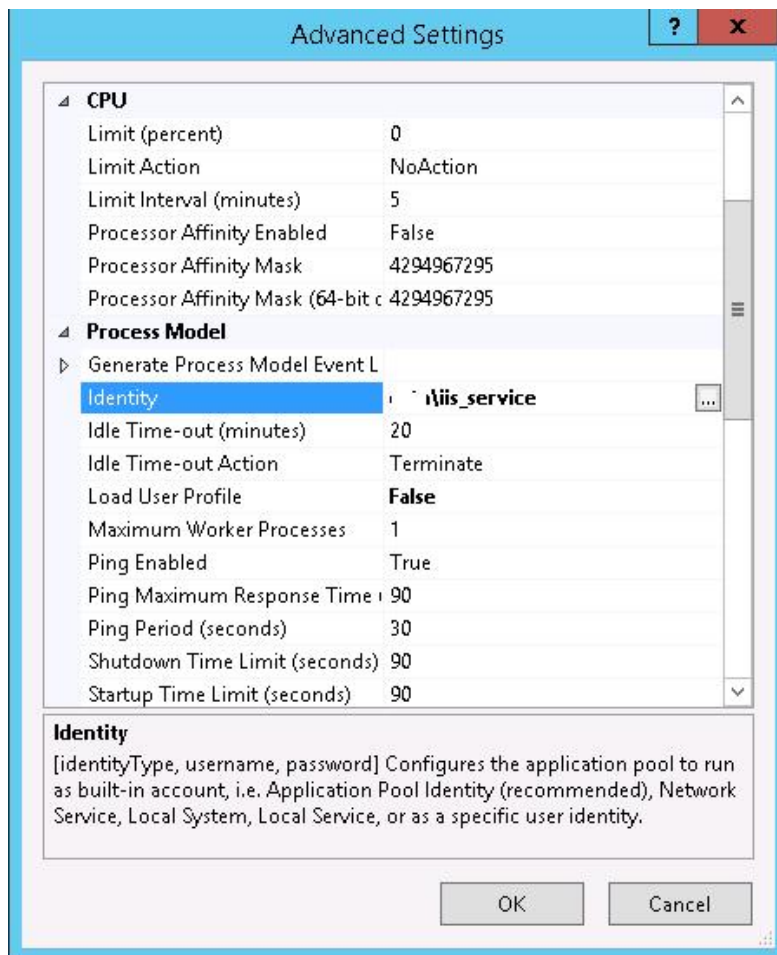
Выберите Application Pool сайта (в нашем примере это DefaultAppPool).

Name	Status	.NET CLR V...	Managed Pipel...	Identity	Applications
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolId...	0
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolId...	0
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolId...	1
WsusPool	Started	v4.0	Integrated	NetworkService	8

Откройте раздел настроек **Advanced Settings** и перейдите к параметру **Identity**.



Измените его с **ApplicationPoolIdentity** на **contoso\iis_service**.



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**



Configuration Editor

Section: system.webServer/security/authentication/... From: ApplicationHost.config <location path='De...>

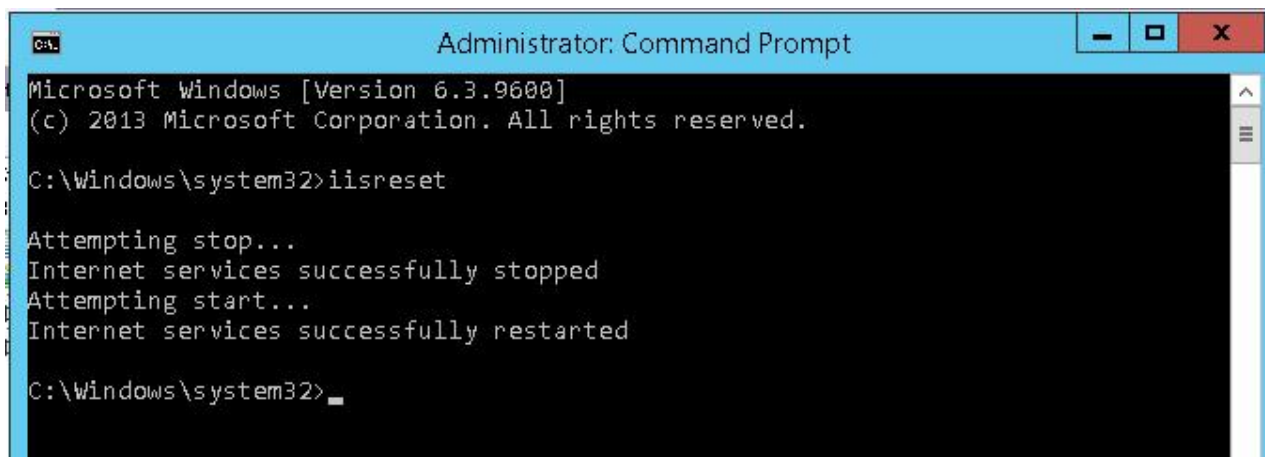
Deepest Path: MACHINE/WEBROOT/APPHOST/Default Web Site	
authPersistNonNTLM	True
authPersistSingleRequest	False
enabled	True
extendedProtection	
providers	(Count=2)
useAppPoolCredentials	True
useKernelMode	True

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

Тем самым мы разрешим IIS использовать доменную учетку для расшифровки билетов Kerberos от клиентов.

Перезапустим IIS командой:

iisreset



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>iisreset

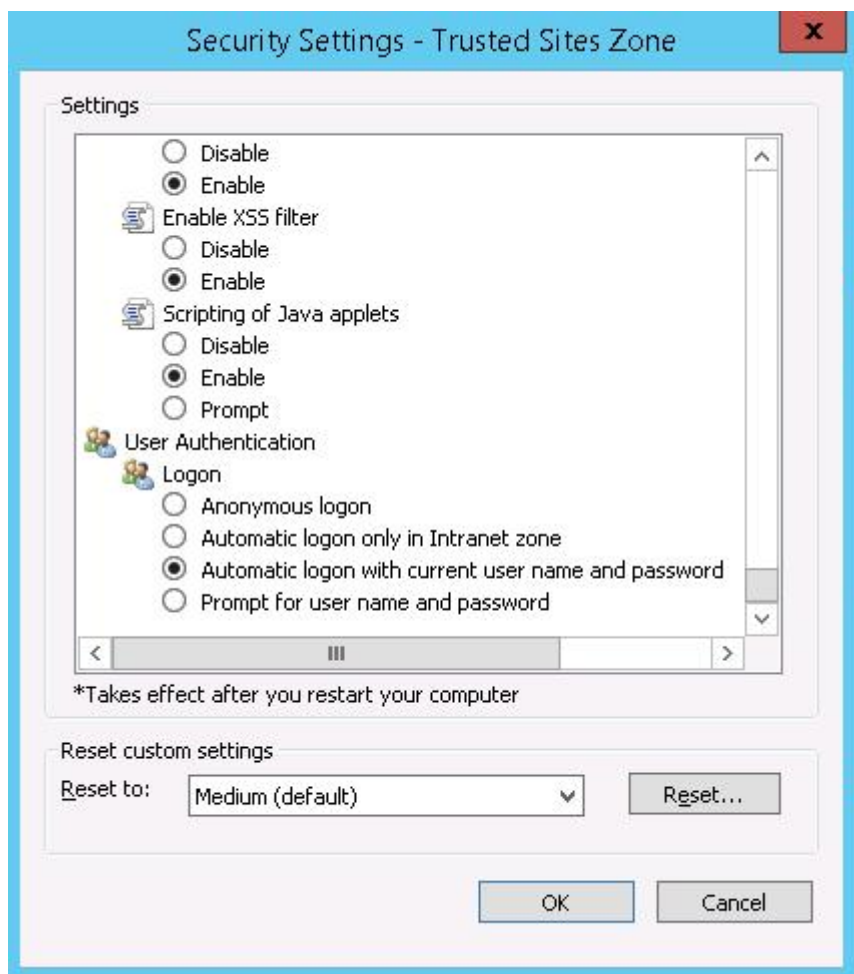
Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted

C:\Windows\system32>_
```

Аналогичную настройку нужно выполнить на всех серверах веб-фермы.

Протестируем работу Kerberos авторизации, открыв в браузере клиента (браузер нужно предварительно настроить для использования Kerberos) 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**



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 сайту. 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.

