



Deploying Microsoft IIS with ZXTM

Accelerating and managing Microsoft IIS with ZXTM

Zeus Technology Limited (UK)
The Jeffreys Building
Cowley Road
Cambridge CB4 0WS
United Kingdom

Sales: +44 (0)1223 568555
Main: +44 (0)1223 525000
Fax: +44 (0)1223 525100
Email: info@zeus.com
Web: www.zeus.com

Zeus Technology, Inc. (U.S.)
1955 Landings Drive
Mountain View
CA 94043
United States of America

Phone: 1-888-ZEUS-INC
Fax: (866) 628-7884
Email: info@zeus.com
Web: www.zeus.com

Contents

Introduction	3
Prerequisites	3
Topology	3
Basic Configuration	4
Create a new service	4
Create a Traffic IP Group (optional)	5
Advanced Configuration Topics	7
Preserving the Client’s IP Address.....	7
Session Persistence	7
Load Balancing Algorithms.....	8
Authentication through ZXTM.....	8
SSL Decryption	9
Exporting SSL keys from IIS	9
Export SSL keys to PKCS12	9
Converting PKCS12 to PEM using OpenSSL.....	9
Importing SSL Certificates into ZXTM.....	10
Using SSL Decryption.....	10
Conclusion	11



Introduction

The pursuit of five nines or 99.999% uptime is what makes a system administrator's life so taxing. Since its first release, ZXTM (Zeus Extensible Traffic Manager) has been designed to help the busy administrator keep control of increasingly complex web infrastructure. This guide gives you the low down on using Microsoft Internet Information Server (IIS) with ZXTM.

Prerequisites

- ZXTM Version 4.1 or later¹
- Microsoft IIS 6.0 or later

We will assume that you are familiar with IIS and have an application installed and configured to your specifications.

Before you proceed, you will need to install ZXTM on one or more machines in front of the IIS server farm. You can use the ZXTM software on Windows, Linux or a supported Unix platform, or the ZXTM appliance.

For help with the initial set up of ZXTM, you may refer to the appropriate Getting Started Guide² available from the ZXTM KnowledgeHub.

Topology

We generally recommend that the ZXTM cluster is placed between your IIS server farm and the border gateway or firewall. This allows ZXTM to manage all traffic to the IIS servers and gives you the option of using a ZXTM protection class to defend against DOS and other malicious attacks.

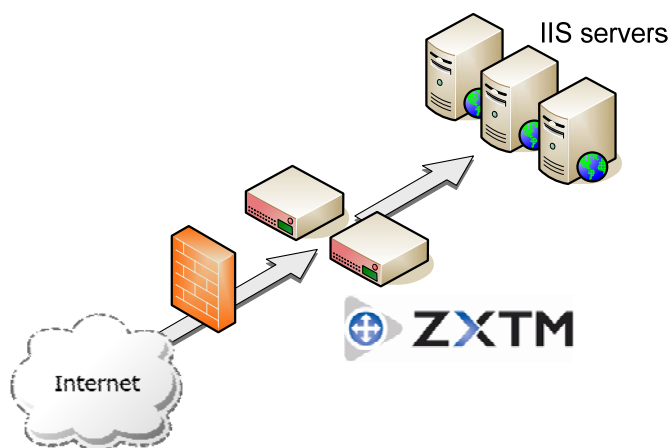


Figure 1

¹ ZXTM 4.1 introduced support for Microsoft NTLM authentication. If you do not use NTLM authentication then you may use ZXTM 4.0.

² <http://knowledgehub.zeus.com/docs/>



Basic Configuration

You need to configure ZXTM to accept traffic and load-balance it across the IIS server nodes. If you have two or more ZXTM systems, you can then optionally configure a Traffic IP group for fault tolerance purposes.

Create a new service

Use the “Manage a new service” wizard to manage a new virtual server and pool.

We want to manage a new service using protocol HTTP and port 80. We can call this service “IIS Farm”:

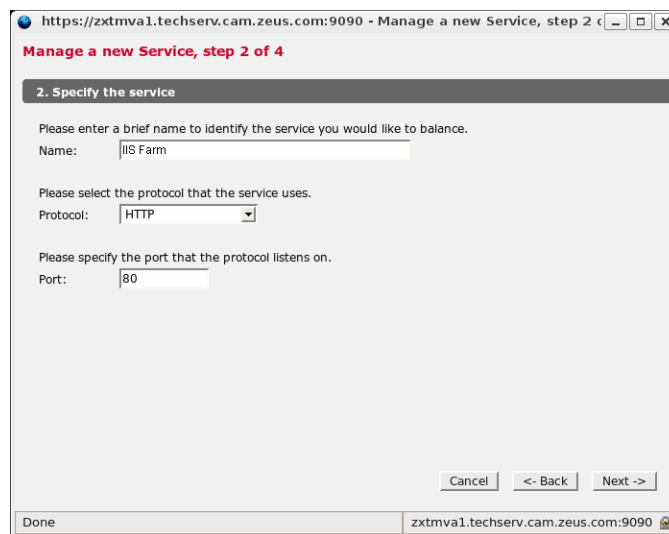


Figure 2

On the next screen we need to add all the IIS server farm members as nodes.

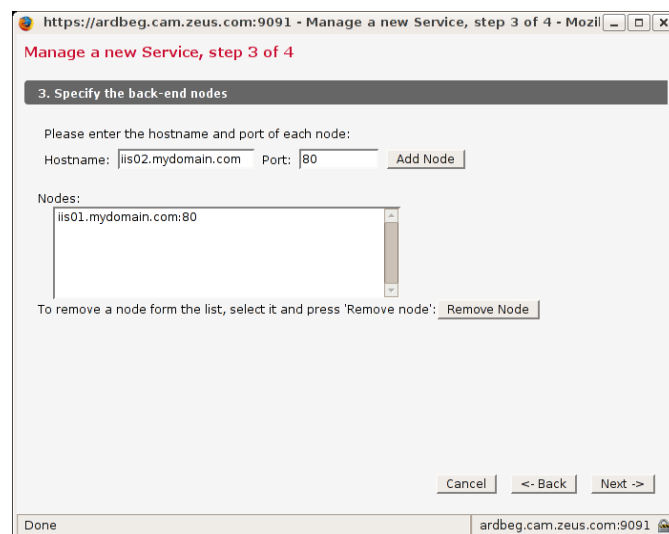


Figure 3



Click “Next” to review the configuration and finish the set up.

Your IIS Farm service should now be running. You can return to the ZXTM home page and observe that the new service has been created and is running:



Figure 4

Now you have your first IIS service up and running you can start sending requests through it. ZXTM will use the default round-robin load balancing algorithm to assign incoming requests evenly amongst the IIS servers.

Test the service out using a url like `http://<ZXTM IP address>/`, using one of the IP addresses that your ZXTM is using.

Generally, when an organization configures a load balancer like ZXTM, they arrange that the DNS name of their service (e.g. `www.mydomain.com`) resolves to the IP address(es) that ZXTM is listening on. The back-end IIS server nodes are configured to accept web requests on all IP addresses.

If you are running several web sites, you would configure them to have different identities (distinguished by host header). These identities should correspond to the DNS names that users use to access the service through ZXTM.

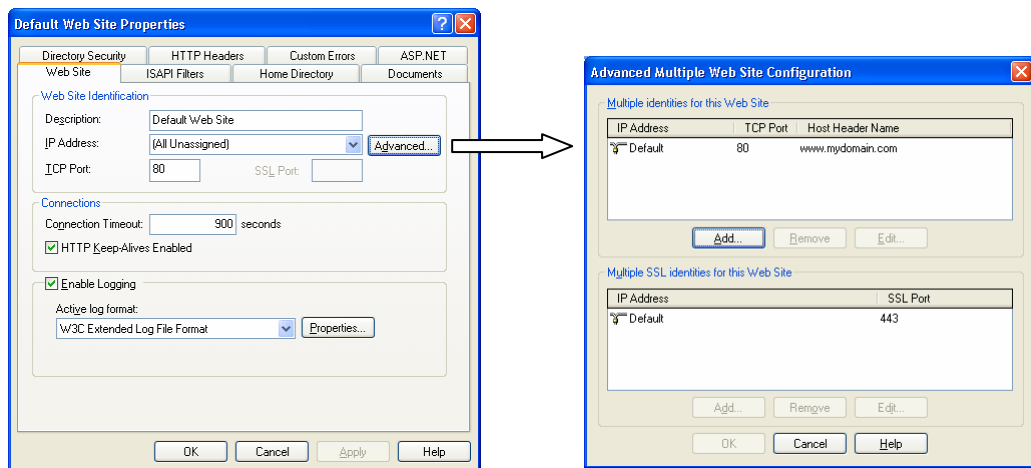


Figure 5

Create a Traffic IP Group (optional)

A Traffic IP Group contains one or more virtual IP addresses. These “Traffic IP addresses” float between the ZXTM machines and are always available, even if some of the ZXTM machines fail.



Traffic IP groups are used to achieve fault tolerance. Services are often published using a DNS name that resolves to a Traffic IP address rather than one of the permanent ZXTM IP addresses.

To create a Traffic IP group, go to **Services** -> **Traffic IP Group**. Create the Traffic IP group, specifying the external IP address(es) to which the host names of your websites resolve:



Traffic Manager	Add
 zxtmva1.techserv.cam.zeus.com 10.100.9.126	<input checked="" type="checkbox"/>
 zxtmva2.techserv.cam.zeus.com 10.100.9.127	<input checked="" type="checkbox"/>

Figure 5

These IP addresses should be different to the permanent IP addresses on the ZXTM machines.

If you wish, you can then go to **Services** -> **Virtual Servers** -> **IIS Farm** and bind the service to the Traffic IP Group you created.



Advanced Configuration Topics

Preserving the Client's IP Address

When ZXTM manages your traffic, the back-end servers observe that the connections come from the ZXTM system rather than the remote client. This can be a problem when your servers log requests, or perform authentication based on the client's IP address.

You have several options at this point:

1. You can enable access logging on ZXTM and keep a separate log of the client connections. Access logging is enabled under **Services -> Virtual Servers -> <ServerName> -> Access Logging**.
2. You can enable the **add_cluster_ip** setting in ZXTM under **Services -> Virtual Server -> <ServerName> -> Connection Settings -> HTTP Specific settings**. Then use a custom ISAPI filter to change the logging behavior of IIS. Source for such a module can be found here³. The header you need to log is "X-Cluster-Client-IP".
3. You can enable IP Transparency on ZXTM⁴. When using IP Transparency, the IIS servers will also need to use the ZXTM cluster as their default gateway.

You can enable transparency under **Services -> Pools -> <Pool Name> -> Connection settings**.

Session Persistence

It's possible you are in the excellent position of having cluster aware applications running on your IIS server farm. It's also possible that these applications share state information so quickly that requests a fraction of a second apart can hit different servers without causing problems.

However, if that's not the case, or you would prefer not to run the risk of a late/lost synchronization message breaking a transaction, then ZXTM Session Persistence can help. ZXTM Session Persistence will ensure that all subsequent requests from a client are sent to the same server as the first request.

ZXTM can use almost anything within the HTTP request to assign session persistence. The most commonly used persistence method is Transparent Session Affinity. ZXTM inserts its own tracking cookie in to the HTTP session and uses this to manage persistence.

Other options include:

- IP Based Persistence. Manage the session based on the client IP address.

3

http://blogs.msdn.com/david.wang/archive/2005/09/28/HOWTO_ISAPI_Filter_which_Logs_original_Client_IP_for_Load_Balanced_IIS_Servers.aspx

⁴ http://knowledgehub.zeus.com/news/2006/04/12/ip_transparency_with_the_zxtm_software



- Universal Session Persistence: The session is managed based on data pulled out of the HTTP transaction itself using TrafficScript™.
- Monitor Application Cookies: ZXTM will monitor a specified cookie, such as ASPSESSIONID to maintain persistence.

The easiest way to use Session Persistence is to:

1. Create a Session Persistence class of the preferred type using **Catalog** -> **Persistence**.
2. Configure your "IIS Farm" pool to use that session persistence class. Use **Services** -> **Pools** -> **IIS Farm** -> **Session Persistence** to do this.

For complicated scenarios, you can use multiple types of session persistence, and you can selectively apply session persistence to just the requests that require it. The KnowledgeHub article 'Controlling Session Persistence'⁵ gives examples of how to do this.

Load Balancing Algorithms

By default, a newly created pool will use a simple round robin algorithm. This takes no account of the load on the back-end servers, and so it is recommended that one of the more sophisticated algorithms is used. The optimal choice will depend on the application being run. See section 5.2.1 of the ZXTM User Manual for details of each algorithm.

The "Least Connections" algorithm is a sensible default if all your backend servers are running on the same hardware.

Authentication through ZXTM

The IIS authentication methods supported through ZXTM are Basic Authentication (plaintext) and Windows Integrated Authentication (NTLM).

⁵ http://knowledgehub.zeus.com/code/2005/07/01/controlling_session_persistence



SSL Decryption

You may use ZXTM to off-load (terminate) any incoming SSL connections. This reduces the load on your application server by making use of the highly optimized SSL engine of ZXTM. If you already have certificates stored in IIS you will need to export them to ZXTM before you can use the SSL Offloading feature.

Exporting SSL keys from IIS

If you need to export an existing certificate from IIS you will first need to export a PKCS12 format file from IIS and then export the keys into a PEM format for upload into ZXTM.

Export SSL keys to PKCS12

From within the IIS services manager you will need to open the properties of the website for which you want to export the keys. Select the Directory security tab and then click the "Server Certificate" button. In the wizard that opens, select to export the certificate to a PFX file.

Converting PKCS12 to PEM using OpenSSL

You now need to extract the certificate and keys from the PKCS12 file store. If you have a preferred certificate management application you should be able to use that to retrieve the keys and export them into PEM format. If you don't have a preferred application then you can use OpenSSL and follow the instructions below. OpenSSL is included with most Linux distributions and a Windows version is also available⁶

To perform the conversion, issue the following commands:

```
openssl pkcs12 -in <input file.pfx> -nodes -nokeys -out server.cert.pem  
openssl pkcs12 -in <input file.pfx> -nodes -nocerts -out server.key.pem
```

You now have the server certificate stored in server.cert.pem and the server key in server.key.pem.

⁶ <http://www.openssl.org/related/binaries.html>



Importing SSL Certificates into ZXTM

You will now need to access the ZXTM administration page and navigate to **Catalogs** -> **SSL** -> **Server Certs** and then select the import certificate option:

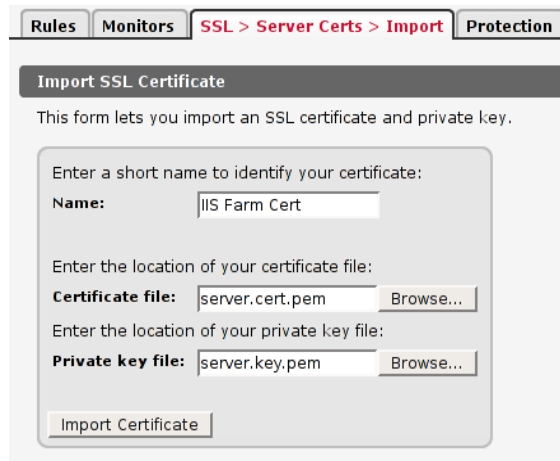


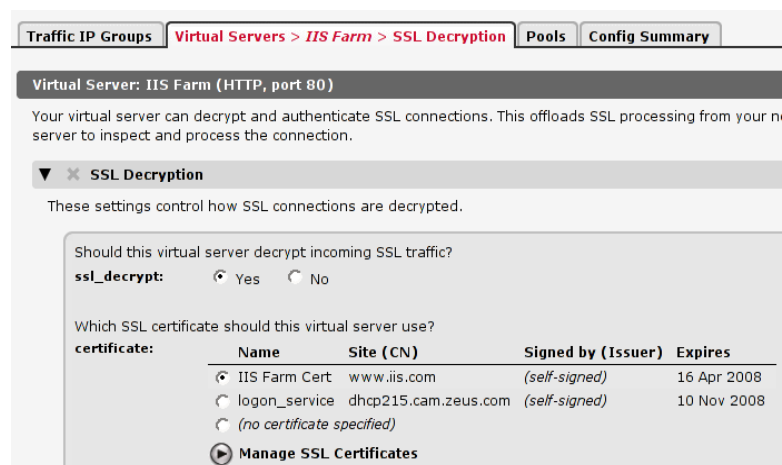
Figure 6

Once the certificate has been imported into the SSL catalog you can start to use it to terminate SSL secured websites at ZXTM.

Using SSL Decryption

ZXTM can support HTTPS as the internal protocol, but when you are using SSL Offloading ZXTM will still process the encapsulated HTTP. For this reason a SSL offloading service should be created in the same way you created the HTTP service, using the HTTP protocol, but port 443 instead of 80. You can either create a new virtual server which uses the same pool as the HTTP server, or if you want all traffic over HTTPS you can modify the previously created "IIS Farm" virtual server to use the HTTPS port (443).

Once you have modified the port or created a new virtual server you will need to enable SSL decryption. This can be found on the virtual server page.



certificate:	Name	Site (CN)	Signed by (Issuer)	Expires
<input checked="" type="radio"/>	IIS Farm Cert	www.iis.com	(self-signed)	16 Apr 2008
<input type="radio"/>	logon_service	dhcp215.cam.zeus.com	(self-signed)	10 Nov 2008
<input type="radio"/>	(no certificate specified)			

Manage SSL Certificates

Figure 7



Once you click update, your virtual server is setup and ready to decrypt incoming SSL connections. If you also want to pass on SSL variables, you can do this by setting the `ssl_headers` option to "yes" in the "SSL Decryption" section.

Conclusion

This document briefly discusses how to configure ZXTM to effectively load balance traffic to a farm of Microsoft IIS servers.

ZXTM is able to manage traffic in a wide variety of ways, to improve site performance, security, reliability and integrity. Please refer to the product documentation and to the ZXTM KnowledgeHub website⁷ for examples of how ZXTM can be deployed to meet a range of service hosting problems.

⁷ <http://knowledgehub.zeus.com/>



Copyright

© Zeus Technology Limited 2007. Copyright in this document belongs to Zeus Technology Limited. All rights are reserved.

Trademarks

Zeus Technology, the Zeus logo, Zeus Web Server, Zeus Load Balancer, Zeus Extensible Traffic Manager, ZXTM, ZXTM Global Load Balancer, ZXTM Virtual Desktop Broker and associated logos and abbreviations, TrafficScript, TrafficCluster and RuleBuilder are trademarks of Zeus Technology Limited. Other trademarks may be owned by third parties.

Contact Information

If you would like to learn more about any of the topics covered by this white paper, please feel free to contact us for more information. You can reach us in a variety of ways:

By Email

For general enquiries:	info@zeus.com
For commercial and technical enquiries:	sales@zeus.com
For reseller information:	partners@zeus.com
For press and public relations information:	press@zeus.com

By Telephone

Zeus Technology UK:	+44 1223 525000
Zeus Technology US:	+1 650 965 4627 or 1-888-ZEUS-INC
Fax:	+44 1223 525100

By Post or in Person

Zeus Technology Limited	Zeus Technology
The Jeffreys Building	1955 Landings Drive
Cowley Road	Mountain View
Cambridge CB4 0WS	CA 94043
United Kingdom	United States

www.zeus.com

Our web site contains a wealth of information on our products, services and solutions, as well as customer case studies and press information. For more information, please visit <http://www.zeus.com/>.

knowledgehub.zeus.com

The ZXTM KnowledgeHub is a key resource for developers and system administrators wishing to learn about ZXTM and Zeus' Traffic Management solutions. It is located at <http://knowledgehub.zeus.com/>.

