



| z/TPF V1.1

TPF Users Group Fall 2008 Apache v2.2.9

Deciding to Upgrade to Apache v2.2.9

Jim Johnston
Distributed Subcommittee

AIM Enterprise Platform Software
IBM z/Transaction Processing Facility Enterprise Edition 1.1.0

Any reference to future plans are for planning purposes only. IBM reserves the right to change those plans at its discretion. Any reliance on such a disclosure is solely at your own risk. IBM makes no commitment to provide additional information in the future.

Decision Goal

- **The IBM TPF lab sees several benefits to upgrading to Apache v2.2.9**
- **Presentation will share the following with you:**
 - Highlights of design changes
 - Highlights of new features with basic use examples
 - Other information specific to z/TPF support of Apache
- **Decide if your organization can leverage these benefits**

What is Apache again?

- **An open-source HTTP server**
- **Maintenance/Development**
 - ~60 development volunteers, Hundreds of Contributors
 - Commercial support for Apache available from numerous companies
- **Market share of active servers (as of 8/08) ***
 - 47% Apache, 35% MS, 6% Google, 12% Others

* Source: <http://www.netcraft.com/>

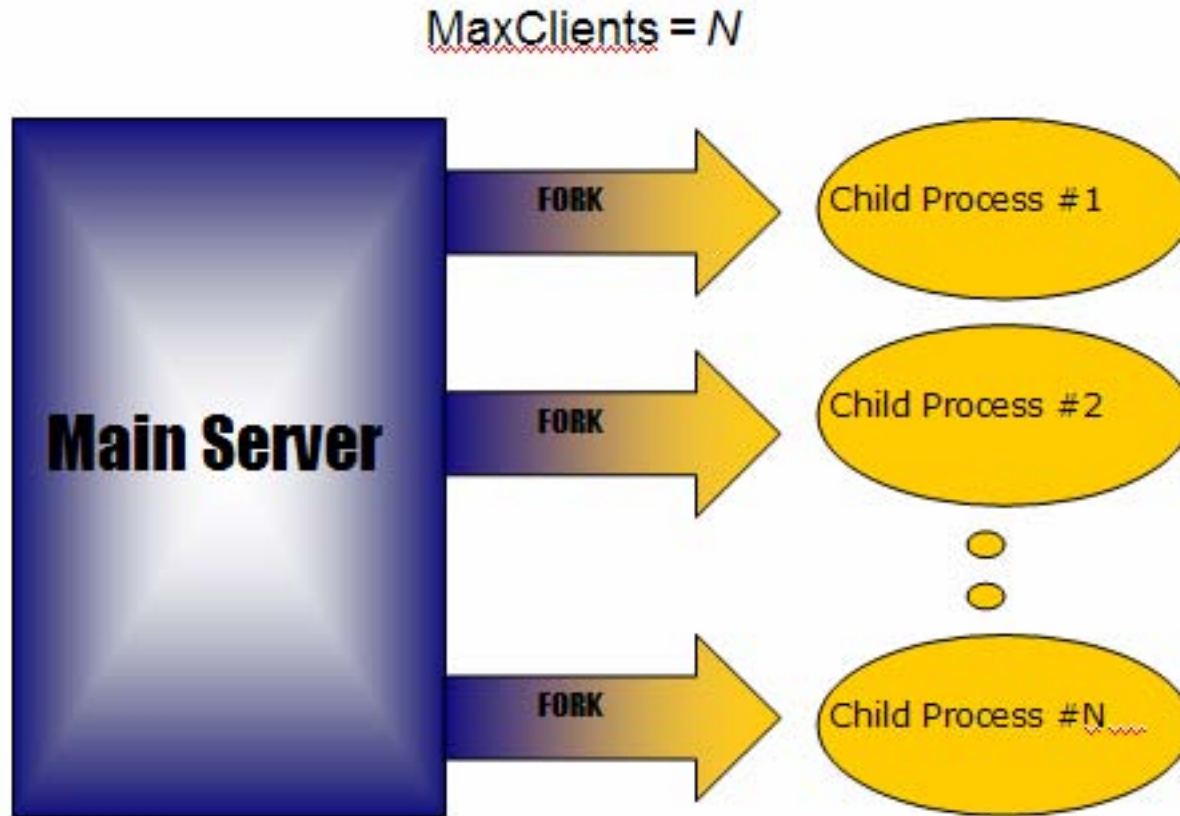
Previous Apache Support on TPF 4.1 and z/TPF

- **Apache v1.3**
 - Does not make use of threads
- **Limitations specific to TPF**
 - No mod_ssl support
 - No mod_rewrite support
 - No mod_so support (Dynamic Shared Object linkage)
 - No more than one “listening” port per server
 - Configuration file read in on a per-child basis

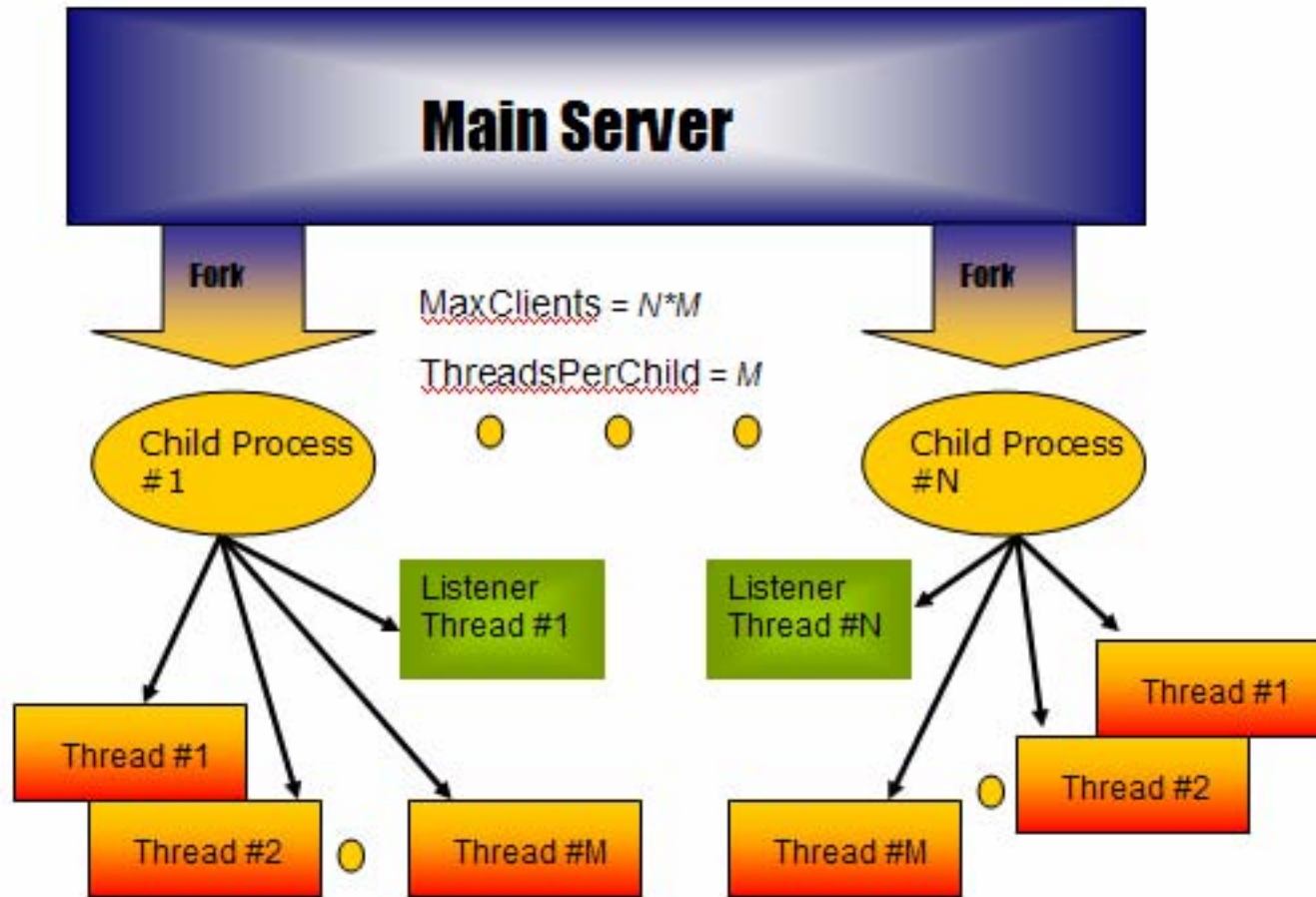
New Apache v2.2.9 (z/TPF only)

- **Server Design Change**
 - New Worker MPM (Multi-Processing Modules)
- **New features & other changes**
 - mod_ssl, mod_deflate, mod_rewrite, and mod_so enabled for z/TPF
 - Authorization & Authentication modules enhanced
 - One server can listen on multiple ports (“Listen” Directive)
 - mod_proxy enhanced with load balancer and manager

Pre-fork MPM Architecture



Worker MPM Architecture



Mod_ssl


- **SSL/TLS (Secure Sockets Layer/Transport Layer Security)**
 - A lot of data is transmitted in “plain text” and “hops” across several other servers before reaching destination.
 - SSL/TLS uses a complex exchange of keys/certificates in order to encrypt data before heading to destination.
 - Several Protocols adopted the use of SSL/TLS
- **How do you tell if your web page is secured?**
 - Url with “https:” or look for “lock” icon on browser

Example of enabling SSL

In httpd.conf

```
Listen 80
Listen 443
...
<VirtualHost _default_:443>
SSLEngine On
SSLCipherSuite ALL:!DH:!EXP:!NULL:!RC2:!RC4:!IDEA:!MD5:+HIGH:+MEDIUM:+LOW
SSLCertificateFile "/example/server.crt"
SSLCertificateKeyFile "/example/server.key"
</VirtualHost>
...
```

Ensure Cipher Selected
takes advantage of
Hardware Cryptography
on z/TPF



More on SSL

- **Enforce Client Certificate Verification**
 - SSLVerifyClient (set to 'require', default is none)
 - SSLCACertificateFile/SSLCACertificatePath
- **Flexible SSL Renegotiations Configuration**
 - SSLCipherSuite (RC4-MD5, AES128-SHA, etc.)
 - Redefine SSLCipherSuite in <Directory> to force renegotiations
- **Apache 2.2.9 compatible with z/TPF PKI project generated private keys**

What is Authentication and Authorization?

- **Authentication**
 - Are you who you say you are?
 - Typical User and Password Interface, password files
- **Authorization**
 - What access do you have?
 - Group files
- **Authentication Types (Not secure without SSL)**
 - Auth_basic or Auth_digest (digest hides password)

Authentication/Authorization Overhaul

Authentication Provider

- mod_authn_alias
- mod_authn_anon
- mod_authn_dbd (new)
- mod_authn_dbm
- mod_authn_default
- mod_authn_file
- mod_authnz_ldap (new)

Authorization Provider


- mod_authnz_ldap (new)
- mod_authz_dbm
- mod_authz_default
- mod_authz_groupfile
- mod_authz_owner
- mod_authz_user

Example LDAP Authorization/Authentication

In `httpd.conf`:

```
...  
<Directory /usr/local/apache2/htdocs>  
AuthType Basic  
AuthName "Restricted Area"  
AuthBasicProvider Idap  
AuthLDAPUrl Idap://ldapservers.com/o=em?cn STARTTLS  
Require Idap-group cn=GroupName,o=em  
AuthLDAPGroupAttribute MemberName  
</Directory>  
...
```

Ensure Cipher Selected
takes advantage of
Hardware Cryptography
on z/TPF



mod_proxy

In httpd.conf:

...

ProxyRequests On

<Proxy *>

Order deny,allow

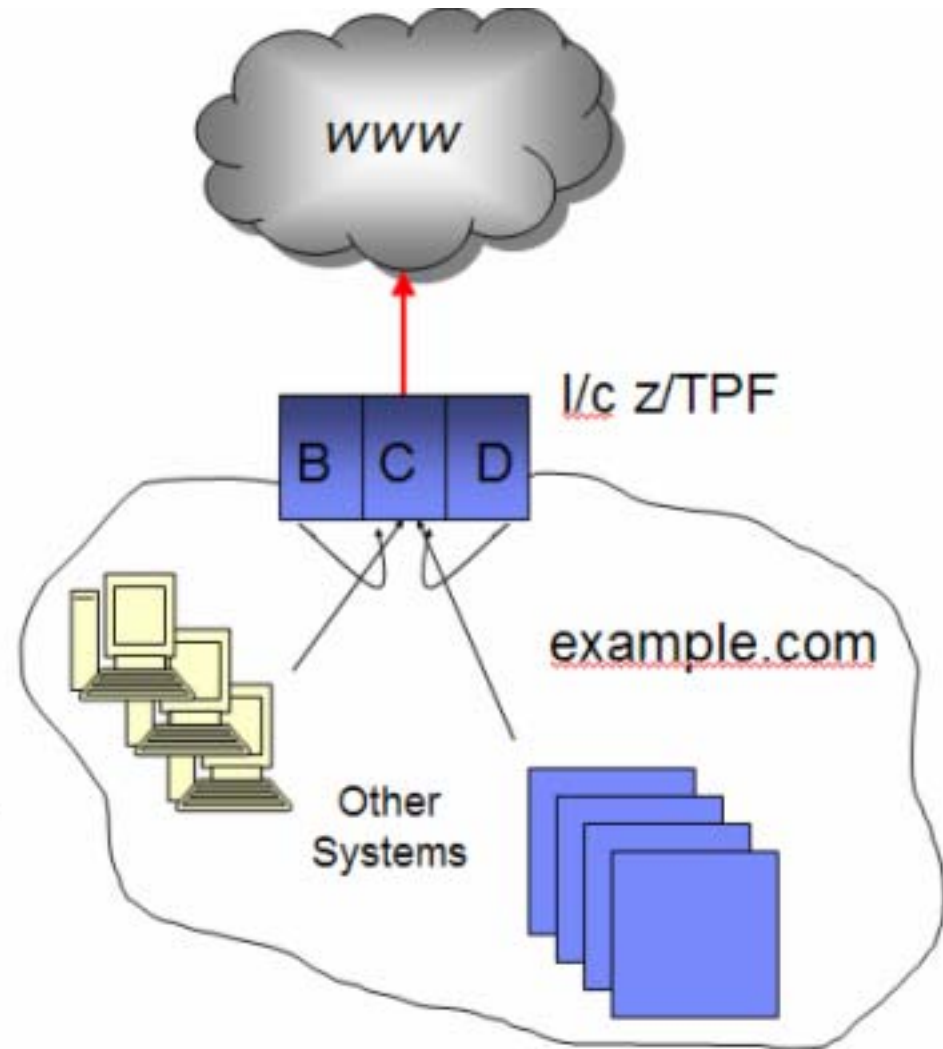
Deny from all

Allow from example.com

</Proxy>

...

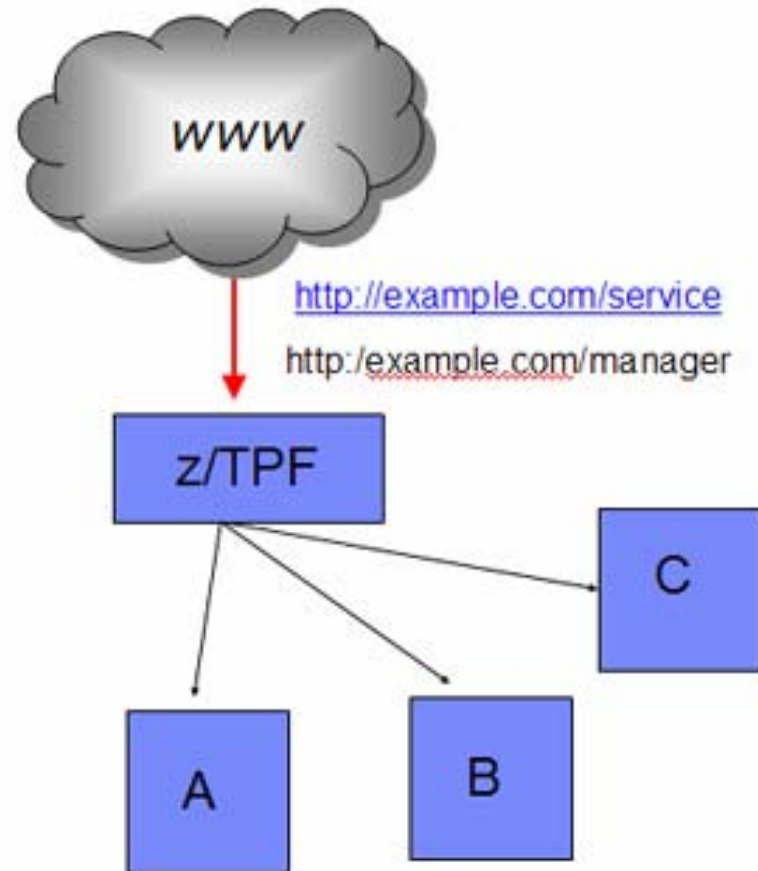
To use SSL with
Proxies:
SSLProxyEngine On
SSLProxyCipherSuite



```
mod_proxy_balancer
```

in httpd.conf:

```
<Location /service>  
ProxyPass balancer://mycluster/  
</Location>  
<Proxy balancer://mycluster> BalanceMember  
http://A.example.com/  
BalanceMember http://B.example.com/  
BalanceMember http://C.example.com/  
</Proxy>  
<Location /manager>  
SetHandler balancer-manager  
CharsetSourceEnc IBM-1047  
CharsetDefault ISO-8859-1  
</Location>  
...
```

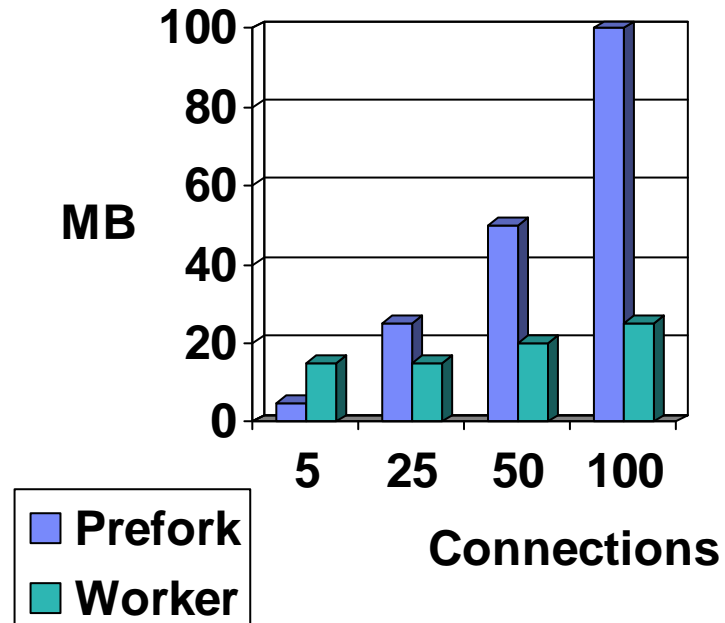


Performance

- **Apache v2.2.9 comparable to Apache 1.3**
- **Path length of ~100k for one 500 byte Web Service request**
- **Prefork and Worker models have comparable path lengths**
- **Worker is more efficient with memory because it takes advantage of threads**

Memory Utilization

(with a pre-allocated of 64k)



Possible Apache uses for z/TPF

- **Web Service Transport (Service Provider)**
- **Non web service access to your z/TPF system via CGI scripting**
- **Proxy'ing**
 - With the possibility of using filters

We are sold! How to get started...

- **z/TPF Apache distribution model change, no longer retrieved from Apache.org**
 - Everything can be accessed from:
 - http://www-01.ibm.com/software/http/tpf/pages/Ztpftech_details.htm
 - z/TPF APARs needed for Apache v2.2.9: PJ34337, PJ34514
 - mod_tpf_soap currently distributed with Apache v2.2.9
- **Follow README for instructions on...**
 - Configuring and Building (over 70 supported modules!)
 - Setting up Online (httpd.conf, zinet add, etc.)
 - And for examples, restrictions, and other considerations.

Migration/Co-existence

- **Apache v1.3 can coexist with Apache v2.2.9**
 - Need to ensure there is a unique IP address and port combination for each server.
- **Converting Apache v1.3 over to Apache v2.2.9**
 - Several Directives in httpd.conf have been made obsolete from v1.3 to v2.2.9
 - <http://httpd.apache.org/docs/2.2/upgrading.html>
 - User written modules written for Apache v1.3 will need to be investigated and updated to work with Apache v2.2.9

Questions or Comments?

Trademarks

- **IBM is a trademark of International Business Machines Corporation in the United States, other countries, or both.**
- **Other company, product, or service names may be trademarks or service marks of others.**
- **Notes**
- **Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.**
- **All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.**
- **This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.**
- **All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.**
- **Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.**
- **Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.**
- **This presentation and the claims outlined in it were reviewed for compliance with US law. Adaptations of these claims for use in other geographies must be reviewed by the local country counsel for compliance with local laws.**