IBM Software Group

IBM HTTP Server 及插件性能调整指南

杨昱球 (youngy@us.ibm.com), Yu-Chiou Young

日期 : 2014 年十月十七日

内容提要：IHS 及插件性能调整

- 插件性能调整
  - 主要参考网站
    - http://www-01.ibm.com/support/docview.wss?uid=swg21318463
    - http://www-01.ibm.com/support/docview.wss?uid=swg21450051

- IHS 性能调整
  - 主要参考网站
    - http://publib.boulder.ibm.com/httpserv/ihsdiag/ihs_performance.html
    - http://publib.boulder.ibm.com/httpserv/ihsdiag/unix_index.html
    - http://www-01.ibm.com/support/docview.wss?uid=swg21167658

插件性能建议

- **Web 服务器插件**
  - 各种计时器
  - **SSL卸载**
  - **ESI缓存**
  - 连接数
  - 多进程的影响
  - 负载均衡
  - 其他设置

各种计时器

- ConnectTimeout
- ServerIOTimeout
- ServerIOTimeoutRetry
- RefreshInterval
- RetryInterval
- PM94198
  - 在 Apache 或 IBM HTTP Server 中设置的环境变量
    - websphere-serveriotimeout
    - websphere-serveriotimeoutretry
    - websphere-shorten-handshake

ConnectTimeout

- 决定连接上应用程序服务器最长会等待多久
  - 五秒的时间通常足够了
  - 长超时可能在大型集群不利
    - 假使集群有十二名成员。半数已关闭进行维护，将可能长达 6×5= 30 秒延迟
    - 考虑删除 plugin-cfg.xml 中的服务器，而不是关闭服务器

ServerIOTimeout

- 确定插件该等待多久从应用服务器回的一个响应
  - 应足够长，以允许对应用服务器运行时间最长的请求
  - 大型集群的重试可能会加长延迟
  - 默认值根据版本而不同
  - 0 – 永不超时
    - 正常情况下，不建议如此设置
  - 负值
    - 标记 WAS 服务器停机
  - 正值
    - 不标记 WAS 服务器停机

ServerIOTimeoutRetry (PM70559)

- 如果 ServerIOTimeout 超时，插件重试该请求。本设置限制重试的次数
  - -1 （默认值）
    - 最多可以到集群成员数加一
  - 0
    - 不重试
  - N
    - 指定实际重试次数

RefreshInterval

- 插件多久检查 plugin-cfg.xml 是否改变
  - plugin-cfg.xml
    - Web 服务器子进程需要能 stat 它
  - 用一个大的 plugin-cfg.xml 时，频繁变动，能导致性能问题
  - 60 秒是默认值
  - -1: 停止插件检查 plugin-cfg.xml 是否改变

RetryInterval

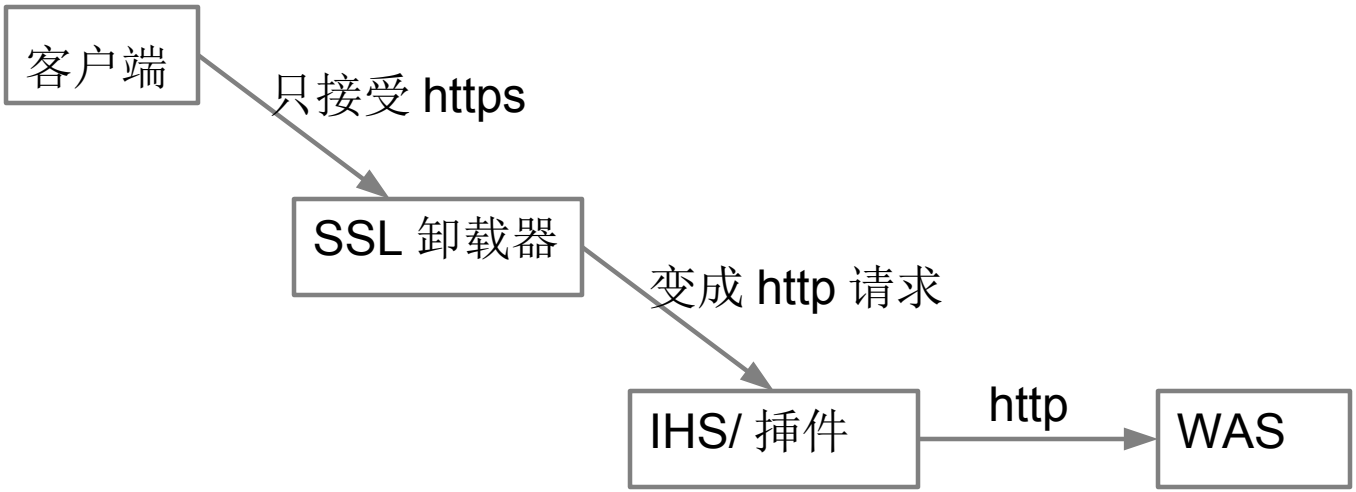
- 何时插件将重试被标记停机的服务器
  - N 秒（ 60 秒是默认值）
    - 太小的值可能会导致频繁长时间响应
    - 过长可能会延迟服务器被标记运作
    - 取决于服务器之所以被标记停机的原因

PM94198

- 介紹新的 Apache 或 IBM HTTP Server 环境变量基于 url 值，优先于 plugin-cfg.xml 内的设置
  - Websphere-serveriotimeout
  - Websphere-serveriotimeoutretry
  - Websphere-shorten-handshake
    - SetEnvIf Request_URI "\.jsp$" websphere-serveriotimeout=10
    - SetEnvIf Request_URI "\.jsp$" websphere-serveriotimeoutretry=-1
    - SetEnvIf Request_URI "\.jsp$" websphere-shorten-handshake=1
    - 7.0.0.31，8.0.0.8，8.5.5.2

解除处理 SSL 的负担

在 Web 服务器前解除处理 SSL 的负担



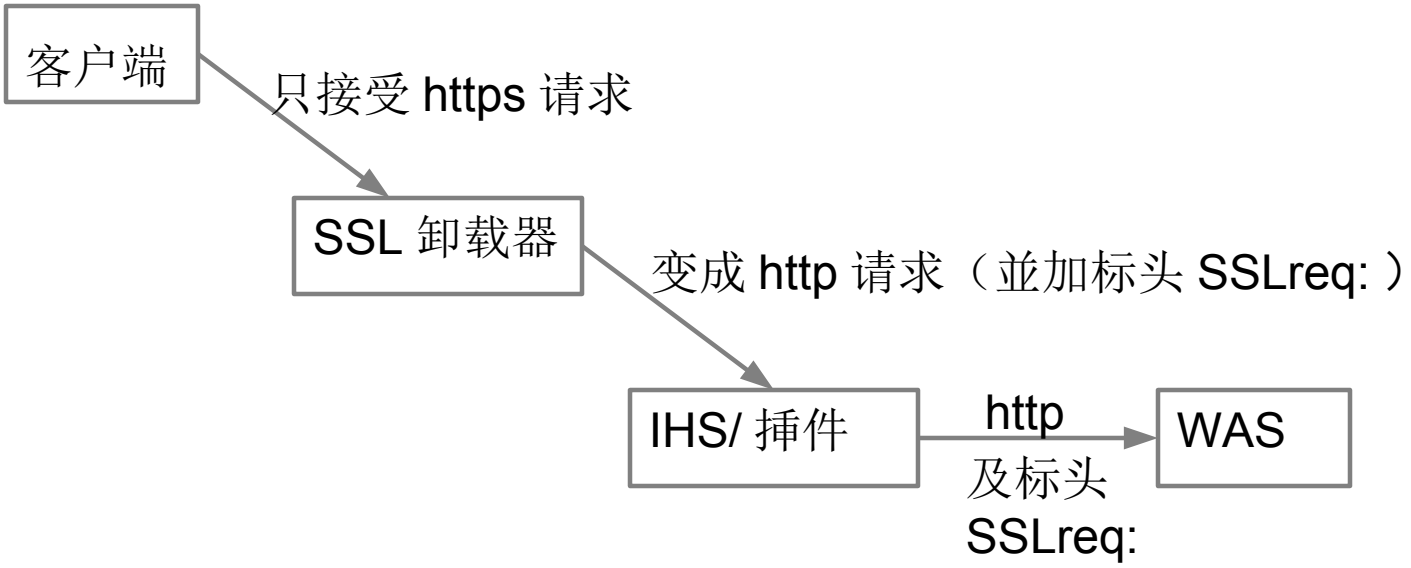
应用程序将返回一个 HTTP 302 状态代码
问题：怎么知道响应 Location: 要用 https://...
如果响应 Location: 是用 http://... ，那么下一个请求会失败

解除处理 SSL 的负担（续）

- 解除 Web 服务器 SSL 的负担
  - HTTPSIndicatorHeader
    - Web 容器属性
    - 其值为一独特的 HTTP 标头
    - 通常由在 Web 服务器之前的 SSL 卸载器设置该 HTTP 标头
    - 如果 SSL 卸载器没有此项功能， IHS 可设置此 HTTP 标头
      - 加载 mod_headers
      - 设置 RequestHeader

HTTPSIndicatorHeader

假设 Web 容器配置 HTTPSIndicatorHeader 值为 SSLreq



WAS 处理 http 请求时，见到标头 SSLreq:
便知原来客户端是 https 请求。
当回 HTTP 302 状态代码时，则知道响应 Location:
要用 https://...

插件的 SSL 处理

- 解除插件 SSL 负担
  - 处理 Web 服务器和应用服务器之间的通信
    - 只有 HTTP 传输，没有 HTTPS 传输
    - GSKit 的错误强制解除插件 SSL 负担 - 在插件预置时，plugin-key.kdb
      - 密码错误
      - 个人证书已过期
      - 8.5.5 后插件改变了行为 （ PM85452 ）
        - UseInsecure true

插件的 SSL 处理（续）

- 插件预置后的 GSKit 错误
  - SSL 握手错误 – HTTP 500 响应码
    - 证书错误
    - 密码不被允许
    - 缺少签名者证书
  - 成功的 SSL 握手
    - 安全级别 – 更高的安全级别，更多的资源销耗
    - 相互验证

插件的 SSL 处理（续）

- PK78456
  - SSLConsolidate (true 是默认值)
    - 在多个集群的环境使用
    - 共享 GSKit 环境
    - 7.0.0.3 及更高
      - 6.1.0.23
  - 也加了 SSLPKCSDriver 和
  - SSLPKCSPassword

ESI 缓存

- ESIEnable
  - True 或 False，True 是默认值
- ESIMaxCacheSize
  - 以一千字节(KB)为单位的整数
  - 默认值是1024
  - 每个进程一个高速缓存
    - 用较少的进程，缓存的利用更有效率。 因此权衡与多进程的性能增益
- ESICacheidFull （PM48820）
  - 将主机名添加到缓存ID, 默认值是 false
- ESIInvalidationMonitor (false 是默认值)
- ESIEnableToPassCookies (false 是默认值)

连接

- MaxConnections
  - 0，-1 (-1 是默认值)
    - 插件不设极限
    - 由应用服务器控制
  - N
    - 允许尚未完成的连接数
      - 一个申请，如果插件已经为它打开到应用服务器的连接，但还没有收到响应，这个连接就是尚未完成的连接
      - 各个进程
      - 插件很难控制

连接（续）

- 持久性连接 （ Web 容器）
  - 由应用服务器设置
    - Web 容器传输链
      - 使用持久（保持活动状态）连接复选框
  - ConnectionTTL （ PM76420 ）
    - Plugin_PersistTimeOut_Reduction 自定义属性
    - PM76420 – 7.0.0.29，8.0.0.6，8.5.0.2
    - 何时插件关闭空闲的套接
    - 默认值是廿八秒

多个进程

- 插件为每个进程有独立的缓存
- 插件为每个进程对每一个属性有个单独的计数器
- 崩溃只会影响一个进程
- 使负载平衡更复杂
- 权衡对 Web 服务器的性能和可靠性

负载平衡

- LoadBalance
  - Random
    - 大型群集通常用它更好
  - Round Robin
  - IgnoreAffinityRequests （默认值是 false, 8.5 以后）
  - 使用 LogLevel=” Stats” 来检查
  - 平衡非关联性的请求
    - 如果是个关联性的请求（例如有 JSESSIONID cookie ），则插件处理时不做平衡运算

其他设置

- LogLevel
  - Trace – 非常冗长，除非用于除错应避免
    - 在故障排除以后重新设置回到 Error
    - 启动新的记录档
  - Error
    - 默认值
- PostBufferSize
  - 当值为 0 时 – 请求不可能再试

IHS 性能调整指南

1. 启用时即应关注的调整
2. 配置变化对性能产生的影响
3. 调整 SSL 注意事项
4. 该避免的配置功能
5. 网络和操作系统相关的调整考虑事项

启用时即应关注的调整

- 计算最大同时连接数
- SSL- 加密算法排序
- Sendfile – 可能会增加 CPU 的占用率
- AIX - MALLOCMULTIHEAP 设置
- 只有部份 Windows/AIX 支持 FRCA （快速响应缓存加速器），或曰 AFPA(先进的快速路径架构)

决定最大同时连接数

- Unix 操作系统
  - 一个单线程的进程 , 启动一个或多个多线程的子进程
  - 相关的配置指令 – StartServer, ServerLimit, ThreadsPerChild ThreadLimit, MaxClients, MaxSpareThreads, MinSpareThreads
  - ThreadLimit 和 ServerLimit 必须配置在其他指令之前
  - ThreadsPerChild 值越大 (意即进程越少) 导致更少的专用 Web 容器线程用來处理 WebSphere 插件废止 ESI 的功能。
  - 在负载很重的 SSL 服务器上增加 ThreadsPerChild 过高，可能招致更多 CPU 和传送率的问题。
  - 内存记憶的约束 – 每个进程的固定内存销耗

决定最大同时连接数（续）

Windows 操作系统

- 在高峰负荷期间最大同时连接数的 125%
- Windows 操作系统中， IHS 是 32 位应用程序 .
  - 单一的多线程子进程
  - ThreadsPerChild – 建议不超过 2000
  - ThreadLimit – 与 ThreadsPerChild 同值 .
  - 提高 ThreadsPerChild 增加子进程崩溃的风险
  - 如用 mod_mem_cache 或是 Rewrite 指令则有更严格的上限

决定最大同时连接数（续）

- 配置 mod_status 或者 mod_mpmstats 决定最大同时连接数
  - mod_status: 给出了当前正在处理的请求总数和总闲散线程数
  - mod_mpmstats: 给出了线程的分布和状态
    - 有助于优化 MaxClient,
    - 可以有助于设置一个适合的 KeepAliveTimeout
    - 可配置的扫描间隔（ ReportInterval ）可帮助设置最佳 MaxClient
- netstat 命令可以用来确定客户机和 IHS 之间的 TCP 连接状态。

配置变化对性能产生的影响

甲 > 设置高 ThreadsPerChild 值的影响

- 较低的内存使用。
- 设置极高可能导致地址空间限制
- 更好地共享“标记 WAS 服务器停机”的 信息
- ESI invalidation servlet / Web 容器线程更有效率
- 处理 SSL 时，会导致较高的 CPU 占用率
- 在旧的 Linux，会导致高 CPU 占用率
- 此外 , RewriteMap, mod_mem_cache, mod_ibm_ldap, mod_ext_filter 会有影响

配置变化对性能产生的影响（续）

乙 > MaxClients

- 增加 Maxclient 设置理当增加 MaxSpareThreads
- 否则，当负载变化量还相对较小时，将消耗 CPU 來终止并创建子进程

丙 > ExtendedStatus

- 当这设置为 On， Web 服务器的 CPU 使用率可能会增加一个百分点。

调整 SSL 注意事项

- 选择在有序列表的第一个支持的密码
- IHS 更倾向于使用 AES 和 RC4 加密算法而非计算昂贵的三重 DES(3DES)
- SSLCipherSpec 指令的顺序决定那个密码算法优先选用

IHS 7.0 及以前版本 SSL 的加密配置

```
<VirtualHost *:443>
  SSLEnable
  Keyfile keyfile.kdb

  ## SSLv3 128 bit Ciphers
  SSLCipherSpec SSL_RSA_WITH_RC4_128_MD5
  SSLCipherSpec SSL_RSA_WITH_RC4_128_SHA

  ## FIPS approved SSLV3 and TLSv1 128 bit AES Cipher
  SSLCipherSpec TLS_RSA_WITH_AES_128_CBC_SHA

  ## FIPS approved SSLV3 and TLSv1 256 bit AES Cipher
  SSLCipherSpec TLS_RSA_WITH_AES_256_CBC_SHA

  ## Triple DES 168 bit Ciphers
  ## These can still be used, but only if the client does
  ## not support any of the ciphers listed above.
  SSLCipherSpec SSL_RSA_WITH_3DES_EDE_CBC_SHA

  ## The following block enables SSLv2. Excluding it in the presence of
  ## the SSLv3 configuration above disables SSLv2 support.
  ## Uncomment to enable SSLv2 (with 128 bit Ciphers)
  #SSLCipherSpec SSL_RC4_128_WITH_MD5
  #SSLCipherSpec SSL_RC4_128_WITH_SHA
  #SSLCipherSpec SSL_DES_192_EDE3_CBC_WITH_MD5

</VirtualHost>
```

IHS 8.0 及以后版本 SSLCipherSpec

- 支持新的密码和 SSLCipherSpec 指令的新语法。
- 不同版本的 TLS 协议可支持不同的密码集
- 默认情况下， SSLv2 处于禁用状态
- 默认情况下，它禁用不夠強的密码
- TLSv12 默认密码 : TLS_RSA_WITH_AES_128_GCM_SHA256
  TLS_RSA_WITH_AES_256_GCM_SHA384
  TLS_RSA_WITH_AES_128_CBC_SHA256
  TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA
  TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
- SSLv3, TLSv10, TLSv11 默认密码 : TLS_RSA_WITH_AES_128_CBC_SHA
  TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_RC4_128_SHA
  TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_3DES_EDE_CBC_SHA

SSL-LogFormat

- LogFormat 指令 :

LogFormat "%h %l %u %t \"%r\" %>s %b \"SSL=**%{HTTPS}e**\" \"**%{HTTPS_CIPHER}e**\" \"**%{HTTPS_KEYSIZE}e**\" \"**%{HTTPS_SECRETKEYSIZE}e**\" \"**%{SSL_PROTOCOL_VERSION}e**\"" ssl-var

CustomLog logs/ssl_cipher.log ssl_var

- ssl_cipher.log:

127.0.0.1 - - [16/Oct/2014:14:57:29 -0400] "GET / HTTP/1.1" 200 3598 "SSL=ON" "TLS_RSA_WITH_AES_128_CBC_SHA256" "128" "128" "TLSV1.2"

SSL- 证书大小

- 每一个密钥大小增加了一倍会消耗四到八倍更多的 CPU
- 最近， IT 界的标准从 1024 位证书变到 2048 位的证书。
- SSL 主要的计算资源是耗在建立新的 SSL 会话期；2048 位的证书用得更多。
- 配置 keep-alive，重覆使用 SSL 会话期，对增进性能有帮助。

与 SSL 连接有关的性能调整

- SSL CPU 占用率与 ThreadsPerChild 成正比
- MALLOCMULTIHEAP 设置（在 AIX IHSRoot/bin/envvars ）
- 使用加密加速器，评估利弊。
- 在有配置 SSL 的 IHS 中配置 HTTP keep-alive 比没有配置 SSL 的 IHS 更能感到性能的增进。 一个小值的 KeepAliveTimeout 要比设置 KeepAlive OFF 好。
- 创建共享密钥给所有负载平衡的 SSL 连接和后续 SSL 连接重用已有的 SSL 会话期能减少在 SSL 握手时为每一个新的连接所引起的 CPU 销耗，。
- 在后续 SSL 连接重用已有的 SSL 会话期之外，有執着性的会话期也可以避免为每一个新的客户端和 Web 服务器之间连接所要创建的共享密钥。
- 在 SSL 握手过程中创建共享密钥很费 CPU

该避免的配置功能

- HostnameLookups On
- IdentityCheck On (7.0 版或更高版本不支持此指令)
- mod_mime_magic
- ContentDigest On
- 配置 MaxRequessPerChild 到不是零的值
- .htaccess 文件
- 详细的记录
- 不用 Options FollowSymLinks

其他性能改善方面的考虑

- 网络调整 - 提高 TCP 接收缓冲区的默认大小
  ReceiveBufferSize
- 调整操作系统 - http://www-01.ibm.com/support/knowledgecenter/SSEQTP_8.5.5/com.ibm.websphere.base.doc/ae/tprf_tuneopsys.html?lang=en
- AIX 启动慢，或响应的时间缓慢。关闭 IPv6 查找
  NSORDER=local4,bind4
  export NSORDER
- WebSphere 插件配置更新以后，重新加载配置文件会造成高 CPU
- 频繁对磁盘进行写操作会降低 IO 性能，建议在 httpd.conf 中添加以下内容
  BufferedLogs on

参考网页

- http://publib.boulder.ibm.com/httpserv/ihsdiag/
- http://publib.boulder.ibm.com/httpserv/ihsdiag/unix_index.html
- http://www-01.ibm.com/software/webservers/appserv/was/library/index.html

最新消息网页

- CVE-2014-3566 (POODLE) 漏洞
  http://www-01.ibm.com/support/docview.wss?uid=swg21687172

- 问专家讨论会：插件配置
  http://www.ibm.com/software/websphere/support/TE/techex_O059108W22994E91.html
  暂定时间：北京时间十月廿三日下午十一时

WebSphere 产品其他的信息资源

- Learn about upcoming WebSphere Support Technical Exchange webcasts, and access previously recorded presentations at:
  http://www.ibm.com/software/websphere/support/supp_tech.html
- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at:
  http://www.ibm.com/developerworks/websphere/community/
- Join the Global WebSphere Community:
  http://www.websphereusergroup.org
- Access key product show-me demos and tutorials by visiting IBM Education Assistant:
  http://www.ibm.com/software/info/education/assistant
- View a webcast replay with step-by-step instructions for using the Service Request (SR) tool for submitting problems electronically:
  http://www.ibm.com/software/websphere/support/d2w.html
- Sign up to receive weekly technical My Notifications emails:
  http://www.ibm.com/software/support/einfo.html

联系我们

1. 发邮件到 **Smart support: swsupt@cn.ibm.com**

2. IBM 软件技术支持 http://weibo.com/IBMSupport

问答时间