BES 宝兰德 BESSYSTEM

毕昇JDK在保兰德产品BES上的应用

北京宝兰德软件股份有限公司

KAE加速引擎与BES中间件适配

BES Application Server中间件(下文简称BES)系列是宝兰德公司推出的企业级JavaEE规范兼容中间件，在电信、金融、政府、能源众多行业获得大规模部署使用，是目前中国移动目前唯一在多省核心业务支撑系统大规模部署使用的国产商用中间件。

KAE加解密是鲲鹏加速引擎的加解密模块，使用鲲鹏硬加速模块实现RSA/SM3/SM4/DH/MD5/AES算法，结合无损用户态驱动框架，提供高性能对称加解密、非对称加解密算法能力，兼容OpenSSL 1.1.1a及其之后版本，支持同步和异步机制。

KAE加速引擎与BES中间件适配

1、BES中间件本身提供基于JSSE以及OpenSSL的https加密通信。

2、BES中间件如何与KAE引擎适配，来提升https处理性能?

KAE加速引擎与BES中间件适配

方案1：

通过jni本地调用方式，直接使用kae engine替换默认的openssl engine，完成https握手

方案2：

通过JCE扩展机制将KAE加解密算法直接集成到bisheng jdk，以Provider形式提供给上层中间件调用。

此方案对中间件来说无需任何改动。

KAE加速引擎与BES中间件适配

测试环境：

服务器类型	TaiShan 200服务器2280裸金属服务器	数量	2台	硬件配置	3*4TB SATA HDD + 1*960GB SAS SSD
内存	16*16GB	CPU	64 cores,2.6 GHz	网卡	1*4*GE

软件	版本	说明
BES	BES9.5.2	
OS	openEuler release 20.03(LTS)	所有环境均使用
JDK	BishengJDKOpenJDK 64-Bit Server VM Bisheng (build 11.0.8+13, mixed mode)openssl1.1.1a	所有环境就使用
KAE	1.3.10	
JMeter	5.4	

KAE加速引擎与BES中间件适配

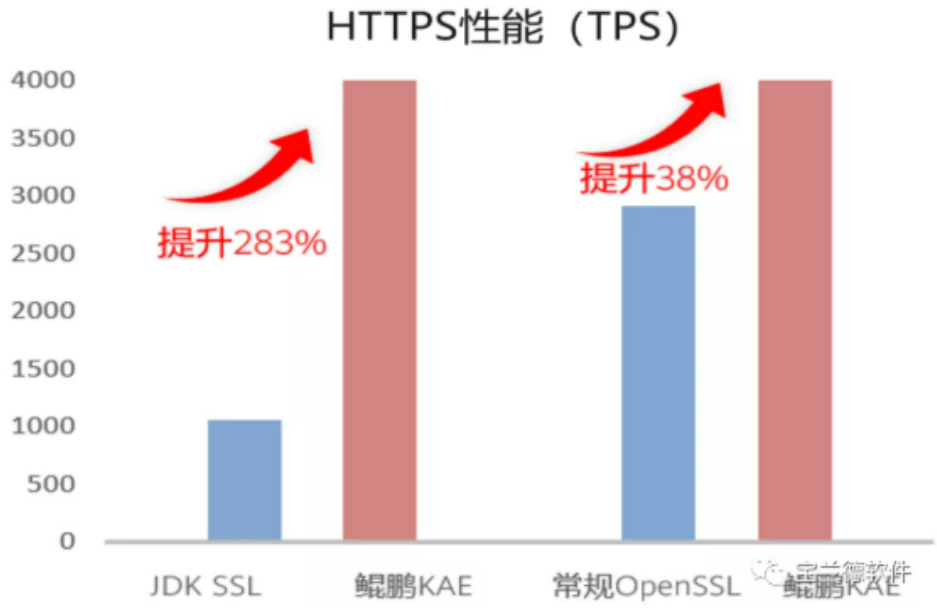
测试结果：

启用SSL session cache

服务器	user	TPS	响应时间	kae性能提升比例
KAE	400	4496	0.091	
	400	4408	0.091	
	400	4452	0.091	
非KAE	400	4445	0.091	
	400	4431	0.091	
	400	4438	0.091	0.32%
JDK	400	4021	0.098	
	400	3997	0.099	
	400	4009	0.0985	11.05%

禁用SSL session cache

服务器	user	TPS	响应时间	kae性能提升比例
KAE	400	4057	0.098	
	400	4001	0.099	
	400	4029	0.0985	
非KAE	400	2938	0.135	
	400	2891	0.137	
	400	2914.5	0.136	38.24%
JDK	400	1055	0.188	
	400	1047	0.188	
	400	1051	0.188	283.35%



KAE加速引擎与BES中间件适配

测试过程中一些问题：

1、openssl长连接和短链接

2、jsse长连接和短链接

3、ssl session缓存

KAE加速引擎与BES中间件适配

bishengjdk8中KAEProvider实现

https://gitee.com/openeuler/bishengjdk-8/wikis/KAE%20Provider%E7%94%A8%E6%88%B7%E4%BD%BF%E7%94%A8%E6%89%8B%E5%86%8C?sort_id=3736254

算法支持

KAE Provider 已经支持的算法列表：

算法	说明
摘要算法	包括MD5、SHA256、SHA384、SM3
对称加密算法AES	支持ECB、CBC、CTR、GCM模式
对称加密算法SM4	包括ECB、CBC、CTR、OFB模式
HMac	包括HmacMD5、HmacSHA1、HmacSHA224、HmacSHA256、HmacSHA384、HmacSHA51
非对称加解密算法RSA	支持512、1024、2048、3072、4096位秘钥大小
DH	包括DHKeyPairGenerator和DHKeyAgreement，支持512、1024、2048、3072、4096位秘钥
ECDH	包括ECKeyPairGenerator和ECDHKeyAgreement，支持曲线secp224r1、prime256v1、secp384r1、secp521r1
RSA签名	包括RSASignature和RSAPSSSignature，私钥只支持RSAPrivateCrtKey

使用KAE Provider

KAE Provider在Bisheng JDK中默认未启用， 可以通过如下方式启用KAE Provider:

- 方式 1： 使用**Security API** 添加KAE Provider ，并设置其优先级。

  例：设置KAE Provider为最高优先级

```
Security.insertProviderAt(new KAEProvider(), 1);
```

- 方式 2：修改jre/lib/security/java.security文件，添加KAE Provider，并设置其优先级。

  例: 设置KAE Provider为最高优先级

```
security.provider.1=org.openeuler.security.openssl.KAEProvider
security.provider.2=sun.security.provider.Sun
security.provider.3=sun.security.rsa.SunRsaSign
security.provider.4=sun.security.ec.SunEC
security.provider.5=com.sun.net.ssl.internal.ssl.Provider
security.provider.6=com.sun.crypto.provider.SunJCE
security.provider.7=sun.security.jgss.SunProvider
security.provider.8=com.sun.security.sasl.Provider
security.provider.9=org.jcp.xml.dsig.internal.dom.XMLDSigRI
security.provider.10=sun.security.smartcardio.SunPCSC
security.provider.11=sun.security.mscapi.SunMSCAPI
```

为何选择bishengjdk

案例

```
tcp    0    0 0.0.0.0:18080          0.0.0.0:*              LISTEN      off (0.00/0/0)
tcp    148  0 192.168.20.13:18080    100.116.9.123:7930     CLOSE_WAIT  off (0.00/0/0)
tcp    148  0 192.168.20.13:18080    100.116.9.123:34736    CLOSE_WAIT  off (0.00/0/0)
tcp    148  0 192.168.20.13:18080    100.116.9.123:59070    CLOSE_WAIT  off (0.00/0/0)
tcp    148  0 192.168.20.13:18080    100.116.9.123:6225     CLOSE_WAIT  off (0.00/0/0)
tcp    148  0 192.168.20.13:18080    100.116.9.123:24736    CLOSE_WAIT  off (0.00/0/0)
tcp    148  0 192.168.20.13:18080    100.116.9.123:44570    CLOSE_WAIT  off (0.00/0/0)
tcp    148  0 192.168.20.13:18080    100.116.9.123:31861    CLOSE_WAIT  off (0.00/0/0)
tcp    148  0 192.168.20.13:18080    100.116.9.123:52440    CLOSE_WAIT  off (0.00/0/0)
tcp    148  0 192.168.20.13:18080    100.116.9.123:26919    CLOSE_WAIT  off (0.00/0/0)
```

```
##|2021-09-17 20:38:19.142|SEVERE|web|_ThreadID=56;_ThreadName=SelectorReaderThread-18080-1|
java.lang.NullPointerException
        [redacted]
        at java.lang.Thread.run(Thread.java:748)
```

```
##|2021-09-17 20:30:47.922|WARNING|web|_ThreadID=56;_ThreadName=SelectorReaderThread-18080-1|Executor rejected socket
java.util.concurrent.RejectedExecutionException: The thread pool's work queue is full after wait 5000 ms, limit: 4096
        at com.bes.enterprise.webtier.core.WorkThreadExecutor.execute(WorkThreadExecutor.java:226)
        at [redacted]
        at [redacted]
        at [redacted]
        at java.lang.Thread.run(Thread.java:748)
```

压测的应用逻辑简单

为何选择bishengjdk

环境：
OS Version: 4.19.90-20.1stable.ky10.aarch64
Architecture: aarch64
Java Home: /opt/application/jdk1.8.0_202/jre
JVM Version: 1.8.0_202-b08
JVM Vendor: Oracle Corporation
CPU： 鲲鹏920

1、经过对异常现象分析，怀疑是oracle jdk的问题
2、研发内部去复现，确定问题
3、反馈给客户现场，替换bishengjdk8，问题得到解决

其他

宝兰德联合北京鲲鹏创新中心，开展了宝兰德应用服务器软件在鲲鹏环境深度优化验证工作，采用多种技术实现了应用服务器软件方案的全栈优化，BES中间件软件通过鲲鹏Validated认证：

- 针对Bisheng JDK进行NUMA优化和参数调整，推动KAE provider在Bisheng JDK中的实现，让基于Bisheng JDK的业务应用可以轻松使用鲲鹏KAE算力
- 对中间件Session管理、负载管理等集群关键组件能力进行优化，为鲲鹏环境下业务应用提供高性能集群服务
- 针对北京海量数据技术股份有限公司的VastbaseG100数据库产品（基于openGauss内核开发）进行JDBC驱动级别的池化管理、使用连接快速回收算法和大量的Statement优化，同时增加多池管理功能，增强数据库访问效率和可靠性
- 所有产品新版本发布都需要支持openEuler平台以及bishengjdk
- 宝兰德《基于鲲鹏全栈的应用中间件解决方案》应用创新大赛获得金奖
- 在openGauss赛道，宝兰德《MySQL到openGauss迁移工具解决方案》也荣获该赛道一等奖


BES
宝兰德
BESSYSTEM