

JAVA和.NET在安全性能分析 PDF转换可能丢失图片或格式，
建议阅读原文

https://www.100test.com/kao_ti2020/285/2021_2022_JAVA_E5_92_8CNE_c104_285127.htm 两个平台的配置都是通过XML或纯文本文件，两个平台最大的区别在于处理安全配置体系的方式不同。在.NET平台，有图形接口和命令行二种方式来修改安全配置参数。Mscorcfg.msc是图形接口方式，Caspol.exe提供了命令行方式，适用于批处理或配置文本。JAVA平台只提供了图形接口的工具policytool.exe。和.NET不同的是，它的目标对象（配置文件）的名字和位置不是固定的。.NET定义了不同范围的安全配置文件：系统范围，本机范围，本用户范围。在配置有冲突时，原则上小范围的参数有优先权。JAVA和J2EE的核心配置文件都保存在固定位置，但扩展配置文件随厂家不同而不同。代码封装：检验 JAVA 和.NET的Common Library Runtime (CLR) 都实行内存安全或类型安全的保护机制，在这些平台开发的 ứng dụng的安全性也是可以检验的。他们的实现机制有很大的不同。在.NET，CLR总是执行编译好的代码，它不解释代码。但是在中间语言（IL）被编译之前，编译器会有验证和检验的步骤。第一步是检查文件的结构和代码完整性；第二步包括一些扩展的检查，内存安全、堆栈跟踪、数据流分析、类型检查等。在运行阶段，由VES (Virtual Execution System) 来负责安全性检查和出错意外情况处理。在JAVA平台，JAVA虚拟机（JVM）负责类的载入、链接、检验和执行。对于已经编译和优化的代码，JVM也用二个无条件调用堆栈来保留最初的字节代码信息。小结：和.NET不同，JVM的默认设置是不检验本地代码。

另外，JVM保留最初的字节代码供运行时检查，而.NET把静态分析和运行时插入检验代码相结合。代码封装：应用隔离在.NET，域隔离建立在内存安全机制的基础上，不同的域不能直接访问彼此的地址空间，只能通过.NET远程通信机制访问。在JAVA平台，应用隔离是通过ClassLoaders和ProtectionDomains相结合来实现的，安全类加载是JVM安全机制的基石。小结：.NET的AppDomains就象操作系统的进程一样，使用起来比JAVA的ProtectionDomains更直接、容易一些。代码封装：语言特征两个平台基本上差不多，.NET在灵活性上稍微好一点。总结：JAVA在安全配置上有较多的优势，.NET在代码封装的选择性和易用性好一些。

第二部分 加密和通信

加密法：概论

.NET的加密法主要基于CryptoAPI和相关扩展。大多数有关加密的类都在System.security.Cryptography, X509Certificates和XML中。 .NET利用基于流的模型来完成加密传输，所有的算法都被默认为最高的安全级别。 .NET也允许用户自己在machine.config中定义自己的算法。 JAVA平台的加密算法分二个部分：Java Cryptography Architecture (JCA) 和 Java Cryptography Extension (JCE)。 JCE的出口受到有关法律的限制。如果要使用用户自己的加密算法，必须得到认证机构（SUN或IBM）的认证。

加密法：算法

.NET主要提供了下面几大类加密算法：非对称算法、HASH算法、对称算法、随机数生成法。 JAVA提供的加密算法更多，但是较少第三方厂商可以在JAVA中提供自己的算法。

安全通信

SSL已经是事实的传输安全的工业标准了。 JAVA和.NET都支持最新版本SSL 3.0。

安全通信：平台

.NET只在基于IIS的应用中使用SSL

来保护HTTP传输，对于非IIS应用，.NET不能保护传输中的数据。在JAVA中，JSSE（Java Secure Socket Extensions）提供了平台级的服务，保证基于TCP/IP的通信安全。除了IIS，.NET没有提供任何其它平台级的通信保护的标准方案，但是JAVA在这方面提供了全套的解决方案。安全通信：应用.NET通过WSA（Web Service Architecture）和WSE（Web Service Extension）包来提供最新的WEB服务安全保证，JAVA目前还没有提供这方面的支持。总结：在加密方法上，JAVA和.NET基本没有太大的差别；在通信保护方面，JAVA比.NET提供了更多的选择方案；但是在WEB服务安全性上，JAVA明显比.NET落后一些。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com