

SOA 第八章作业

1. 比较数据库中事务与 web 服务事务概念的异同。

数据库中的事务和 Web 服务事务是两个概念，它们在范围和应用场景上存在一些异同。

答：

1. 范围不同。数据库中的事务是指一系列数据库操作（例如插入、更新、删除等）的逻辑单元，要么全部成功执行，要么全部回滚至初始状态，以保证数据的一致性和完整性。而 Web 服务事务是指涉及多个分布式系统之间的交互的事务，包括调用不同的 Web 服务、消息传递等，确保这些操作的一致性和可靠性。

2. 应用场景和目标也有所不同。数据库事务常用于维护数据库中的数据完整性和一致性，例如在转账过程中确保金额操作的正确性。而 Web 服务事务常用于跨多个分布式系统的业务流程中，例如在线购物过程中涉及到库存管理、支付系统、物流系统等的协同操作。

3. 实现方式也有所不同。数据库事务常使用 ACID（原子性、一致性、隔离性、持久性）属性来保证操作的正确性和可靠性。而 Web 服务事务通常使用协议或框架来处理跨系统之间的事务，例如使用 WS-AtomicTransaction 协议或者 BPEL（Business Process Execution Language）等。

总结起来，数据库中的事务和 Web 服务事务在范围和应用场景上有所不同。数据库事务主要关注维护单个数据库的数据一致性和完整性，而 Web 服务事务则涉及多个分布式系统之间的交互和协作，以保证整

个业务流程的一致性和可靠性。

2. Web 服务的安全标准包括哪些内容？

答：

1. 认证和权限

通过在 SOAP 消息头中包含认证和权限信息实现。

SAML (Security Assertions Markup Language) 和 XACML (XML Access Control Markup Language) 规范可以一起实现单点登录 SSO (Single Sign-on)。

2. 机密性

通过 XML-Encryption 规范实现。

3. 完整性

通过 XML-Encryption 规范实现。

3. WS-Security 是 Web 服务安全的标准语言，请介绍在 SOAP 消息中添加用户名/密码信息，Kerberos 安全证书，X. 509 数字签名，以及为 SOAP 消息体加密的方法。

答：

1. WS-Security 在 SOAP 消息中增加用户名/密码信息。

```
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope
  xmlns:s="http://schemas.xmlsoap.org/soap/envelop"
  xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/12/secext">
  <s:Header>
    <wsse:Security>
      <!-- 用户名和密码 -->
      <wsse:UsernameToken>
        <wsse:Username>students</wsse:Username>
        <wsse:Password>software</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security>
  </s:Header>
  ...
</s:Envelope>
```

2. WS-Security 在 SOAP 消息中增加 Kerberos 安全证书。

```
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope
  xmlns:s="http://schemas.xmlsoap.org/soap/envelop"
  xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/12/secext">
  <s:Header>
    <wsse:Security>
      <!-- Kerberos 安全证书声明-->
      <wsse:BinarySecurityToken>
        ValueType="wsse:Kerberosv5ST"
        EncodingType="wsse:Base64Binary">
          XSETt...
        </wsse:BinarySecurityToken>
    </wsse:Security>
  </s:Header>
  ...
</s:Envelope>
```

3. WS-Security 在 SOAP 消息中增 X. 509 数字签名。

```
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope
  xmlns:s="http://schemas.xmlsoap.org/soap/envelop"
  xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/12/secext">
  <s:Header>
    <wsse:Security>
      <!-- X.509 安全证书凭证声明-->
      <wsse:BinarySecurityToken>
        ValueType="wsse:X509v3" wsu:Id="X509Cert"
        EncodingType="wsse:Base64Binary">
          XSETt...
        </wsse:BinarySecurityToken>
      <!-- 数字签名声明-->
      <ds:Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod>
            Algorithm="http://www.w3.org/2000/10/xml-3xc-c14N/">
          </ds:CanonicalizationMethod>
          <ds:SignatureMethod>
            Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
          </ds:SignatureMethod>
          <ds:Reference URI="MessageBody">
            <ds:DigestValue>...</ds:DigestValue>
          </ds:Reference>
          <ds:SignedValue>
            ...
          </ds:SignedValue>
          <ds:keyInfo> ... </ds:keyInfo>
        </ds:SignedInfo>
      </ds:Signature>
    </wsse:Security>
  </s:Header>
  <s:Body wsu:Id="MessageBody">
    ...
  </s:Body>
</s:Envelope>
```

4. WS-Security 为 SOAP 消息体加密。

```
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope
  xmlns:s="http://schemas.xmlsoap.org/soap/envelop"
  xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/12/secext"
  xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility"
  xmlns:ds="http://www.w3.org/2002/09/xmldsig#"
  xmlns:xenc="http://www.w3.org/2002/09/xmlenc#">
  <s:Header>
    <wsse:Security>
      <!-- 加密方法声明-->
      <xenc:EncryptionKey>
        <xenc:EncryptionMethod
          Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
        <ds:KeyInfo>
          <ds:KeyName>
            CN=Key13, C=US
          </ds:KeyName>
        </ds:KeyInfo>
        <xenc:CipherData>
          <xenc:CipherValue>
            fds7#rt...
          </xenc:CipherValue>
        </xenc:CipherData>
        <xenc:ReferenceList>
          <xenc:DataReference URI="#EncryptionMessageBody"/>
        </xenc:ReferenceList>
      </xenc:EncryptionKey>
    </wsse:Security>
  </s:Header>
  <s:Body>
    <!-- 加密声明 -->
    <xenc:EncryptedData wsu="EncryptedMessageBody">
      <xenc:EncryptedMethod
        Algorithm="http://www.w3.org/2001/04/xmlenc#triplededs-cbc"/>
      <xenc:CipherData>
        <xenc:CipherValues>
          GDSW#df...
        </xenc:CipherValues>
      </xenc:CipherData>
    </xenc:EncryptedData>
  </s:Body>
</s:Envelope>
```