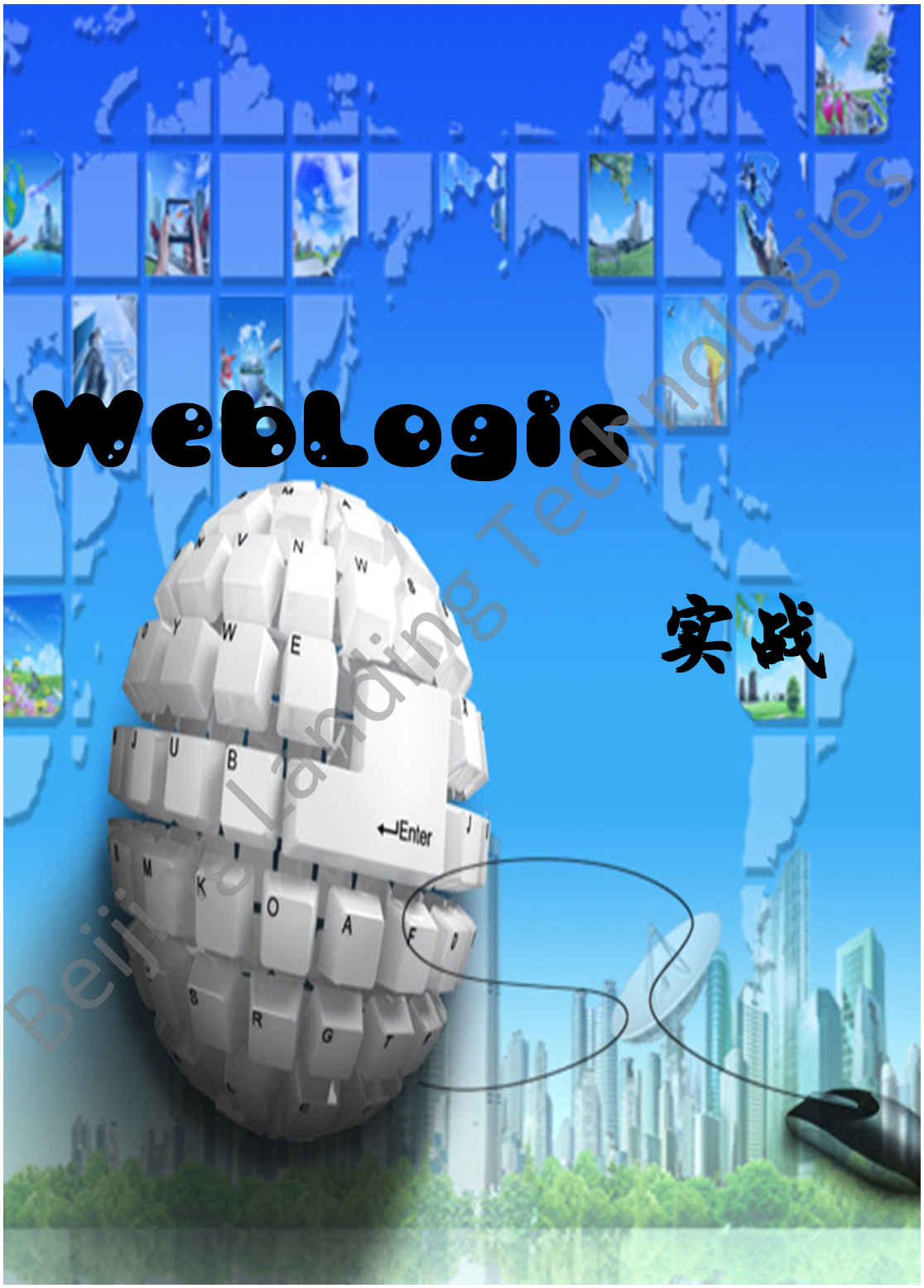
联动北方
LANDING

企业级 IT 运维宝典系列



联动北方 出品

目　录

目　录.....2

第 31 章　域信任问题故障.....3
31.1　定位域信任问题故障.....3
31.1.1　基本概念回顾.....3
31.1.2　域信任考虑事项.....3
31.1.3　域信任故障症状.....3
31.1.4　设置域 Credential.....6
31.1.4.1　配置 Credential Mappings.....6
31.1.4.2　配置 Credential Mapping Providers.....7
31.2　故障排除检查清单.....8

第 31 章 域信任问题故障

域信任，顾名思义，一般在多个 WebLogic Server 域互相之间通讯的时候会涉及，由于其设置不当引起的种种原因，也经常令人头疼和费解。

31.1 定位域信任问题故障

首先，来讨论对于域信任问题的仔细定位。让我们从域之间信任关系的基本概念开始。

31.1.1 基本概念回顾

在 WebLogic Server 域之间建立信任的目的：使一个域中的 Principal（用户）可作为另一个域中的 Principal（用户）而被接受，也就是说，一位用户登录到一个域后，将允许其对另一个域进行调用。

信任建立的要求：一个域的域 Credential 属性必须与另一个域的域 Credential 匹配。

WebLogic Server 域 Credential：缺省情况下在第一次启动域时随机生成，因此，缺省情况下每个域的域 Credential 都不相同，要在两个域之间建立信任，必须将其显式设置为相同的值，示例图如下：

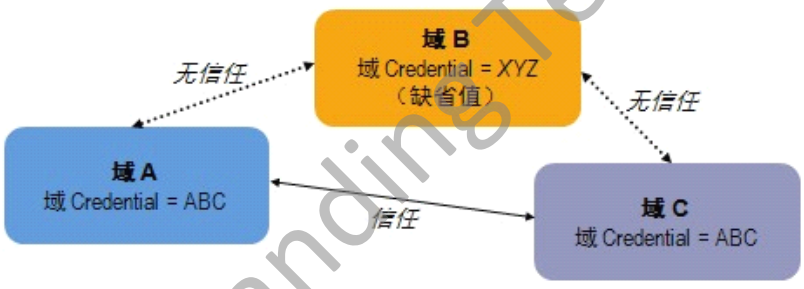


图 31-1

31.1.2 域信任考虑事项

请考虑以下域信任因素：

- 在本地域的身份验证数据库中没有定义远程用户时，将会发生授权问题；
- 一个域的某一组成员资格的已验证身份的用户将会继承所有受信任域中的相同组成员资格；
- 如果域 2 既信任域 1 又信任域 3，则域 1 和域 3 之间将隐式建立相互信任关系，并因此允许进行域间用户访问；
- 如果在一个域中扩展了 WLS User Principal 类和 WLS Group Principal 类，则在彼此信任的所有域中的 CLASSPATH 中也需要有这些自定义类。

31.1.3 域信任故障症状

出现域信任问题时，可能的故障症状包括：两个 WebLogic Server 域之间的双向通信（例如，JNDI 查找）失败；抛出安全异常(两端)；服务器日志中出现错误消息(两端)；重新启动的管理服务器无法再与已发现的(已在运行的)被管服务器连接。

如果信任失败，WebLogic 域服务器将会记录输出消息：

```
    java.lang.SecurityException: Authentication for user system denied in realm
wl_realm
    Start server side stack trace:
    java.lang.SecurityException: Authentication for user system denied in realm
wl_realm
    at weblogic.security.acl.Realm.authenticate(Realm.java:212)
    at weblogic.security.acl.Realm.getAuthenticatedName(Realm.java:233)
    at weblogic.security.acl.internal.Security.authenticate(Security.java:171)
    at weblogic.security.acl.internal.Security.verify(Security.java:95)
    at weblogic.rmi.internal.BasicServerRef.handleRequest
    (BasicServerRef.java:292)
    at weblogic.rmi.internal.BasicExecuteRequest.execute
    (BasicExecuteRequest.java:22)
    at weblogic.kernel.ExecuteThread.execute(ExecuteThread.java:140)
    at weblogic.kernel.ExecuteThread.run(ExecuteThread.java:121)
    End server side stack trace
    at weblogic.rjvm.BasicOutboundRequest.sendReceive
    (BasicOutboundRequest.java:108)
    at weblogic.rmi.cluster.ReplicaAwareRemoteRef.invoke
    (ReplicaAwareRemoteRef.java:284)
    at weblogic.rmi.cluster.ReplicaAwareRemoteRef.invoke
    (ReplicaAwareRemoteRef.java:244)
    at weblogic.jndi.internal.ServerNamingNode_811_WLStub.lookup(Unknown Source)
    at weblogic.jndi.internal.WLContextImpl.lookup(WLContextImpl.java:338)
    at . . .
```

示例 31-1

WebLogic 客户端输出示例：

```
    java.lang.SecurityException: [Security:090398]Invalid Subject:
      principals=[weblogic, Administrators]
    at weblogic.rjvm.BasicOutboundRequest.sendReceive
    (BasicOutboundRequest.java:108)
    at weblogic.rmi.cluster.ReplicaAwareRemoteRef.invoke
    (ReplicaAwareRemoteRef.java:284)
    at weblogic.rmi.cluster.ReplicaAwareRemoteRef.invoke
    (ReplicaAwareRemoteRef.java:244)
    at weblogic.jndi.internal.ServerNamingNode_812_WLStub.lookup(Unknown Source)
    at weblogic.jndi.internal.WLContextImpl.lookup(WLContextImpl.java:343)
    at weblogic.jndi.internal.WLContextImpl.lookup(WLContextImpl.java:336)
    at javax.naming.InitialContext.lookup(InitialContext.java:347)
    at bea.SourceServlet.m1(SourceServlet.java:50)
```

```
    at bea.SourceServlet.doGet(SourceServlet.java:26)
    at  javax.servlet.http.HttpServlet.service(HttpServlet.java:740)
    at  javax.servlet.http.HttpServlet.service(HttpServlet.java:853)
    at weblogic.servlet.internal.ServletStubImpl$ServletInvocationAction.run
    (ServletStubImpl.java:971)
    at weblogic.security.acl.internal.AuthenticatedSubject.doAs
    (AuthenticatedSubject.java:317)
    at weblogic.security.service.SecurityManager.runAs
    (SecurityManager.java:118)
    at weblogic.servlet.internal.ServletStubImpl.invokeServlet
    (ServletStubImpl.java:400)
    at . . .
```

示例 31-2

如果在一个域内建立信任如果遇到故障，也会有相应的记录消息。

管理服务器将在查找被管服务器的过程中记录消息，示例如下：

```
    Mar 31, 2009 4:41:56 PM EST> <Error> <Management> <BEA-141135> <The managed
server discovery service could not be started on the admin
server.weblogic.management.
    NoAccessRuntimeException: Access not allowed for subject: principals=[], on
ResourceType: ServerRuntime Action: execute, Target: reconnectToAdminServer
    at weblogic.rjvm.BasicOutboundRequest.sendReceive
    (BasicOutboundRequest.java:108)
    at weblogic.rmi.internal.BasicRemoteRef.invoke(BasicRemoteRef.java:138)
    at weblogic.management.internal.RemoteMBeanServerImpl_812_WLStub.invoke
    (Unknown Source)
    at weblogic.management.internal.MBeanProxy.invoke(MBeanProxy.java:946)
    at weblogic.management.internal.MBeanProxy.invokeForCachingStub
    (MBeanProxy.java:481)
    at weblogic.management.runtime.ServerRuntimeMBean_Stub
    .reconnectToAdminServer (ServerRuntimeMBean_Stub.java:1359)
    at weblogic.management.ManagedServerLocator.discoverManagedServer
(ManagedServerLocator.java:260)
    at weblogic.management.ManagedServerLocator.discoverAllKnownServers
(ManagedServerLocator.java:130)
    . . . Caused by: weblogic.management.NoAccessRuntimeException: Access not
allowed forsubject: principals=[], on ResourceType: ServerRuntime Action:
execute, Target: reconnectToAdminServer
```

示例 31-3

被管服务器也将记录消息，示例如下：

```
    <Mar 31, 2009 4:41:56 PM EST> <Error> <Security> <BEA-090513>
<ServerIdentity failed validation, downgrading to anonymous.>
    <Mar 31, 2009 4:41:56 PM EST> <Warning> <RMI> <BEA-080003>
<RuntimeException thrown by rmi server:
weblogic.management.internal.RemoteMBeanServerImpl.invoke
    (Ljavax.management.ObjectName;Ljava.lang.String;
```

```
    [Ljava.lang.Object;[Ljava.lang.String;)
    weblogic.management.NoAccessRuntimeException: Access not allowed for
subject: principals=[], on ResourceType: ServerRuntime Action: execute, Target:
reconnectToAdminServer.
    weblogic.management.NoAccessRuntimeException: Access not allowed for
subject: principals=[], on ResourceType: ServerRuntime Action: execute, Target:
reconnectToAdminServer
    at weblogic.management.internal.SecurityHelper
    $IsAccessAllowedPrivilegeAction.wlsRun (SecurityHelper.java:564)
    at weblogic.management.internal.SecurityHelper
    $IsAccessAllowedPrivilegeAction.run(SecurityHelper.java:456)
    at weblogic.security.acl.internal.AuthenticatedSubject
    .doAs(AuthenticatedSubject.java:317)
    at weblogic.security.service.SecurityManager.runAs
    (SecurityManager.java:118)
    . . .
```

示例 31-4

31.1.4 设置域 Credential

31.1.4.1 配置 Credential Mappings

1、 登录管理控制台，点击左侧面板下方的 Security Realms，之后点击您想设定的 realm 的名字，例如:myrealm;

2、 选择 Credential Mappings 选项卡->Default;

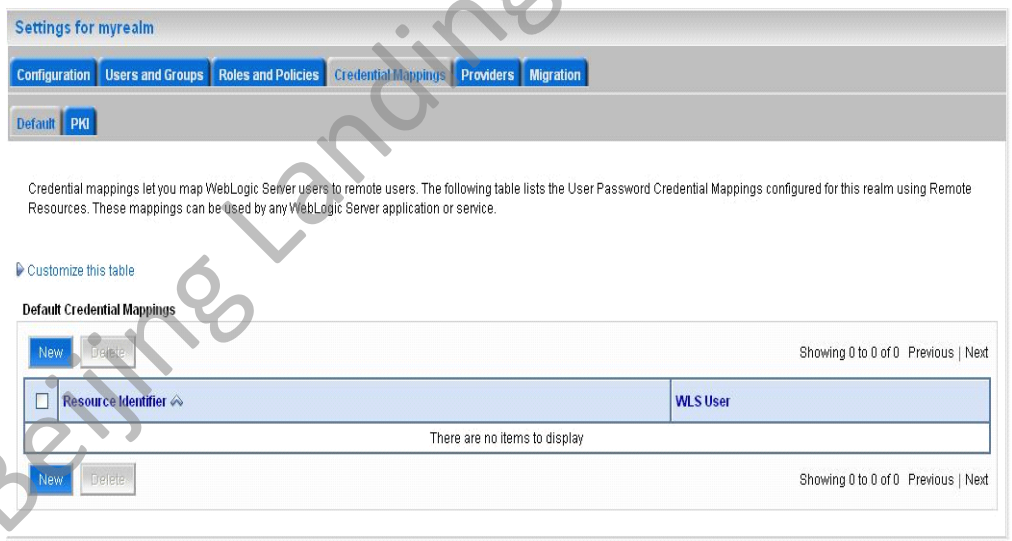


图 31-2

3、 点击新建按钮创建远程资源，如果不是用跨域协议，请使 Use cross-domain protocol 选项不被勾选

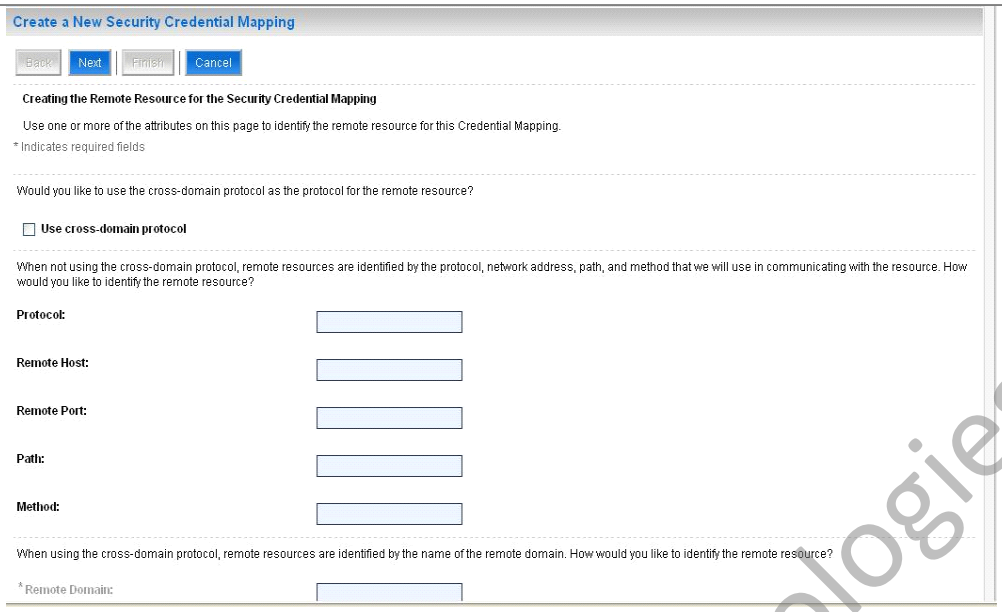


图 31-3

4、 点击 next 按钮进行下一步

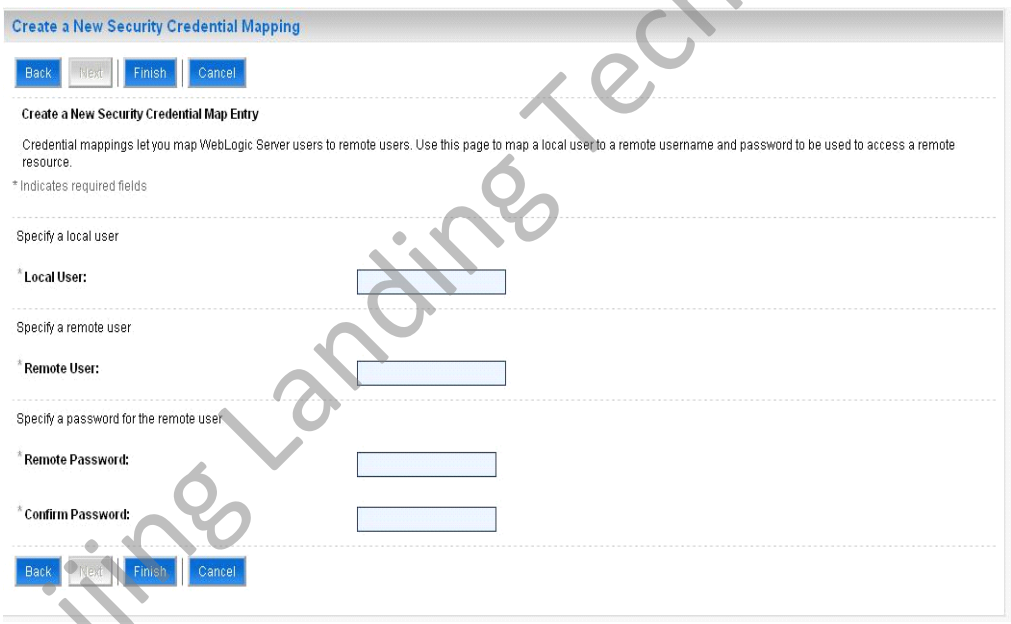


图 31-4

5、 填写完毕点击 Finish 完成。

31.1.4.2 配置 Credential Mapping Providers

6、 登录管理控制台，点击左侧面板下方的 Security Realms，点击您想设定的 realm 的名字如 myrealm。

7、 选择 Providers > Credential Mapping.

图 31-5

8、 单击新建按钮，在 name 框中输入您想为 Credential Mapping Providers 取的名字，在类型下拉列表框内选择 Credential Mapping Providers 的类型

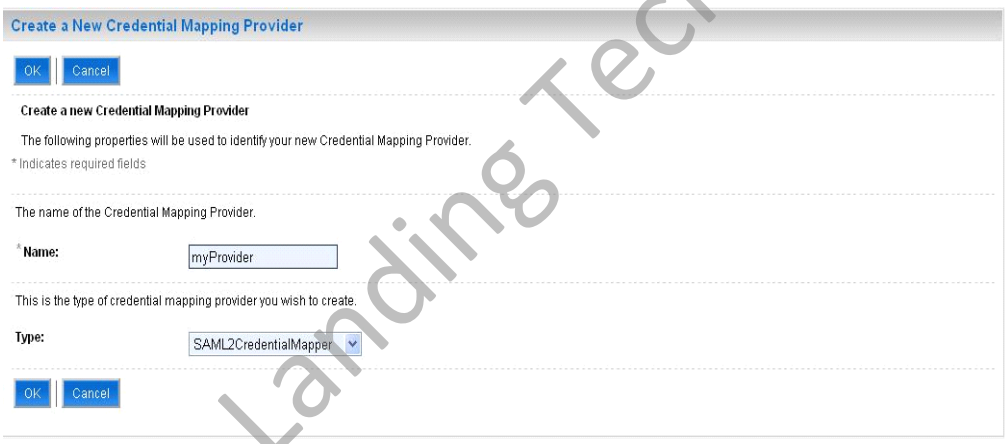


图 31-6

9、 点击 OK 按钮选择刚刚创建的 Credential Mapping Providers 的名字，configuration->Provider Specific，填写具体内容

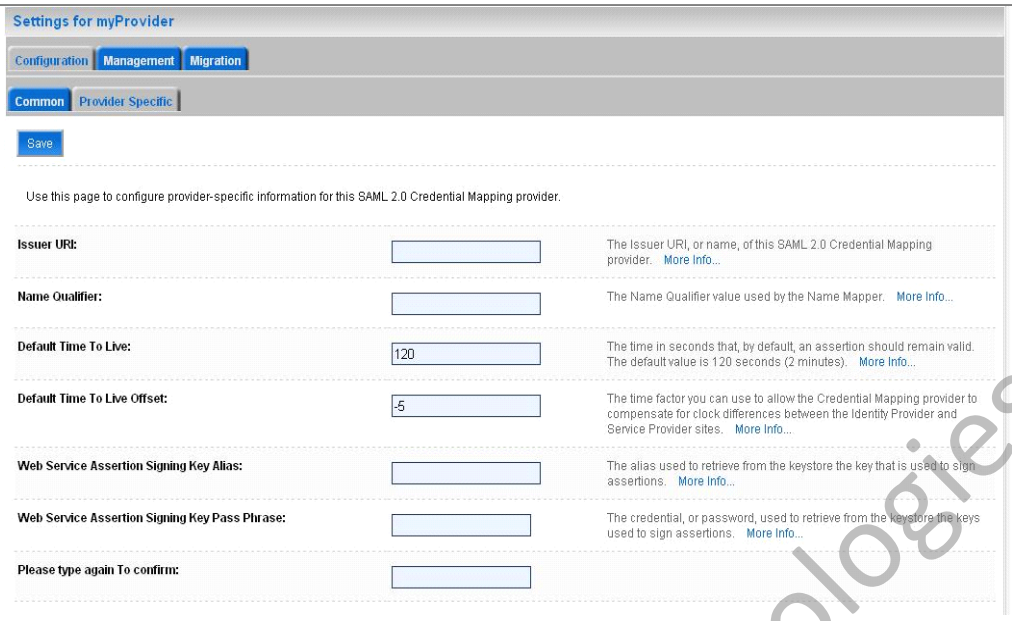


图 31-7

10、点击保存按钮保存刚才所做的设置

31.2 故障排除检查清单

故障排除策略：

1. 收集所有信任问题的诊断数据，例如：哪些域之间需要互操作，在哪里无法建立信任，所使用的 WebLogic 版本；
2. 设置适当的域 Credential（或系统用户密码）值，以建立信任；
3. 重新启动域的管理服务器和被管服务器，以确保域内信任得以保留。