IBM SOA
Policy Gateway Pattern

目录

第 1 章 SOA 策略概述

策略管理以结构化且一致的方式在管理策略方面起到关键的作用。策略可以用于在任何面向服务的环境中支持更好的监管。面向服务体系结构 (SOA) 实践帮助企业识别和关注业务的关键服务。通过添加策略，我们添加了业务和信息技术的控制点和敏捷性。结果，SOA 使用更广泛、在降低业务用户的项目成本的同时，提高了产生价值的速度，并加速了 SOA 解决方案的应用。

策略是可应用于一个或多个资源（包括不同服务）的独立元素。策略和任何相关元数据的分配（尤其在分布式环境中）可以产生于各种实施点和决策点。

SOA 策略体系结构

SOA 策略体系结构描述策略编写点 (PAP)、策略执行点 (PEP)、策略决策点 (PDP)、策略信息点 (PIP) 和策略监控点 (PMP) 的交互。在该模式中，使用 WSRR 实现 PAP，并使用 WebSphere® DataPower® 实现 PEP。

那些关键点的基本策略体系结构和定义的组织如下:

- **策略编写点** - 提供运行时期间编写策略、管理和监管策略及其向资源的分配和管理策略结果的策略功能。包含一个用于存储策略的存储库。在此模式中，这是使用 WSRR 获取的。
- **策略执行点** - 策略执行点是在中间件上运行的功能点，用于:
  - 执行策略。
  - 接收执行策略更新并准备好这些更新或进行转换以备使用。
  - 提供对策略监控点的实施度量。
  - 提供执行策略结果以及对策略管理点和策略监控点的分析。
  - 根据生命周期阶段更改策略实际应用和执行的位置:
    - 设计时期间，服务注册表和存储库本身就是执行点。
    - 运行时期间，通常由将服务提供者与消费者连接起来的底层中间人（中间件）系统执行策略。

  在此模式中，这是使用 WebSphere DataPower 获取的。
- **策略决策点** - 策略决策点可根据相关策略或合同以及属性对参与者请求进行评估。它提出授权、资格或验证决策以提供计算的结果。
- **策略信息点** - 策略信息点向策略决策点提供外部信息（如 LDAP 属性信息）或来自数据库的结果（必须对信息评估以做出策略决策）。
- **策略监控点** - 为整个体系结构提供详细策略监控功能的功能组件；例如，分布式环境中策略的概述。这包括:
  - 接收监控策略更新并准备好这些更新或进行转换以备使用。
  - 捕获要显示的实时收集和统计分析。
  - 通过各种实时收集器（包括策略执行点）使数据订阅源相关联、分析数据订阅源并使数据订阅源可视。

– 管理控制台，提供对策略执行点的分布式网络的管理以及这些执行的状态的可视性。
– 记录、聚集测量和突出显示监控策略指定的重大事件。
– 提供对策略管理点和策略执行点的监控策略分析。

注: 此模式中不包括监控。

消费者和提供者都与中间件进行交互，中间件转而与存储库和任何监控软件进行交互。

如何与 SOA 策略体系结构一起使用

图 1 和下面描述了 SOA 策略可操作模式流。

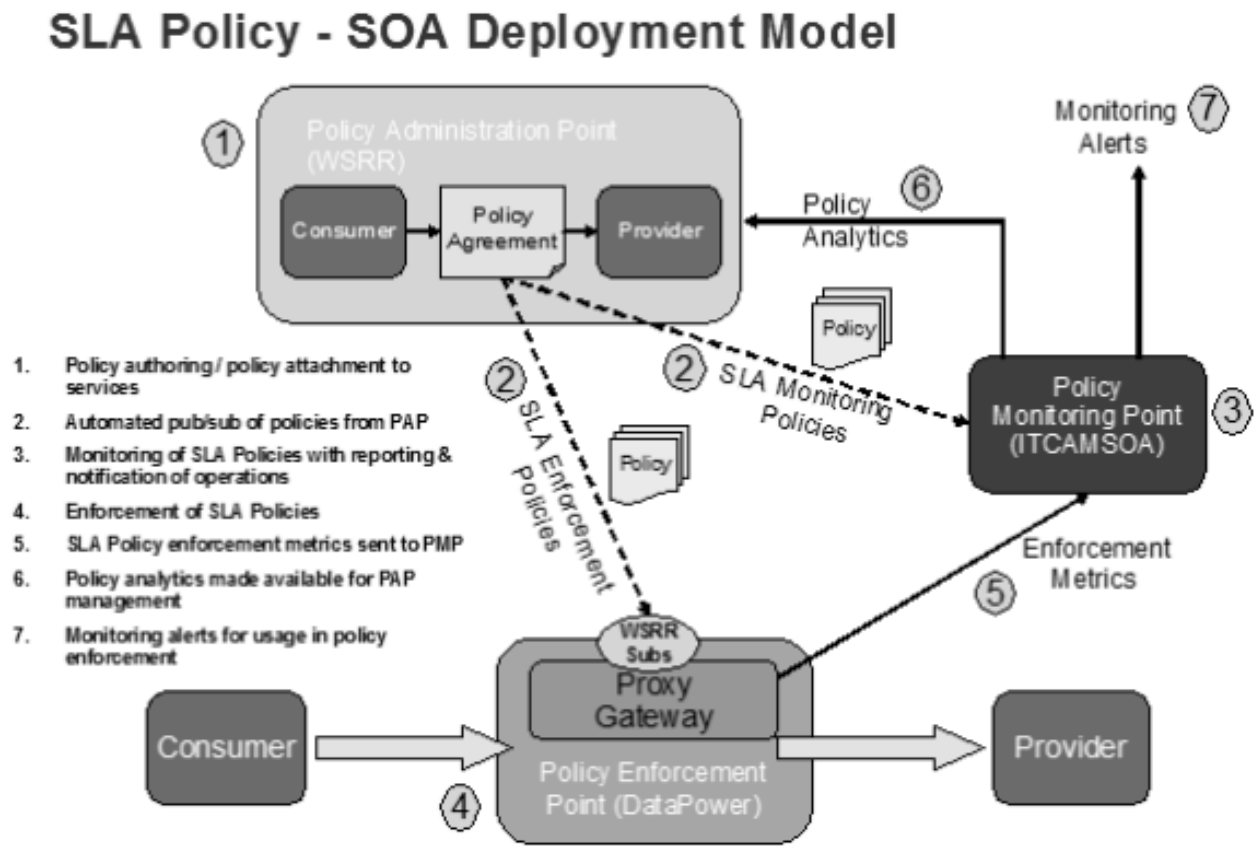


图 1. 服务级别协议 (SLA) 策略 - SOA 部署模型

1. 编写策略，然后将其附加到需要该策略的服务。通常，遵循以下顺序:
   a. 在服务存储库中装入或创建服务集合。这是策略编写点的一部分。
   b. 使用策略生命周期在策略编写点中创建所需的策略集:
      1) 根据需要，在服务、操作或端点层面，将策略附加到需要那些策略的服务。
2. 自动将策略从策略编写点发布/预订到策略执行点和策略监控点。

   注: 在此模式中，不包含使用 ITCAM for SOA 进行监控。
   a. 设置过程中，ITCAM for SOA 从 WSRR 预订监控策略。这只发生一次。

b. 设置过程中，代理网关是在具有策略执行的服务事务的每个 WebSphere DataPower® 设备中创建。这只发生一次，并且根据需要添加或更改。

c. 设置过程中，设备中的每个代理网关针对它负责的服务预订 WSRR 中的策略。这只发生一次，并且根据需要添加或更改。

d. 设置过程中，配置 WebSphere DataPower，以便该策略可由集群中其他设备共享。这只发生一次，并且根据需要添加或更改。

e. ITCAM for SOA 在发布时下载监控策略。

f. ITCAM for SOA 将策略转换为内部说明调用的情况策略。

g. WebSphere DataPower 针对它负责处理的服务下载 WSDL。

h. WebSphere DataPower 在收到 WSRR 的通知时，针对它负责的服务下载策略。

i. WebSphere DataPower 将策略转换为采用 SLM 格式的内部 WebSphere DataPower 说明。

3. 利用报告和通知操作来监控 SOA 策略:

a. 在 SOA 情况策略的 ITCAM 中，监控策略是活动的。

b. ITCAM for SOA 接收监控信息并将该信息放置在工作空间中。

注: 此模式中不提供监控。

4. SOA 策略的执行:

a. 各种 WebSphere DataPower 设备中的执行策略是活动的。

b. WebSphere DataPower 针对该消费者服务和提供者服务接收服务事务和应用策略。

5. 策略执行点会将 SOA 策略执行统计信息发送至策略监控点。

注: 此模式中不包括监控。

6. 策略监控点会将监控事件发送至策略编写点。

a. 在策略编写点中设置需要从策略监控点监控的事件。这只发生一次，并且根据需要添加或更改。

b. 当情况策略求值为 true 时，将事件从策略监控点推送到策略编写点。

注: 此模式中不包括监控。

7. 警报的监控:

a. 定期运行情况策略并按策略中的指定采取可行操作。缺省值为每 5 分钟。

SOA 策略生命周期

使用 SOA 策略生命周期监管调解策略。这将使策略从最初识别，一直到部署到生产中，最后在不再需要时弃用。

有关 SOA 策略生命周期中生命周期转换和状态的更多信息，请参阅 IBM® WebSphere Service Registry and Repository V8.0 信息中心 - SOA 策略生命周期。

策略标准

Web 技术社区团体（W3C 和 OASIS）已创建了一些标准，以满足定义适用于 Web Service 的策略的需求。

- **WS-Policy**: Web Services Mediation Policy 1.0 域定义了一组策略断言，用于描述服务的调解需求。
- **Web Services Policy 1.5 - Framework**: 定义用于表达策略的框架和模型，策略引用基于 Web Service 系统中实体的特定于域的功能、需求和一般特征。

定义特定于域的策略断言的规范示例:

- WS-MediationPolicy
- WS-SecurityPolicy
- WS-ReliableMessaging 和 WS-ReliableMessagingPolicy
- WS-SecureConversation
- WS-Security
- WS-Transactions
- WS-Trust

有关 WS-MediationPolicy 的更多信息，请参阅 ftp://public.dhe.ibm.com/software/solutions/soa/pdfs/WSMediationPolicy1.6-20120124.pdf。

WS-Policy 数据模型包括:

- **策略**: “策略备用”的无序集合。
- **策略备用**: 策略备用是“策略断言”的集合。
- **策略断言**: 代表个人喜好; 例如，需求或功能。
- **策略参数**: “策略断言”抽象的有效内容。
- **策略主题**: 策略表达式可以绑定到的实体。这用于 WS-PolicyAttachment 文档中。

以下示例（图 2）显示了使用在 WS-Security 和 WS-SecurityPolicy 中定义的断言的安全策略表达式:

```
(01) <wsp:Policy
   xmlns:sp=http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702
   xmlns:wsp=http://www.w3.org/ns/ws-policy
   xmlns:wsu=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
   wsu:Id="SecureMessages">  <!-- policy expression -->
(02)   <wsp:ExactlyOne>
(03)     <wsp:All>    <!-- policy alternative #1 -->
(04)       <sp:SignedParts>;   <!-- policy assertion -->
(05)         <sp:Body>   <!-- policy assertion parameter -->
(06)       </sp:SignedParts>
(07)     </wsp:All>
(08)     <wsp:All>    <!-- policy alternative #2 -->
(09)       <sp:EncryptedParts> <!-- policy assertion -->
(10)         <sp:Body/>   <!-- policy assertion parameter -->
(11)       </sp:EncryptedParts>
(12)     </wsp:All>
(13)   </wsp:ExactlyOne>
(14) </wsp:Policy>
```

行 (03-07) 代表用于签名消息体的一个策略备用。

行 (08-12) 代表用于加密消息体的第二个策略备用。

行 (02-13) 显示 ExactlyOne 策略操作程序。策略操作程序将策略断言分成策略备用。上面策略的有效解释将是 Web service 的调用或者是签署消息体，或者是加密消息体，但不可能是两者兼得。

图 2. 使用具有安全策略断言的 Web Service 策略

图 3 显示策略定义。

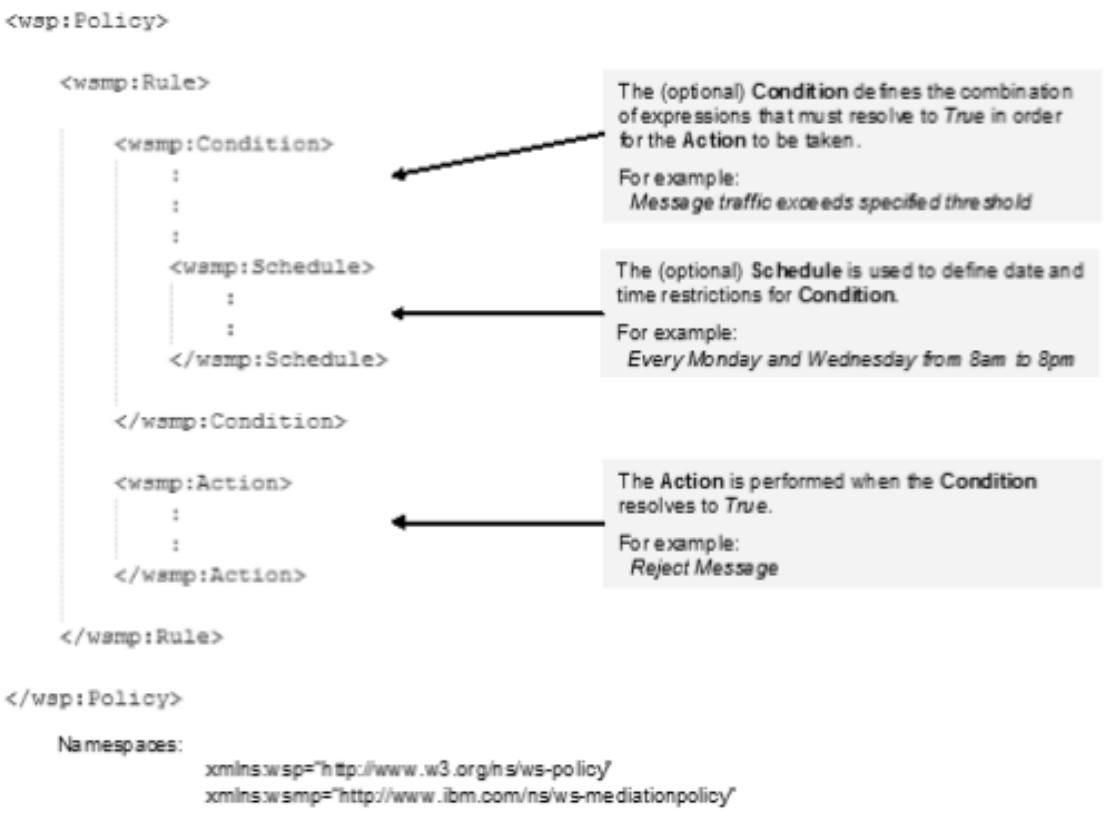


图 3. 策略结构概述

策略附件

策略附件文档角色用于将一组 WS-Policy 策略与执行的特定服务附加点（如 Web Service 附加点）相关联。

例如，Web Service 平台可以支持基于以下元素的附加点:

- WSDL Element URI 1.1 元素
- WS-Addressing 元素

语法是在 WS-PolicyAttachment 规范中定义的:

```
<wsp:PolicyAttachment>
    <wsp:AppliesTo>


    </wsp:AppliesTo>
    <wsp:Policy>


    </wsp:Policy>
</wsp:PolicyAttachment>
```

图 4. WS-PolicyAttachment 规范

WSRR 显示 REST 接口以获取 SLA 模型中适当的策略附件。将有关策略应用于的消费者-提供者对的信息以 WS-PolicyAttachment 格式传递给 ESB。语法是在 WS-PolicyAttachment: Message Content Filters 规范中定义的。

可以仅为提供者服务、特定消费者-提供者对或匿名消费者指定策略。匿名消费者提供一种用于定义缺省策略的方式，此缺省策略仅适用于未应用其他策略的消费者。

在第 5 页的图 4 中，策略应用于的特定于域的策略主题（提供者）包含在后跟策略应用于的消费者-上下文过滤器（消费者）的 <wsp:AppliesTo> 部分。然后，在 <wsp:Policy> 部分中，声明或引用一个或多个策略。

第 2 章 模式概述

IBM SOA Policy Gateway Pattern 是一组提供策略执行点和策略管理点的虚拟系统模式。策略管理点由在多层体系结构中供应 WSRR 的虚拟系统模式提供，交付生产和登台环境。策略执行点由 WebSphere DataPower 设备提供，在虚拟系统模式部署期间在该设备中创建域。

如果并非所有都是面向服务的体系结构 (SOA) 环境，那么有多个策略示例。服务生产者和使用者在设计阶段就服务的功能、性能和特征达成一致。要执行此操作，您可以使用服务级别定义 (SLD) 和服务级别协议 (SLA)。此模式使您能够以高效管理、定义、监管和利用的方式定义 SLD 和 SLA 的策略。此模式中使用的策略类型包含以下项:

- **调解策略** -
  - 拒绝 - 拒绝或控制以大于所定义值的速率到达的请求。
  - 日志记录 - 在调用服务时，使用策略执行点创建日志消息。
  - 变换。
  - 验证 - 根据服务定义验证服务调用。
  - 路由 - 根据消息，路由至特定端点。
- **安全策略**: 在样本中，我们演示执行 XACML 访问控制安全策略的方式。此时不会在策略管理点中监管这些策略。

IBM SOA Policy Gateway Pattern 模式包含以下虚拟系统模式:

- SOA Policy Gateway Basic Runtime Sample
- SOA Policy Gateway Governance Master
- SOA Policy Gateway Basic Runtime
- SOA Policy Gateway Advanced Runtime

四个虚拟系统模式共同提供一个多阶段服务监管环境。IBM SOA Policy Gateway Pattern 还提供在模式部署期间供应针对监管环境配置的多个 DataPower 域的功能。联合提供以下部署拓扑:

- 独立部署
- 试运行部署
- 完整生产部署

有关 SOA 策略的更多信息，请参阅第 1 页的第 1 章，『SOA 策略概述』。

可以手动配置已部署的虚拟系统模式，以包含通过 ITCAM for SOA V7 进行的监控。这将提供对事件的基本监控，并扩展策略支持以包含监控策略。监控策略允许在策略编写点 (PAP) 中定义事件情况，并将这些情况附加到服务定义，这样在发生事件情况时，使监控器能够发挥作用。

相关概念:

第 1 页的第 1 章, 『SOA 策略概述』
策略管理以结构化且一致的方式在管理策略方面起到关键的作用。策略可以用于在任何面向服务的环境中支持更好的监管。面向服务体系结构 (SOA) 实践帮助企业识别和关注业务的关键服务。通过添加策略，我们添加了业务和信息技术的控制点和敏捷性。结果，SOA 使用更广泛、在降低业务用户的项目成本的同时，提高了产生价值的速度，并加速了 SOA 解决方案的应用。

第 17 页的『SOA Policy Gateway Basic Runtime』
SOA Policy Gateway Basic Runtime 提供一种简单的方法来提供可单独使用或与已部署的 SOA Policy Gateway Governance Master 模式进行集成的运行时。 SOA Policy Gateway Basic Runtime 模式支持部署已配置为与该模式中供应的 WSRR 运行时服务器进行通信的 DataPower 域。

第 14 页的『SOA Policy Gateway Basic Runtime Sample』
SOA Policy Gateway Basic Runtime Sample 向 SOA Policy Gateway Basic Runtime 供应样本接口和应用程序，以演示当前在此发行版中受支持的策略。

第 15 页的『SOA Policy Gateway Governance Master』
SOA Policy Gateway Governance Master 模式提供集群管理环境以用于编写和管理服务和策略。为该环境供应了已配置的 WSRR 缺省“监管支持概要文件”。缺省“监管支持概要文件”支持两个提升目标: 登台和生产。

第 19 页的『SOA Policy Gateway Advanced Runtime』
SOA Policy Gateway Advanced Runtime 包含更多高可用性选项，必须与 SOA Policy Gateway Governance Master 一起使用。

第 3 章 IBM SOA Policy Gateway Pattern 入门

此模式使用 WebSphere DataPower 来控制使用 WSRR 中的受管策略和服务定义的消息。请查看本部分中的主题，以了解此场景中涉及的内容、企业可能想要采用此场景的原因、涉及的用户角色以及通过产品交付的功能的概述。

开始之前

您可以在 IBM PureApplication System 或 IBM Workload Deployer 设备上使用 IBM IBM SOA Policy Gateway Pattern。

过程

要使用 IBM SOA Policy Gateway Pattern，请完成以下步骤:

1. 下载并安装 IBM SOA Policy Gateway Pattern。 有关从 Passport Advantage® 下载软件包的更多信息，请参阅『下载并安装模式』。
2. 可选: 配置用户访问。有关更多信息，请参阅第 12 页的『配置用户访问』。
3. 配置并部署模式
   a. 接受 WSRR 的已导入虚拟系统映像许可证。
   b. 接受 DB2® Enterprise 上的所有许可证协议。
   c. 部署模式:
      1) 确定部署拓扑。有关更多信息，请参阅IBM WebSphere Service Registry and Repository V8.0 信息中心 - 部署拓扑。
      2) 如果使用独立部署拓扑，那么会部署单个 Basic Runtime 模式而不配置提升。
      3) 对于其他拓扑，首先部署 SOA Policy Gateway Governance Master 模式。这会为服务和策略提供一个监管环境。
      4) 在成功部署 Governance Master 模式后，选择需要的运行时环境的类型。对于测试或登台环境，Basic Runtime 通常已足够。对于生产环境，请选择 Advanced Runtime 环境。通过 Governance Master 的“监管支持概要文件”提升配置，可以注册运行时。提升选项包含生产、登台或无提升（针对手动提升配置）。

      有关更多信息，请参阅第 56 页的『部署模式』。
   d. 验证部署。 请参阅第 62 页的『验证部署』。
   e. 保护 WSRR 环境安全性。有关规划和配置 WSRR 安全性的更多信息，请参阅 IBM WebSphere Service Registry and Repository V8.0 信息中心。
   f. 配置供应的 DataPower 域。有关更多信息，请参阅第 49 页的『安全管理』。
4. 使用部署的实例。有关更多信息，请参阅第 85 页的第 6 章，『使用已部署的实例』。

下载并安装模式

用于 IBM Workload Deployer V3.1.0.2 或 IBM PureApplication System 的 IBM SOA Policy Gateway Pattern 已打包，以供从 Passport Advantage 下载。

开始之前

确保针对 CI9G9ML.tar.gz 文件有 10 GB 可用空间，并且另外有 10 - 14 GB 空间可用于解压缩的文件。

必须将 CI9G9ML.tar.gz 文件下载至运行 Linux 或 Microsoft Windows 的系统。而且，必须先安装 Java™ Runtime Environment (JRE) V6，然后才能启动模式安装。您可以从以下地址下载此版本的 Linux：http://www.ibm.com/developerworks/java/jdk/linux/download.html。

关于此任务

IBM SOA Policy Gateway Pattern 打包在 CI9G9ML.tar.gz 文件中。此归档包含开放式虚拟归档 (OVA) 文件、脚本软件包文件和模式定义文件。

过程

要从 Passport Advantage 下载 IBM SOA Policy Gateway Pattern 映像，请完成以下步骤:

1. 访问 Passport Advantage Web 站点：Passport Advantage。
2. 下载包含要使用的映像、脚本程序包和模式的归档文件。该文件名为 CI9G9ML.tar.gz。
3. 打开 Linux 上的终端或 Windows 上的命令提示符窗口，并浏览至下载 CI9G9ML.tar.gz 文件的目录。
4. 将 CI9G9ML.tar.gz 文件的内容解压缩到本地文件系统。在 Linux 上，解压缩命令为： 在 Linux 上，解压缩命令为:

   ```
   tar xvzf CI9G9ML.tar.gz
   ```

   在 Windows 上，请使用额外的归档解压缩软件来解压缩 CI9G9ML.tar.gz 的内容。
5. 确保以下解压缩的文件在 Linux 系统上具有执行许可权:
   - chmod a+x installer/installer
   - chmod a+x installer/deployer.cli/bin/deployer
   - chmod a+x installer/deployer.cli/bin/3.1.0.2-20120531075842/deployer
6. 切换至 installer 目录:

   ```
   cd installer
   ```
7. 要在云设备中安装 IBM SOA Policy Gateway Pattern，请运行安装程序。命令名称为 installer.bat (Microsoft Windows) 或 installer (Linux)。 输入以下命令: installer -h *<host>* -u *<username>* -p *<password>*，其中，<host> 是云设备，username 和 password 是云管理员凭证。例如:

   ```
   ./installer -h apiliwd.rchland.ibm.com -u cbadmin -p cbadmin
   ```
8. 在提示时，接受 IBM SOA Policy Gateway Pattern 许可证。
   a. 在 Microsoft Windows 上：在接受许可证协议后，如果终端中的换行显示 >>>，type quit()，那么请按 Enter 键。重复步骤 7。
9. 模式已导入。 在安装每个模式时，安装程序中会显示一条消息，表明已成功安装。例如:

   ```
   Importing pattern "SOA Policy Gateway 2.0.0.0 - Governance Master" ...
   Import pattern "SOA Policy Gateway 2.0.0.0 - Governance Master" successfully.
   ```

结果

这样会装入模式和脚本，并创建虚拟系统模式。

注: 如果目录中已存在 IBM SOA Policy Gateway Pattern 中使用的正确版本级别的虚拟系统模式，那么不会进行覆盖。

下一步做什么

接受 IBM Workload Deployer 设备或 IBM PureApplication System 中的许可证。

要验证安装，请参阅『验证已安装的模式』。

验证已安装的模式

您可以验证模式是否已成功安装，并接受任何必需的许可证以使用模式。

开始之前

确保 第 9 页的『下载并安装模式』 中的所有步骤都已完成。

关于此任务

在安装模式之后，您可以验证模式安装。在可以使用任何虚拟映像之前，必需接受它的必需许可证。

过程

要验证 IBM SOA Policy Gateway Pattern 的安装，请完成以下步骤:

1. 登录到安装模式的 IPAS 控制台或 IWD 控制台。
2. 通过浏览至目录 > 虚拟映像来验证“虚拟映像”，并查找: DB2 9.7.5.0 和 WebSphere Service Registry and Repository 8.0.0.1。如果未接受许可证，那么映像图标将包含一个打叉的红色框。
   a. 要接受许可证，请单击映像以查看其详细信息。此时将显示当前状态。单击“许可证协议”中的**接受**，然后单击在可以使用虚拟映像前必须接受的任何许可证。当前状态将显示“只读”，并且在完成时许可证协议将显示“已接受”。
3. 浏览至"目录 -> 脚本软件包"，查找:
   - SOA Policy Gateway 2.0.0.0 - DataPower Domain
   - SOA Policy Gateway 2.0.0.0 - Promotion
   - SOA Policy Gateway 2.0.0.0 - Sample
   - SOA Policy Gateway 2.0.0.0 - Security

   成功的安装中包含所有这些脚本软件包。
4. 浏览至"模式 -> 虚拟系统"，并查找:
   - SOA Policy Gateway 2.0.0.0 - Advanced Runtime
   - SOA Policy Gateway 2.0.0.0 - Basic Runtime
   - SOA Policy Gateway 2.0.0.0 - Basic Runtime Sample
   - SOA Policy Gateway 2.0.0.0 - Governance Master

   成功的安装中包含所有这些模式。

结果

您已验证 IBM SOA Policy Gateway Pattern 的安装。

下一步做什么

如果安装成功，那么可以进入: 第 47 页的第 5 章，『使用 IBM SOA Policy Gateway Pattern』。如果安装失败，请重复主题第 9 页的『下载并安装模式』自步骤 7 开始的步骤。

配置用户访问

要使用户能够访问设备上的映像和模式，设备管理员首先必须允许用户访问。您可以先创建用户，然后将用户添加到组，或者先创建组然后创建用户，并将用户添加到组。

关于此任务

管理用户（通常为设备管理员）可以添加其他用户来访问和管理模式。

过程

要配置用户访问，请完成以下步骤:

1. 选择以下一个选项以配置用户和用户组（可选）:
   - 从界面的“用户”窗口添加并配置用户。
     a. 从菜单中，单击**系统 > 用户**。
     b. 单击**添加**图标。
     c. 提供短用户名以及用户的实际名称、电子邮件地址和密码，然后单击**确定**。
     d. 选择在“用户”面板中添加的用户以配置访问。配置所选用户的访问和操作。
     e. 在**用户组**字段中，将用户添加到一个或多个用户组。
   - 创建用户组。
     a. 从菜单中，单击**系统 > 用户组**。
     b. 单击**添加**图标。提供组的名称和描述。
     c. 选择在“用户组”面板中添加的组以配置访问。
     d. 在**组成员**字段中添加成员，并提供许可权以应用于组。
2. 可选: 如果已添加虚拟映像，请向虚拟映像添加用户和组的访问权。从菜单中，单击**目录 > 虚拟映像**以打开“虚拟映像”窗口。从左侧面板中选择 IBM SOA Policy Gateway Pattern 虚拟映像，然后在右侧面板中添加用户或组。

下一步做什么

如果尚未添加虚拟映像，请进行添加，然后向其提供用户或组的访问权。

相关信息:

IBM PureApplication System: 管理用户和组

IBM Workload Deployer: 管理用户和组

第 4 章 模式、部件和脚本程序包

IBM SOA Policy Gateway Pattern 部件是模式的功能组件。每个部件表示单个虚拟机。模式为可以共享的可重复部署提供了拓扑定义。

模式描述由虚拟系统中每个虚拟机提供的功能。每个功能都标识为模式中的部件。模式呈现其相关联部件的特征。例如，将 WSRR 部件放入随后进行部署的模式中后，其结果是带有正在运行的 WSRR 实例的虚拟机。

部件

部件描述了虚拟机上配置的组件。每个部件都具有一组属性（参数），在部署期间用于帮助定义虚拟系统的整体配置。将 IBM SOA Policy Gateway Pattern 映像装入 IBM Workload Deployer 时，会将部件包含在内。

模式

IBM SOA Policy Gateway Pattern 模式包含四个模式:

- SOA Policy Gateway Basic Runtime
- SOA Policy Gateway Basic Runtime Sample
- SOA Policy Gateway Advanced Runtime
- SOA Policy Gateway Governance Master

有关使用 IBM Workload Deployer 访问现有模式或创建定制模式的详细信息，请访问 http://publib.boulder.ibm.com/infocenter/worlodep/v3r0m0/topic/com.ibm.worlodep.doc/welcome.html。

模式

将虚拟映像装入 IBM Workload Deployer 或 IBM PureApplication System 并为用户分配适当的访问权之后，用户可以开始使用映像的模式。

模式提供了可以部署到云的可重复拓扑。已部署模式是在云中运行的虚拟系统。不管是预定义的模式还是创建的模式都包含部件。将模式作为虚拟系统部署到云时，模式需要一些部件才能运行。

SOA Policy Gateway Basic Runtime

SOA Policy Gateway Basic Runtime 包含以下必需部件:

- DB2 Enterprise
- WSRR 独立服务器

SOA Policy Gateway Basic Runtime Sample

SOA Policy Gateway Basic Runtime Sample 包含以下必需部件:

- DB2 Enterprise
- WSRR 独立服务器

SOA Policy Gateway Advanced Runtime

SOA Policy Gateway Advanced Runtime 包含以下必需部件:

- WSRR 部署管理器
- DB2 Enterprise HADR Primary
- DB2 Enterprise HADR Standby
- WSRR 定制节点

SOA Policy Gateway Governance Master

SOA Policy Gateway Governance Master 包含以下必需部件:

- WSRR 部署管理器
- DB2 Enterprise HADR Primary
- DB2 Enterprise HADR Standby
- WSRR 定制节点

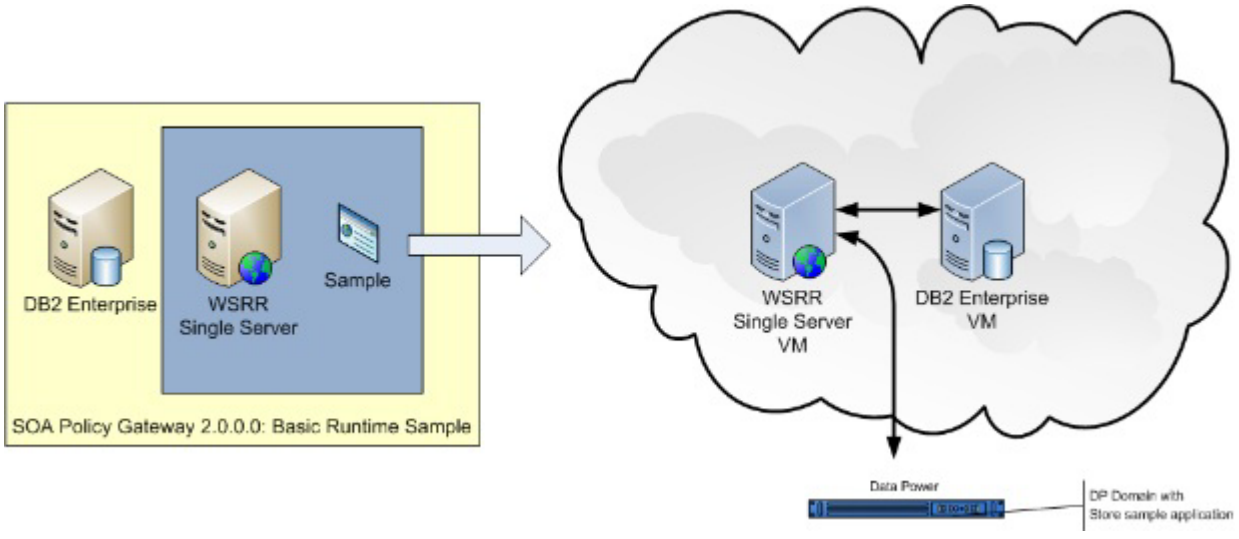
SOA Policy Gateway Basic Runtime Sample

SOA Policy Gateway Basic Runtime Sample 向 SOA Policy Gateway Basic Runtime 供应样本接口和应用程序，以演示当前在此发行版中受支持的策略。

SOA Policy Gateway Basic Runtime Sample 模式需要以下部件:

- WSRR 独立服务器
- DB2 Enterprise

SOA Policy Gateway Basic Runtime Sample 模式在部署环境中安装样本应用程序。在实施简单服务的 DataPower 中安装样本域，在服务的 WSRR 中安装样本 WSDL 和连接策略，并提供测试应用程序以演示执行的策略。有关样本应用程序的更多信息，请参阅第 64 页的『样本应用程序』。将在 DataPower 中安装样本域，在 WSRR 中安装样本 WSDL 和策略，并演示针对服务的多个策略。



实施的策略包括:

表 1. 包含在 Basic Runtime with Sample 模式中的策略

策略类型	描述
日志记录	根据请求上下文标识，在 DataPower 中记录请求。
路由	根据请求上下文标识，将请求路由至指定的端点。
验证	根据服务实施 WSDL 来验证请求。
拒绝	根据以下操作的消息计数来控制对服务的请求：拒绝、排队和其他。
安全性 AAA	使用基于 XACML 的用户授权控制对服务的访问。XACML 未存储在 WSRR 中。
安全性编辑	根据 XACML 编辑响应消息的某些部分。XACML 未存储在 WSRR 中。

脚本和高级选项

SOA Policy Gateway Basic Runtime 模式需要以下脚本。

在 WSRR 独立服务器部件上:

- SOA Policy Gateway 2.0.0.0 - Sample

查看部件和脚本参数:

- 第 23 页的『SOA Policy Gateway Basic Runtime Sample 模式的 DB2 Enterprise 部件配置参数』
- 第 35 页的『SOA Policy Gateway Basic Runtime Sample 模式的 WSRR 独立服务器部件配置参数』
- 第 42 页的『SOA Policy Gateway Basic Runtime Sample 模式的 SOA Policy Gateway 2.0.0.0 - Sample 脚本配置参数』

相关概念:

第 22 页的『DB2 Enterprise 部件』
DB2 Enterprise 部件提供了一些配置选项。

第 34 页的『WSRR 独立服务器部件』
WSRR 独立服务器部件提供了一些配置选项。

第 41 页的『脚本: SOA Policy Gateway 2.0.0.0 - Sample』
Sample 脚本配置了样本应用程序参数以用于 SOA Policy Gateway Basic Runtime Sample 模式。

第 64 页的『样本应用程序』
样本应用程序是可配置的 DataPower Domain 和一组可用于演示模式功能的 WSRR 工件。

SOA Policy Gateway Governance Master

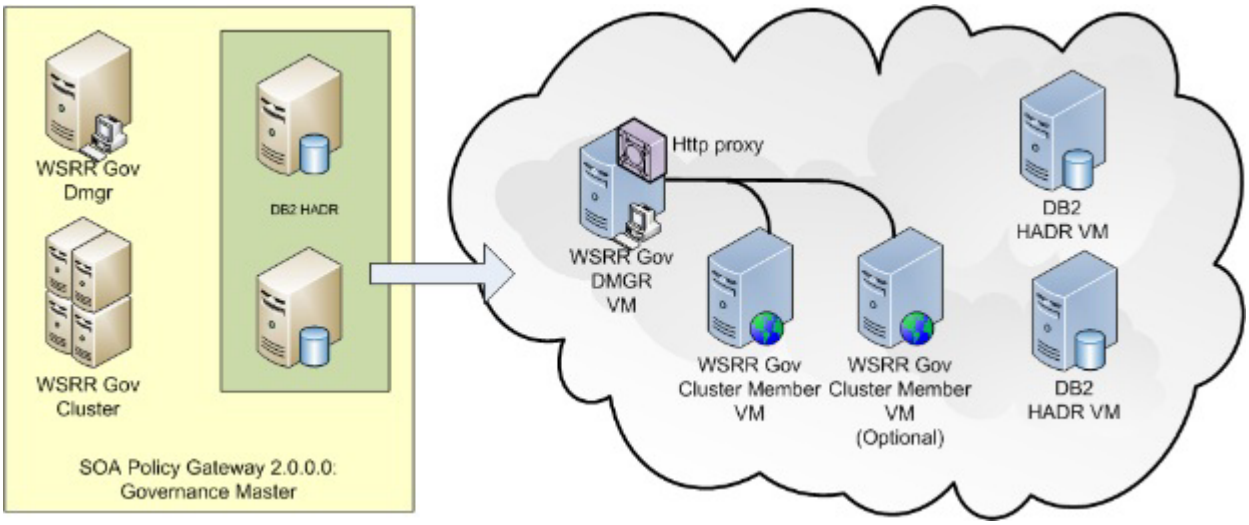
SOA Policy Gateway Governance Master 模式提供集群管理环境以用于编写和管理服务和策略。为该环境供应了已配置的 WSRR 缺省“监管支持概要文件”。缺省“监管支持概要文件”支持两个提升目标: 登台和生产。

SOA Policy Gateway Governance Master 模式需要以下部件:

- DB2 HADR Primary

- DB2 HADR Standby
- WSRR 部署管理器
- WSRR 定制节点

注: 必须在部署运行时模式之前部署 Governance Master 模式。用于配置 Governance Master 模式的参数由运行时模式用于通过 Governance Master 配置自身。只能将 SOA Policy Gateway Basic Runtime 模式或 SOA Policy Gateway Advanced Runtime 配置到 Governance Master 中。



脚本和高级选项

SOA Policy Gateway Governance Master 模式需要以下脚本:

- SOA Policy Gateway 2.0.0.0 - Security
- SOA Policy Gateway 2.0.0.0 - Promotion
- SOA Policy Gateway 2.0.0.0 - DataPower Domain

查看部件和脚本参数:

- 第 31 页的『SOA Policy Gateway Governance Master 模式的 DB2 Enterprise HADR Primary 部件配置参数』
- 第 33 页的『SOA Policy Gateway Governance Master 模式的 DB2 Enterprise HADR Standby 部件配置参数』
- 第 36 页的『SOA Policy Gateway Governance Master 模式的 WSRR 部署管理器部件配置参数』
- 第 38 页的『SOA Policy Gateway Governance Master 模式的 WSRR 定制节点部件配置参数』

将 Governance 模式用作 Governance Master

SOA Policy Gateway Governance Master 模式通过包含两个提升阶段（登台和生产）的缺省 WSRR 监管支持概要文件来部署。有关 WSRR 中的“监管支持概要文件”的更多信息，请参阅 IBM WebSphere Service Registry and Repository V8.0 信息中心 - 监管支持概要文件。可以将 SOA Policy Gateway Basic Runtime 和 SOA Policy Gateway

Advanced Runtime 模式作为提升目标部署到此集成中。有关如何对此进行配置的更多信息，请参阅第 62 页的『场景: 将额外的运行时添加到模式』。

相关概念:

第 24 页的『DB2 Enterprise HADR Primary 部件』
DB2 Enterprise HADR Primary 部件提供了一些配置选项。

第 32 页的『DB2 Enterprise HADR Standby 部件』
DB2 Enterprise HADR Standby 部件提供了一些配置选项。

第 35 页的『WSRR 部署管理器部件』
WSRR 部署管理器部件提供了一些配置选项。

第 37 页的『WSRR 定制节点部件』
WSRR 定制节点部件提供了一些配置选项。

相关信息:

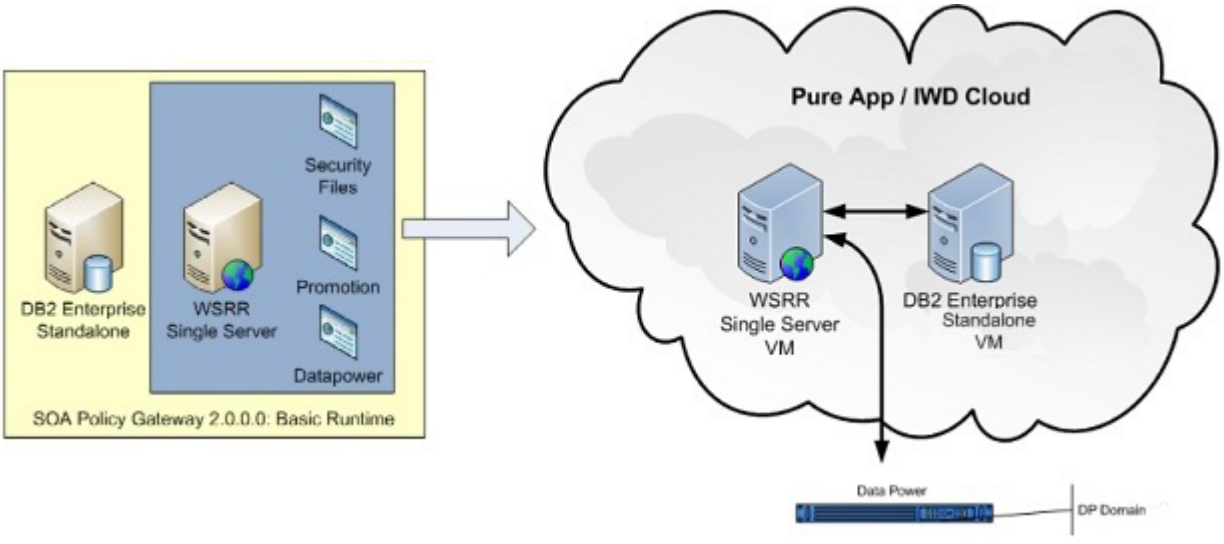
IBM WebSphere Service Registry and Repository V8.0 信息中心 - 监管支持概要文件

SOA Policy Gateway Basic Runtime

SOA Policy Gateway Basic Runtime 提供一种简单的方法来提供可单独使用或与已部署的 SOA Policy Gateway Governance Master 模式进行集成的运行时。 SOA Policy Gateway Basic Runtime 模式支持部署已配置为与该模式中供应的 WSRR 运行时服务器进行通信的 DataPower 域。

SOA Policy Gateway Basic Runtime 模式需要以下部件:

- WSRR 独立服务器
- DB2 Enterprise



脚本和高级选项

SOA Policy Gateway Basic Runtime 模式需要以下脚本。

在 WSRR 独立服务器部件上:

- SOA Policy Gateway 2.0.0.0 - Security
- SOA Policy Gateway 2.0.0.0 - Promotion
- SOA Policy Gateway 2.0.0.0 - DataPower Domain

查看部件和脚本参数:

- 第 34 页的『SOA Policy Gateway Basic Runtime 模式的 WSRR 独立服务器部件配置参数』
- 第 22 页的『SOA Policy Gateway Basic Runtime 模式的 DB2 Enterprise 部件配置参数』
- 第 45 页的『SOA Policy Gateway Basic Runtime 模式的 SOA Policy Gateway 2.0.0.0 - Security 脚本配置参数』
- 第 40 页的『SOA Policy Gateway Basic Runtime 模式的 SOA Policy Gateway 2.0.0.0 - Promotion 脚本配置参数』
- 第 39 页的『SOA Policy Gateway Basic Runtime 模式的 SOA Policy Gateway 2.0.0.0 - DataPower Domain 脚本配置参数』

将 SOA Policy Gateway Basic Runtime 提升到 Governance Runtime 中

使用 Governance Master 模式配置 Basic Runtime 模式时，将发生以下情况:

- 将配置跨单元安全性
- 将使用 Basic Runtime 部署的部署数据更新 Governance Master 上的 `promotion.xml` 文件。

要配置提升，必须选择以下某个登台选项:

- 生产
- 登台
- 其他或取消设置

这些选项与 WSRR 中的“监管支持概要文件”提供的级别保持一致。如果管理概要文件有所不同，那么请在更改 Governance Master 的管理概要文件时选择“其他”。有关 WSRR 中的“监管支持概要文件”的更多信息，请参阅 IBM WebSphere Service Registry and Repository V8.0 信息中心 - 监管支持概要文件。

相关概念:

第 64 页的『样本应用程序』
样本应用程序是可配置的 DataPower Domain 和一组可用于演示模式功能的 WSRR 工件。

第 22 页的『DB2 Enterprise 部件』
DB2 Enterprise 部件提供了一些配置选项。

第 34 页的『WSRR 独立服务器部件』
WSRR 独立服务器部件提供了一些配置选项。

第 44 页的『脚本: SOA Policy Gateway 2.0.0.0 - Security』
Security 脚本将 ZIP 文件中包含的与 DataPower 设备进行通信所需的安全信息从支持 Linux 安全复制程序 (SCP) 的外部文件服务器复制到部署管理器或 WSRR 机器。

第 40 页的『脚本: SOA Policy Gateway 2.0.0.0 - Promotion』
Promotion 脚本支持将 SOA Policy Gateway Basic Runtime 或 SOA Policy Gateway Advanced Runtime 模式与预部署的 SOA Policy Gateway Governance Master 模式集成。 它在 Runtime 和 Governance 模式之间建立跨单元安全性，同时可选择将 WSRR 提升配置到 Governance Master 中。

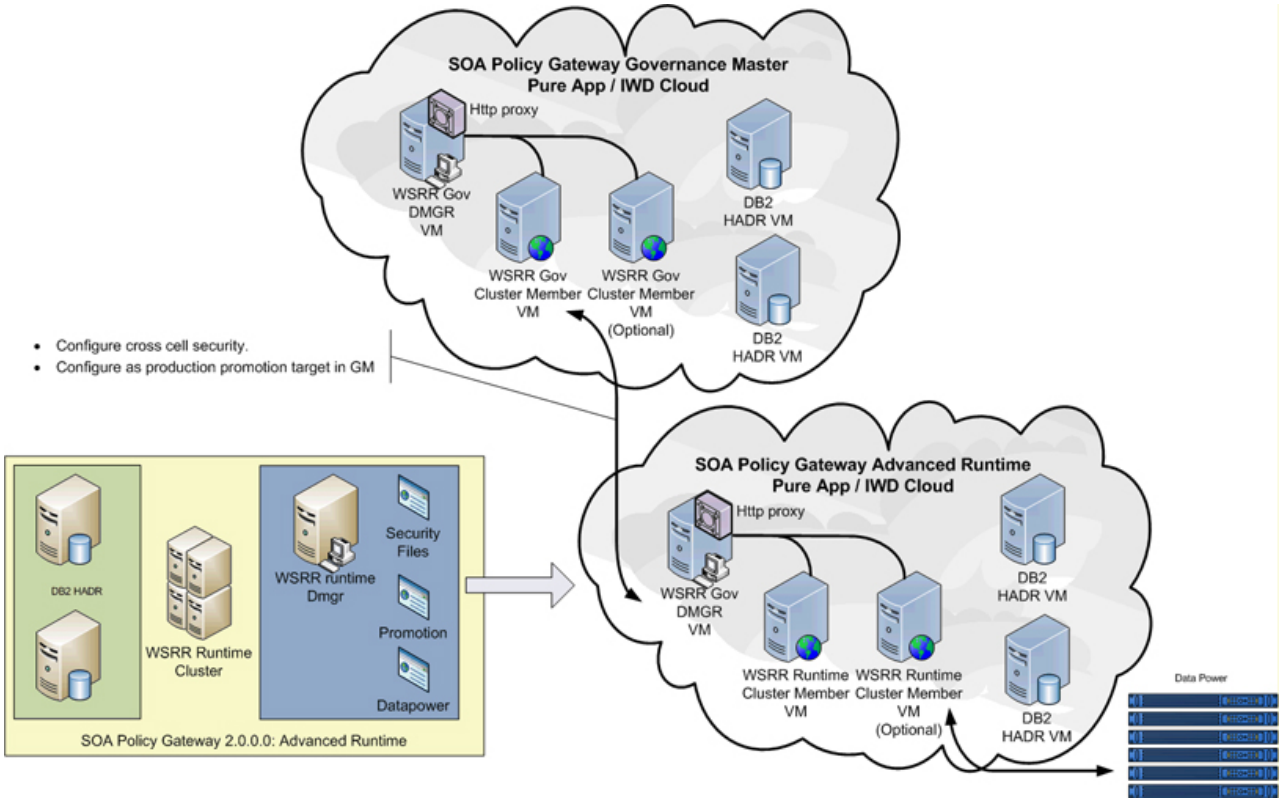
第 38 页的『脚本: SOA Policy Gateway 2.0.0.0 - DataPower Domain』
DataPower Domain 脚本在部署期间供应 DataPower 域。该脚本在单个 DataPower 域和 WSRR 运行时之间配置连接。与 WSRR 运行时连接的每个 DataPower 域需要单独的 DataPower Domain 脚本。

SOA Policy Gateway Advanced Runtime

SOA Policy Gateway Advanced Runtime 包含更多高可用性选项，必须与 SOA Policy Gateway Governance Master 一起使用。

SOA Policy Gateway Advanced Runtime 模式需要以下部件:

- DB2 HADR Primary
- DB2 HADR Standby
- WSRR 部署管理器
- WSRR 定制节点



脚本和高级选项

SOA Policy Gateway Governance Master 模式需要 WSRR 部署管理器部件上的以下脚本:

- SOA Policy Gateway 2.0.0.0 - Security
- SOA Policy Gateway 2.0.0.0 - Promotion
- SOA Policy Gateway 2.0.0.0 - DataPower Domain（每个 DataPower 域对应一个）

查看部件和脚本参数:

- 第 25 页的『SOA Policy Gateway Advanced Runtime 模式的 DB2 Enterprise HADR Primary 部件配置参数』
- 第 32 页的『SOA Policy Gateway Advanced Runtime 模式的 DB2 Enterprise HADR Standby 部件配置参数』
- 第 36 页的『SOA Policy Gateway Advanced Runtime 模式的 WSRR 部署管理器部件配置参数』
- 第 37 页的『SOA Policy Gateway Advanced Runtime 模式的 WSRR 定制节点部件配置参数』
- 第 45 页的『SOA Policy Gateway Advanced Runtime 模式的 SOA Policy Gateway 2.0.0.0 - Security 脚本配置参数』
- 第 41 页的『SOA Policy Gateway Advanced Runtime 模式的 SOA Policy Gateway 2.0.0.0 - Promotion 脚本配置参数』
- 第 39 页的『SOA Policy Gateway Advanced Runtime 模式的 SOA Policy Gateway 2.0.0.0 - DataPower Domain 脚本配置参数』

将 SOA Policy Gateway Advanced Runtime 提升到 Governance Runtime 中

使用 Governance Master 模式配置 Advanced Runtime 模式时，将发生以下情况:

- 将配置跨单元安全性
- 将使用 Advanced Runtime 部署中的数据更新 Governance Master 上的 promotion.xml 文件。

要配置提升，必须选择以下某个登台选项:

- 生产
- 登台
- 其他或“Unset”

这些选项与 WSRR 中的“监管支持概要文件”提供的级别保持一致。如果已更改 Governance Master 上的监管概要文件，请使用“其他”作为提升级别。有关 WSRR 中的“监管支持概要文件”的更多信息，请参阅 IBM WebSphere Service Registry and Repository V8.0 信息中心 - 监管支持概要文件。

相关概念:

第 24 页的『DB2 Enterprise HADR Primary 部件』
DB2 Enterprise HADR Primary 部件提供了一些配置选项。

第 32 页的『DB2 Enterprise HADR Standby 部件』
DB2 Enterprise HADR Standby 部件提供了一些配置选项。

第 35 页的『WSRR 部署管理器部件』
WSRR 部署管理器部件提供了一些配置选项。

第 37 页的『WSRR 定制节点部件』
WSRR 定制节点部件提供了一些配置选项。

第 44 页的『脚本: SOA Policy Gateway 2.0.0.0 - Security』
Security 脚本将 ZIP 文件中包含的与 DataPower 设备进行通信所需的安全信息从支持 Linux 安全复制程序 (SCP) 的外部文件服务器复制到部署管理器或 WSRR 机器。

第 40 页的『脚本: SOA Policy Gateway 2.0.0.0 - Promotion』
Promotion 脚本支持将 SOA Policy Gateway Basic Runtime 或 SOA Policy Gateway Advanced Runtime 模式与预部署的 SOA Policy Gateway Governance Master 模式集成。 它在 Runtime 和 Governance 模式之间建立跨单元安全性，同时可选择将 WSRR 提升配置到 Governance Master 中。

第 38 页的『脚本: SOA Policy Gateway 2.0.0.0 - DataPower Domain』
DataPower Domain 脚本在部署期间供应 DataPower 域。该脚本在单个 DataPower 域和 WSRR 运行时之间配置连接。与 WSRR 运行时连接的每个 DataPower 域需要单独的 DataPower Domain 脚本。

部件

以下部件组成了 IBM SOA Policy Gateway Pattern。

DB2 Enterprise 部件

DB2 Enterprise 部件提供了一些配置选项。

在下表中描述了 DB2 Enterprise 9.7.5 虚拟系统映像的可配置参数:

表 2. 可配置的参数

参数名称	描述
虚拟 CPU 数	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	分配给此虚拟机的内存量（以兆字节为单位）。
密码 (db2inst1)	操作系统的用户标识 db2inst1 的密码。此用户标识用作 DB2 实例的安装所有者以及数据库和模式的所有者。
确认密码	确认 db2inst1 密码。
密码 (db2fenc1)	用于在 DB2 数据库使用的地址空间外部运行用户定义的函数 (UDF) 和存储过程的用户标识的密码。受防护用户是能够使用减少的操作系统权限运行某些存储过程（“受防护”存储过程）的用户。这可帮助阻止受防护存储过程覆盖实例文件，因为操作系统将阻止这种情况。
确认密码	确认 db2fenc1 密码。
密码 (dasusr1)	用于在系统上运行 DB2 管理服务器的 DB2 管理服务器用户的用户标识。缺省用户为 dasusr1，并且缺省组为 dasadm1。此用户标识还由 DB2 GUI 工具用于针对本地服务器数据库实例和数据库执行管理任务。
确认密码	确认 dasusr1 密码。
密码 (root)	root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	确认 root 密码。
密码 (virtuser)	操作系统的 virtuser 用户标识的密码。此用户标识用作虚拟机的非 root 用户标识。
确认密码	确认 virtuser 密码。

其他参数将从基本虚拟系统模式继承并且将被锁定。

SOA Policy Gateway Basic Runtime 模式的 DB2 Enterprise 部件配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 3. 可配置的参数

参数名称	必需	缺省值	描述
虚拟 CPU 数	是	1	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	是	2048	分配给此虚拟机的内存量（以兆字节为单位）。
密码 (db2inst1)	是		操作系统的用户标识 db2inst1 的密码。此用户标识用作 DB2 实例的安装所有者以及数据库和模式的所有者。
确认密码	是		确认 db2inst1 密码。

表 3. 可配置的参数 (续)

参数名称	必需	缺省值	描述
密码 (db2fenc1)	是		用于在 DB2 数据库使用的地址空间外部运行用户定义的函数 (UDF) 和存储过程的用户标识的密码。受防护用户是能够使用减少的操作系统权限运行某些存储过程（“受防护”存储过程）的用户。这可帮助阻止受防护存储过程覆盖实例文件，因为操作系统将阻止这种情况。
确认密码	是		确认 db2fenc1 密码。
密码 (dasusr1)	是		用于在系统上运行 DB2 管理服务器的 DB2 管理服务器用户的用户标识。缺省用户为 dasusr1，并且缺省组为 dasadm1。此用户标识还由 DB2 GUI 工具用于针对本地服务器数据库实例和数据库执行管理任务。
确认密码	是		确认 dasusr1 密码。
密码 (root)	是		root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	是		确认 root 密码。
密码 (virtuser)	是		操作系统的 virtuser 用户标识的密码。此用户标识用作虚拟机的非 root 用户标识。
确认密码	是		确认 virtuser 密码。

SOA Policy Gateway Basic Runtime Sample 模式的 DB2 Enterprise 部件配置参数

在 SOA Policy Gateway Basic Runtime Sample 中，为所有参数预配置了缺省值。

表 4. 已配置的参数

参数名称	必需	缺省值	描述
虚拟 CPU 数	是	1	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	是	2048	分配给此虚拟机的内存量（以兆字节为单位）。
密码 (db2inst1)	是	password	操作系统的用户标识 db2inst1 的密码。此用户标识用作 DB2 实例的安装所有者以及数据库和模式的所有者。
确认密码	是	password	确认 db2inst1 密码。
密码 (db2fenc1)	是	password	用于在 DB2 数据库使用的地址空间外部运行用户定义的函数 (UDF) 和存储过程的用户标识的密码。受防护用户是能够使用减少的操作系统权限运行某些存储过程（“受防护”存储过程）的用户。这可帮助阻止受防护存储过程覆盖实例文件，因为操作系统将阻止这种情况。
确认密码	是	password	确认 db2fenc1 密码。
密码 (dasusr1)	是	password	用于在系统上运行 DB2 管理服务器的 DB2 管理服务器用户的用户标识。缺省用户为 dasusr1，并且缺省组为 dasadm1。此用户标识还由 DB2 GUI 工具用于针对本地服务器数据库实例和数据库执行管理任务。
确认密码	是	password	确认 dasusr1 密码。
密码 (root)	是	password	root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	是	password	确认 root 密码。

表 4. 已配置的参数 (续)

参数名称	必需	缺省值	描述
密码 (virtuser)	是	password	操作系统的 virtuser 用户标识的密码。此用户标识用作虚拟机的非 root 用户标识。
确认密码	是	password	确认 virtuser 密码。

DB2 Enterprise HADR Primary 部件

DB2 Enterprise HADR Primary 部件提供了一些配置选项。

在下表中描述了 DB2 Enterprise HADR Primary 部件的可配置参数:

表 5. 可配置的参数

参数名称	描述
虚拟 CPU 数	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	分配给此虚拟机的内存量（以兆字节为单位）。
密码 (db2inst1)	操作系统的用户标识 db2inst1 的密码。此用户标识用作 DB2 实例的安装所有者以及数据库和模式的所有者。
确认密码	确认 db2inst1 密码。
密码 (db2fenc1)	用于在 DB2 数据库使用的地址空间外部运行用户定义的函数 (UDF) 和存储过程的用户标识的密码。受防护用户是能够使用减少的操作系统权限运行某些存储过程（“受防护”存储过程）的用户。这可帮助阻止受防护存储过程覆盖实例文件，因为操作系统将阻止这种情况。
确认密码	确认 db2fenc1 密码。
密码 (dasusr1)	用于在系统上运行 DB2 管理服务器的 DB2 管理服务器用户的用户标识的密码。缺省用户为 dasusr1，并且缺省组为 dasadm1。此用户标识还由 DB2 GUI 工具用于针对本地服务器数据库实例和数据库执行管理任务。
确认密码	确认 dasusr1 密码。
密码 (root)	root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	确认 root 密码。
密码 (virtuser)	操作系统的 virtuser 用户标识的密码。此用户标识用作虚拟机的非 root 用户标识。
确认密码	确认 virtuser 密码。

其他参数将从基本虚拟系统模式继承并且将被锁定。

SOA Policy Gateway Advanced Runtime 模式的 DB2 Enterprise HADR Primary 部件配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 6. 可配置的参数

参数名称	必需	缺省值	描述
虚拟 CPU 数	是	1	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	是	2048	分配给此虚拟机的内存量（以兆字节为单位）。

表 6. 可配置的参数 (续)

参数名称	必需	缺省值	描述
密码 (db2inst1)	是		操作系统的用户标识 db2inst1 的密码。此用户标识用作 DB2 实例的安装所有者以及数据库模式的所有者。
确认密码	是		确认 db2inst1 密码。

表 6. 可配置的参数 (续)

参数名称	必需	缺省值	描述
密码 (db2fenc1)	是		用于在 DB2 数据库用地址空间外部运行用户定义函数 (UDF) 和存储过程用户的密码。受防护例程能够使用少量操作系统权限运行某些存储过程（“受防护”存储过程）用户。这可帮助阻止受防护存储过程覆盖文件，因为

表 6. 可配置的参数 (续)

参数名称	必需	缺省值	描述
确认密码	是		确认 db2fenc1 密码。

表 6. 可配置的参数 (续)

参数名称	必需	缺省值	描述
密码 (dasusr1)	是		用于在系统上运行 DB2 管理服务器的 DB2 管理服务器用户的用户标识的密码。缺省用户为 dasusr1，并且缺省组为 dasadm1。此用户标识还由 DB2 GUI 工具用于对本地数据库实例和数据库执行管理任务。

表 6. 可配置的参数 (续)

参数名称	必需	缺省值	描述
确认密码	是		确认 dasusr1 密码。
密码 (root)	是		root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	是		确认 root 密码。
密码 (virtuser)	是		操作系统的 virtuser 用户标识的密码。此用户标识用作虚拟机的非 root 用户标识。
确认密码	是		确认 virtuser 密码。

SOA Policy Gateway Governance Master 模式的 DB2 Enterprise HADR Primary 部件配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 7. 可配置的参数

参数名称	必需	缺省值	描述
虚拟 CPU 数	是	1	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	是	2048	分配给此虚拟机的内存量（以兆字节为单位）。
密码 (db2inst1)	是		操作系统的用户标识 db2inst1 的密码。此用户标识用作 DB2 实例的安装所有者以及数据库和模式的所有者。
确认密码	是		确认 db2inst1 密码。
密码 (db2fenc1)	是		用于在 DB2 数据库使用的地址空间外部运行用户定义的函数 (UDF) 和存储过程的用户标识的密码。受防护用户是能够使用减少的操作系统权限运行某些存储过程（“受防护”存储过程）的用户。这可帮助阻止受防护存储过程覆盖实例文件，因为操作系统将阻止这种情况。
确认密码	是		确认 db2fenc1 密码。
密码 (dasusr1)	是		用于在系统上运行 DB2 管理服务器的 DB2 管理服务器用户的用户标识的密码。缺省用户为 dasusr1，并且缺省组为 dasadm1。此用户标识还由 DB2 GUI 工具用于针对本地服务器数据库实例和数据库执行管理任务。
确认密码	是		确认 dasusr1 密码。
密码 (root)	是		root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	是		确认 root 密码。
密码 (virtuser)	是		操作系统的 virtuser 用户标识的密码。此用户标识用作虚拟机的非 root 用户标识。

表 7. 可配置的参数 (续)

参数名称	必需	缺省值	描述
确认密码	是		确认 virtuser 密码。

DB2 Enterprise HADR Standby 部件

DB2 Enterprise HADR Standby 部件提供了一些配置选项。

表 8. 可配置的参数

参数名称	描述
虚拟 CPU 数	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	分配给此虚拟机的内存量（以兆字节为单位）。
密码 (db2inst1)	操作系统的用户标识 db2inst1 的密码。此用户标识用作 DB2 实例的安装所有者以及数据库和模式的所有者。
确认密码	确认 db2inst1 密码。
密码 (db2fenc1)	用于在 DB2 数据库使用的地址空间外部运行用户定义的函数 (UDF) 和存储过程的用户标识的密码。受防护用户是能够使用减少的操作系统权限运行某些存储过程（“受防护”存储过程）的用户。这可帮助阻止受防护存储过程覆盖实例文件，因为操作系统将阻止这种情况。
确认密码	确认 db2fenc1 密码。
密码 (dasusr1)	用于在系统上运行 DB2 管理服务器的 DB2 管理服务器用户的用户标识的密码。缺省用户为 dasusr1，并且缺省组为 dasadm1。此用户标识还由 DB2 GUI 工具用于针对本地服务器数据库实例和数据库执行管理任务。
确认密码	确认 dasusr1 密码。
密码 (root)	root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	确认 root 密码。
密码 (virtuser)	操作系统的 virtuser 用户标识的密码。此用户标识用作虚拟机的非 root 用户标识。
确认密码	确认 virtuser 密码。

其他参数将从基本虚拟系统模式继承并且将被锁定。

SOA Policy Gateway Advanced Runtime 模式的 DB2 Enterprise HADR Standby 部件配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 9. 可配置的参数

参数名称	必需	缺省值	描述
虚拟 CPU 数	是	1	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	是	2048	分配给此虚拟机的内存量（以兆字节为单位）。
密码 (db2inst1)	是		操作系统的用户标识 db2inst1 的密码。此用户标识用作 DB2 实例的安装所有者以及数据库和模式的所有者。
确认密码	是		确认 db2inst1 密码。

表 9. 可配置的参数 (续)

参数名称	必需	缺省值	描述
密码 (db2fenc1)	是		用于在 DB2 数据库使用的地址空间外部运行用户定义的函数 (UDF) 和存储过程的用户标识的密码。受防护用户是能够使用减少的操作系统权限运行某些存储过程（“受防护”存储过程）的用户。这可帮助阻止受防护存储过程覆盖实例文件，因为操作系统将阻止这种情况。
确认密码	是		确认 db2fenc1 密码。
密码 (dasusr1)	是		用于在系统上运行 DB2 管理服务器的 DB2 管理服务器用户的用户标识的密码。缺省用户为 dasusr1，并且缺省组为 dasadm1。此用户标识还由 DB2 GUI 工具用于针对本地服务器数据库实例和数据库执行管理任务。
确认密码	是		确认 dasusr1 密码。
密码 (root)	是		root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	是		确认 root 密码。
密码 (virtuser)	是		操作系统的 virtuser 用户标识的密码。此用户标识用作虚拟机的非 root 用户标识。
确认密码	是		确认 virtuser 密码。

SOA Policy Gateway Governance Master 模式的 DB2 Enterprise HADR Standby 部件配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 10. 可配置的参数

参数名称	必需	缺省值	描述
虚拟 CPU 数	是	1	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	是	2048	分配给此虚拟机的内存量（以兆字节为单位）。
密码 (db2inst1)	是		操作系统的用户标识 db2inst1 的密码。此用户标识用作 DB2 实例的安装所有者以及数据库和模式的所有者。
确认密码	是		确认 db2inst1 密码。
密码 (db2fenc1)	是		用于在 DB2 数据库使用的地址空间外部运行用户定义的函数 (UDF) 和存储过程的用户标识的密码。受防护用户是能够使用减少的操作系统权限运行某些存储过程（“受防护”存储过程）的用户。这可帮助阻止受防护存储过程覆盖实例文件，因为操作系统将阻止这种情况。
确认密码	是		确认 db2fenc1 密码。
密码 (dasusr1)	是		用于在系统上运行 DB2 管理服务器的 DB2 管理服务器用户的用户标识的密码。缺省用户为 dasusr1，并且缺省组为 dasadm1。此用户标识还由 DB2 GUI 工具用于针对本地服务器数据库实例和数据库执行管理任务。
确认密码	是		确认 dasusr1 密码。
密码 (root)	是		root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	是		确认 root 密码。

表 10. 可配置的参数 (续)

参数名称	必需	缺省值	描述
密码 (virtuser)	是		操作系统的 virtuser 用户标识的密码。此用户标识用作虚拟机的非 root 用户标识。
确认密码	是		确认 virtuser 密码。

WSRR 独立服务器部件

WSRR 独立服务器部件提供了一些配置选项。

下表中描述了 WSRR 独立服务器部件的可配置参数:

表 11. 已配置的参数

参数名称	描述
虚拟 CPU 数	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	分配给此虚拟机的内存量（以兆字节为单位）。
密码 (root)	root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	确认“密码 (root)”的用户输入。
WebSphere 管理用户名	WebSphere 环境管理用户名。
WebSphere 管理密码	WebSphere 环境管理用户密码。
确认密码	确认“WebSphere 管理密码”的用户输入。
预留物理内存	预留以供此虚拟机专用的物理内存。

其他参数将从基本虚拟系统模式继承并且将被锁定。

SOA Policy Gateway Basic Runtime 模式的 WSRR 独立服务器部件配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 12. 可配置的参数

参数名称	必需	缺省值	描述
虚拟 CPU 数	是	1	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	是	4096	分配给此虚拟机的内存量（以兆字节为单位）。
预留物理内存	是	False	预留以供此虚拟机专用的物理内存。
单元名称	是	SOAPolicyBasicCell	Basic Runtime 模式下虚拟机上的 WebSphere 单元名。
节点名	是	SOAPolicyBasicNode	Basic Runtime 模式下虚拟机上的 WebSphere 节点名。
密码 (root)	是		root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	是		确认“密码 (root)”的用户输入。
WebSphere 管理用户名	是	virtuser	WebSphere 环境管理用户名。
WebSphere 管理密码	是		WebSphere 环境管理用户密码。
确认密码	是		确认“WebSphere 管理密码”的用户输入。

SOA Policy Gateway Basic Runtime Sample 模式的 WSRR 独立服务器部件配置参数

在 SOA Policy Gateway Basic Runtime Sample 中，为所有参数预配置了缺省值。

表 13. 已配置的参数

参数名称	必需	缺省值	描述
虚拟 CPU 数	是	1	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	是	4096	分配给此虚拟机的内存量（以兆字节为单位）。
预留物理内存	是	False	预留以供此虚拟机专用的物理内存。
密码 (root)	是	password	root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	是	password	确认“密码 (root)”的用户输入。
WebSphere 管理用户名	是	virtuser	WebSphere 环境管理用户名。
WebSphere 管理密码	是	password	WebSphere 环境管理用户密码。
确认密码	是	password	确认“WebSphere 管理密码”的用户输入。

WSRR 部署管理器部件

WSRR 部署管理器部件提供了一些配置选项。

下表中描述了 WSRR 部署管理器部件的可配置参数:

表 14. 可配置的参数

参数名称	描述
虚拟 CPU 数	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	分配给此虚拟机的内存量（以兆字节为单位）。
预留物理 CPU	预留以供此虚拟机专用的物理 CPU。
预留物理内存	预留以供此虚拟机专用的物理内存。
单元名称	Advanced Runtime 模式的 WebSphere 单元名称。
节点名	位于 Advanced Runtime 模式下部署管理器虚拟机上的 WebSphere 节点的节点名。
密码 (root)	root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	确认“密码 (root)”的用户输入。
WebSphere 管理用户名	WebSphere 环境管理用户名。
WebSphere 管理密码	WebSphere 环境管理用户密码。
确认密码	确认“WebSphere 管理密码”的用户输入。

其他参数将从基本虚拟系统模式继承并且将被锁定。

SOA Policy Gateway Advanced Runtime 模式的 WSRR 部署管理器部件配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 15. 可配置的参数

参数名称	必需	缺省值	描述
虚拟 CPU 数	是	1	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	是	2048	分配给此虚拟机的内存量（以兆字节为单位）。
预留物理 CPU	是	False	预留以供此虚拟机专用的物理 CPU。
预留物理内存	是	False	预留以供此虚拟机专用的物理内存。
单元名称	是	SOAPolicyAdvancedCell	Advanced Runtime 模式的 WebSphere 单元名称。
节点名	是	SOAPolicyAdvancedNode	位于 Advanced Runtime 模式下部署管理器虚拟机上的 WebSphere 节点的节点名。
密码 (root)	是		root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	是		确认“密码 (root)”的用户输入。
WebSphere 管理用户名	是	virtuser	WebSphere 环境管理用户名。
WebSphere 管理密码	是		WebSphere 环境管理用户密码。
确认密码	是		确认“WebSphere 管理密码”的用户输入。

SOA Policy Gateway Governance Master 模式的 WSRR 部署管理器部件配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 16. 可配置的参数

参数名称	必需	缺省值	描述
虚拟 CPU 数	是	1	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	是	2048	分配给此虚拟机的内存量（以兆字节为单位）。
预留物理 CPU	是	False	预留以供此虚拟机专用的物理 CPU。
预留物理内存	是	False	预留以供此虚拟机专用的物理内存。
单元名称	是	SOAPolicyGMCell	Advanced Runtime 模式的 WebSphere 单元名称。
节点名	是	SOAPolicyGMNode	位于 Advanced Runtime 模式下部署管理器虚拟机上的 WebSphere 节点的节点名。
密码 (root)	是		root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	是		确认“密码 (root)”的用户输入。
WebSphere 管理用户名	是	virtuser	WebSphere 环境管理用户名。
WebSphere 管理密码	是		WebSphere 环境管理用户密码。
确认密码	是		确认“WebSphere 管理密码”的用户输入。

WSRR 定制节点部件

WSRR 定制节点部件提供了一些配置选项。

下表中描述了 WSRR 定制节点部件的可配置参数:

表 17. 可配置的参数

参数名称	描述
虚拟 CPU 数	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	分配给此虚拟机的内存量（以兆字节为单位）。
预留物理 CPU	预留以供此虚拟机专用的物理 CPU。
预留物理内存	预留以供此虚拟机专用的物理内存。
单元名称	将忽略定制节点部件配置中的单元名称值。将使用在部署管理器部件配置中指定的单元名称。
节点名	位于 Advanced Runtime 模式下定制节点虚拟机上的 WebSphere 节点的节点名。
密码 (root)	root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	确认“密码 (root)”的用户输入。
WebSphere 管理用户名	WebSphere 环境管理用户名。
WebSphere 管理密码	WebSphere 环境管理用户密码。
确认密码	确认“WebSphere 管理密码”的用户输入。

其他参数将从基本虚拟系统模式继承并且将被锁定。

SOA Policy Gateway Advanced Runtime 模式的 WSRR 定制节点部件配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 18. 可配置的参数

参数名称	必需	缺省值	描述
虚拟 CPU 数	是	2	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	是	4096	分配给此虚拟机的内存量（以兆字节为单位）。
预留物理 CPU	是	False	预留以供此虚拟机专用的物理 CPU。
预留物理内存	是	False	预留以供此虚拟机专用的物理内存。
节点名	是	SOAPolicyAdvancedNode	位于 Advanced Runtime 模式下定制节点虚拟机上的 WebSphere 节点的节点名。
密码 (root)	是		root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	是		确认“密码 (root)”的用户输入。
WebSphere 管理用户名	是	virtuser	WebSphere 环境管理用户名。
WebSphere 管理密码	是		WebSphere 环境管理用户密码。
确认密码	是		确认“WebSphere 管理密码”的用户输入。

SOA Policy Gateway Governance Master 模式的 WSRR 定制节点部件配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 19. 可配置的参数

参数名称	必需	缺省值	描述
虚拟 CPU 数	是	2	为此部件表示的虚拟机分配的虚拟处理器数量。
内存大小 (MB)	是	4096	分配给此虚拟机的内存量（以兆字节为单位）。
预留物理 CPU	是	False	预留以供此虚拟机专用的物理 CPU。
预留物理内存	是	False	预留以供此虚拟机专用的物理内存。
节点名	是	SOAPolicyGMNode	位于 Advanced Runtime 模式下定制节点虚拟机上的 WebSphere 节点的节点名。
密码 (root)	是		root 用户标识的密码。这是模式中此部件所表示虚拟机的操作系统的密码。
确认密码	是		确认“密码 (root)”的用户输入。
WebSphere 管理用户名	是	virtuser	WebSphere 环境管理用户名。
WebSphere 管理密码	是		WebSphere 环境管理用户密码。
确认密码	是		确认“WebSphere 管理密码”的用户输入。

脚本程序包

随 IBM SOA Policy Gateway Pattern 提供了 4 个脚本程序包。

此模式随附的脚本程序包有:

- SOA Policy Gateway 2.0.0.0 - DataPower Domain
- SOA Policy Gateway 2.0.0.0 - Promotion
- SOA Policy Gateway 2.0.0.0 - Samples
- SOA Policy Gateway 2.0.0.0 - Security

脚本: SOA Policy Gateway 2.0.0.0 - DataPower Domain

DataPower Domain 脚本在部署期间供应 DataPower 域。该脚本在单个 DataPower 域和 WSRR 运行时之间配置连接。与 WSRR 运行时连接的每个 DataPower 域需要单独的 DataPower Domain 脚本。

参数

表 20. 可配置的参数

参数名称	描述
DataPower_hostname	样本应用程序将安装在的 DataPower 设备的主机名。
DataPower_XML_mgmt_port	用于 DataPower XML 管理接口的端口，通常是 5550。
Datapower_admin_id	具有使用 XML 管理接口的适当许可权的管理员用户标识。
DataPower_admin_password	DataPower_admin_id 的密码。
确认密码	确认 DataPower_admin_password 的用户输入。

表 20. 可配置的参数 (续)

参数名称	描述
New_DataPower_domain	要在 DataPower 设备上创建的新域名。它不得与任何现有域匹配，否则脚本程序包将失败或退出。值不能包含任何空格。
securityFileCleanUp	确定是否已从运行脚本程序包的 WSRR 实例中删除上载到 DataPower 的 DomainZipFile.zip 文件和 WSRR 证书。如果未除去该文件，那么当证书仍在该实例上时，这将是一个安全风险。

SOA Policy Gateway Basic Runtime 模式的 SOA Policy Gateway 2.0.0.0 - DataPower Domain 脚本配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 21. 可配置的参数

参数名称	必需	缺省值	描述
DataPower_hostname	是		样本应用程序将安装在的 DataPower 设备的主机名。
DataPower_XML_mgmt_port	是	5550	用于 DataPower XML 管理接口的端口，通常是 5550。
Datapower_admin_id	是		具有使用 XML 管理接口的适当许可权的管理员用户标识。
DataPower_admin_password	是		DataPower_admin_id 的密码。
确认密码	是		确认 DataPower_admin_password 的用户输入。
New_DataPower_domain	是		要在 DataPower 设备上创建的新域名。它不得与任何现有域匹配，否则脚本程序包将失败或退出。值不能包含任何空格。
Remove_security_files	是	true	确定是否已从运行脚本程序包的 WSRR 实例中删除上载到 DataPower 的 DomainZipFile.zip 文件和 WSRR 证书。如果未除去该文件，那么当证书仍在该实例上时，这将是一个安全风险。

SOA Policy Gateway Advanced Runtime 模式的 SOA Policy Gateway 2.0.0.0 - DataPower Domain 脚本配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 22. 可配置的参数

参数名称	必需	缺省值	描述
DataPower_hostname	是		样本应用程序将安装在的 DataPower 设备的主机名。
DataPower_XML_mgmt_port	是	5550	用于 DataPower XML 管理接口的端口，通常是 5550。
Datapower_admin_id	是		具有使用 XML 管理接口的适当许可权的管理员用户标识。
DataPower_admin_password	是		DataPower_admin_id 的密码。
确认密码	是		确认 DataPower_admin_password 的用户输入。
New_DataPower_domain	是		要在 DataPower 设备上创建的新域名。它不得与任何现有域匹配，否则脚本程序包将失败或退出。值不能包含任何空格。
Remove_security_files	是	true	确定是否已从运行脚本程序包的 WSRR 实例中删除上载到 DataPower 的 DomainZipFile.zip 文件和 WSRR 证书。如果未除去该文件，那么当证书仍在该实例上时，这将是一个安全风险。

脚本: SOA Policy Gateway 2.0.0.0 - Promotion

Promotion 脚本支持将 SOA Policy Gateway Basic Runtime 或 SOA Policy Gateway Advanced Runtime 模式与预部署的 SOA Policy Gateway Governance Master 模式集成。它在 Runtime 和 Governance 模式之间建立跨单元安全性，同时可选择将 WSRR 提升配置到 Governance Master 中。

参数

表 23. 可配置的参数

参数名称	描述
WSRR_GOV_DMGR_hostname	WSRR 集群的部署管理器的主机名。
WSRR_GOV_DMGR_cellname	WSRR 集群的 WebSphere 单元名称。
WSRR_GOV_admin_user	WebSphere WSRR 管理单元的管理标识。
WSRR_GOV_admin_password	WebSphere WSRR 监管单元的管理标识的密码。
确认密码	确认 WSRR_GOV_admin_password 的用户输入。
Promotion_environment	必须为 staging、production 或 Unset 之一。这些值区分大小写，并且必须准确匹配。
LTPA_key_password	LTPA 密钥将在来自 Governance Master 的脚本程序包期间导出和使用，并在提升环境中的所有单元中使用。这是在导出该 LTPA 密钥时使用的密码。
确认密码	确认 LTPA_key_password 的用户输入。

SOA Policy Gateway Basic Runtime 模式的 SOA Policy Gateway 2.0.0.0 - Promotion 脚本配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 24. 可配置的参数

参数名称	必需	缺省值	描述
WSRR_GOV_DMGR_hostname	是		WSRR 集群的部署管理器的主机名。
WSRR_GOV_DMGR_cellname	是		WSRR 集群的 WebSphere 单元名称。
WSRR_GOV_admin_user	是		WebSphere WSRR 管理单元的管理标识。
WSRR_GOV_admin_password	是		WebSphere WSRR 监管单元的管理标识的密码。
确认密码	是		确认 WSRR_GOV_admin_password 的用户输入。
Promotion_environment	是		必须为 staging、production 或 Unset 之一。这些值区分大小写，并且必须准确匹配。
LTPA_key_password	是		LTPA 密钥将在来自 Governance Master 的脚本程序包期间导出和使用，并在提升环境中的所有单元中使用。这是在导出该 LTPA 密钥时使用的密码。
确认密码	是		确认 LTPA_key_password 的用户输入。

SOA Policy Gateway Advanced Runtime 模式的 SOA Policy Gateway 2.0.0.0 - Promotion 脚本配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 25. 可配置的参数

参数名称	必需	缺省值	描述
WSRR_GOV_DMGR_hostname	是		WSRR 集群的部署管理器的主机名。
WSRR_GOV_DMGR_cellname	是		WSRR 集群的 WebSphere 单元名称。
WSRR_GOV_admin_user	是		WebSphere WSRR 管理单元的管理标识。
WSRR_GOV_admin_password	是		WebSphere WSRR 监管单元的管理标识的密码。
确认密码	是		确认 WSRR_GOV_admin_password 的用户输入。
Promotion_environment	是		必须为 staging、production 或 Unset 之一。这些值区分大小写，并且必须准确匹配。
LTPA_key_password	是		LTPA 密钥将在来自 Governance Master 的脚本程序包期间导出和使用，并在提升环境中的所有单元中使用。这是在导出该 LTPA 密钥时使用的密码。
确认密码	是		确认 LTPA_key_password 的用户输入。

脚本: SOA Policy Gateway 2.0.0.0 - Sample

Sample 脚本配置了样本应用程序参数以用于 SOA Policy Gateway Basic Runtime Sample 模式。

参数

注: 任何需要值 Unset 的参数都区分大小写。

表 26. 可配置的参数

参数名称	描述
SCP_host	包含 `DomainZipFile.zip` 的 SCP 服务器的主机名。
SCP_user	用于连接到 SCP 服务器的用户名。
SCP_password	用于登录 SCP 服务器的密码。
确认密码	确认 SCP_password 的用户输入。
SCP_zip_location	`DomainZipFile.zip` 的 URI 位置。例如，`/files/DomainZipFile.zip`。
CLIENT_PUBLIC_KEY_file	用于连接到 DataPower 设备 XML 管理接口端口的 PEM 证书文件的名称。仅对服务器认证且在不使用 SSL 的情况下使用“Unset”值。
CLIENT_PUBLIC _KEY_password	用于连接到 DataPower 设备 XML 管理接口端口的公用证书的密码。如果未使用任何密码，该值为“Unset”。
确认密码	确认 CLIENT_PUBLIC_KEY_password 的用户输入。
CLIENT_PRIVATE_KEY_file	用于连接到 DataPower 设备 XML 管理接口端口的 PEM 密钥文件的名称。此参数对于相互认证而言是必需的。仅对服务器认证且在不使用 SSL 的情况下使用“Unset”值。
CLIENT_PRIVATE_KEY_password	用于连接到 DataPower 设备 XML 管理接口端口的密钥文件的密码。此参数对于相互认证而言是必需的。如果未使用任何密码，该值为“Unset”。

表 26. 可配置的参数 (续)

参数名称	描述
确认密码	确认 CLIENT_PRIVATE_KEY_password 的用户输入。
CLI_FILE_file	包含在 DomainZipFile.zip 文件中的 CLI 文件的名称。此 CLI 在域安装和 WSRR 服务器配置的末尾执行。
确认密码	确认 LTPA_KEY_password 的用户输入。
DataPower_hostname	样本应用程序将安装在的 DataPower 设备的主机名。
DataPower_XML_mgmt_port	用于 DataPower XML 管理接口的端口。
DataPower_admin_id	具有使用 XML 管理接口的适当许可权的管理员用户标识。
DataPower_admin_password	DataPower_admin_id 的密码。
确认密码	确认 DataPower_admin_password 的用户输入。
SOAPolicySample_DataPower_domain	样本域名。它不得与 DataPower 设备上的任何现有域匹配。
SamplePolicySample_starting_port	应用程序需要 5 个空闲端口，将根据此值按顺序使用这 5 个端口。例如，如果值为 62000，那么将使用端口 62000-62004。关于这些端口是否空闲，脚本不会执行任何检查。
LDAP_hostname	样本使用 LDAP 服务器，这是该服务器的主机名。
LDAP_port	LDAP 服务器的非安全端口。通常为 389。
LDAP_password	与 LDAP_DN 绑定时所使用的密码。
确认密码	确认 LDAP_password 的用户输入。
LDAP_DN	用于绑定到 LDAP 的专有名称。例如，cn=root、dc=ibm.com。

SOA Policy Gateway Basic Runtime Sample 模式的 SOA Policy Gateway 2.0.0.0 - Sample 脚本配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

注: 任何需要值 Unset 的参数都区分大小写。

表 27. 可配置的参数

参数名称	必需	缺省值	描述
SCP_host	是		包含 DomainZipFile.zip 的 SCP 服务器的主机名。
SCP_user	是		用于连接到 SCP 服务器的用户名。
SCP_password	是		用于登录 SCP 服务器的密码。
确认密码	是		确认 SCP_password 的用户输入。
SCP_zip_location	是		DomainZipFile.zip 的 URI 位置。例如，/files/DomainZipFile.zip。
CLIENT_PUBLIC_KEY_file	是		用于连接到 DataPower 设备 XML 管理接口端口的 PEM 证书文件的名称。仅对服务器认证且在不使用 SSL 的情况下使用“Unset”值。

表 27. 可配置的参数 (续)

参数名称	必需	缺省值	描述
CLIENT_PUBLIC_KEY_password	是		用于连接到 DataPower 设备 XML 管理接口端口的公用证书的密码。如果未使用任何密码，该值为“Unset”。
确认密码	是		确认 CLIENT_PUBLIC_KEY_password 的用户输入。
CLIENT_PRIVATE_KEY_file	是		用于连接到 DataPower 设备 XML 管理接口端口的 PEM 密钥文件的名称。此参数对于相互认证而言是必需的。仅对服务器认证且在不使用 SSL 的情况下使用“Unset”值。
CLIENT_PRIVATE_KEY_password	是		用于连接到 DataPower 设备 XML 管理接口端口的密钥文件的密码。此参数对于相互认证而言是必需的。如果未使用任何密码，该值为“Unset”。
确认密码	是		确认 CLIENT_PRIVATE_KEY_password 的用户输入。
DataPower_hostname	是		样本应用程序将安装在的 DataPower 设备的主机名。
DataPower_XML_mgmt_port	是	5550	用于 DataPower XML 管理接口的端口。
DataPower_admin_id	是		具有使用 XML 管理接口的适当许可权的管理员用户标识。
DataPower_admin_password	是		DataPower_admin_id 的密码。
确认密码	是		确认 DataPower_admin_password 的用户输入。
SOAPolicySample_DataPower_domain	是	SOAPolicySample	样本域名。它不得与 DataPower 设备上的任何现有域匹配。
SOAPolicySample_starting_port	是	62001	应用程序需要 5 个空闲端口，将根据此值按顺序使用这 5 个端口。例如，如果值为 62000，那么将使用端口 62000-62004。关于这些端口是否空闲，脚本不会执行任何检查。
LDAP_hostname	是		样本使用 LDAP 服务器，这是该服务器的主机名。

表 27. 可配置的参数 (续)

参数名称	必需	缺省值	描述
LDAP_port	是	389	LDAP 服务器的非安全端口。通常为 389。
LDAP_password	是		与 LDAP_DN 绑定时所使用的密码。
确认密码	是		确认 LDAP_password 的用户输入。
LDAP_DN	是		用于绑定到 LDAP 的专有名称。例如，cn=root、dc=ibm.com。

脚本: SOA Policy Gateway 2.0.0.0 - Security

Security 脚本将 ZIP 文件中包含的与 DataPower 设备进行通信所需的安全信息从支持 Linux 安全复制程序 (SCP) 的外部文件服务器复制到部署管理器或 WSRR 机器。

复制的安全文件包含以下内容:

- DPC 访问证书
- DPC 访问公用证书
- DPC 专用密钥
- DP CLI 脚本
- 证书链的文件夹

DataPower 的命令行界面 (CLI) 脚本允许您在模式部署阶段期间配置已部署的域。

注: 应在部署之后从外部文件服务器中删除机密安全证书。

参数

表 28. 可配置的参数

参数名称	描述
SCP_host	包含 `DomainZipFile.zip` 文件的 SCP 服务器的主机名。
SCP_user	用于连接到 SCP 服务器的用户名。
SCP_password	用于登录 SCP 服务器的密码。
确认密码	确认 SCP_password 的用户输入。
SCP_zip_location	`DomainZipFile.zip` 文件的 URI 位置；例如，`/files/DomainZipFile.zip`。
CLIENT_PUBLIC_KEY_file	用于连接到 DataPower 设备 XML 管理接口端口的 PEM 证书文件的名称。
CLIENT_PUBLIC_KEY_password	用于连接到 DataPower 设备 XML 管理接口端口的客户机证书的密码。此参数对于相互认证而言是必需的（如果可用）。如果未使用任何密码，该值可以是“Unset”。
CLIENT_PRIVATE_KEY_file	用于连接到 DataPower 设备 XML 管理接口端口的 PEM 密钥文件的名称。此参数对于相互认证而言是必需的。

表 28. 可配置的参数 (续)

参数名称	描述
CLIENT_PRIVATE_KEY_password	用于连接到 DataPower 设备 XML 管理接口端口的密钥文件的密码。此参数对于相互认证而言是必需的。如果未使用任何密码，该值可以是“Unset”。
CLI_file	包含在 DomainZipFile.zip 中的 CLI 文件的名称。此 CLI 在域安装和 WSRR 服务器配置的末尾运行。

SOA Policy Gateway Basic Runtime 模式的 SOA Policy Gateway 2.0.0.0 - Security 脚本配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 29. 可配置的参数

参数名称	必需	缺省值	描述
SCP_host	是		包含 DomainZipFile.zip 文件的 SCP 服务器的主机名。
SCP_user	是		用于连接到 SCP 服务器的用户名。
SCP_password	是		用于登录 SCP 服务器的密码。
确认密码	是		确认 SCP_password 的用户输入。
SCP_zip_location	是		DomainZipFile.zip 文件的 URI 位置；例如，/files/DomainZipFile.zip。
CLIENT_PUBLIC_KEY_file	是		用于连接到 DataPower 设备 XML 管理接口端口的 PEM 证书文件的名称。
CLIENT_PUBLIC_KEY_password	是		用于连接到 DataPower 设备 XML 管理接口端口的客户机证书的密码。此参数对于相互认证而言是必需的（如果可用）。如果未使用任何密码，该值可以是“Unset”。
CLIENT_PRIVATE_KEY_file	是		用于连接到 DataPower 设备 XML 管理接口端口的 PEM 密钥文件的名称。此参数对于相互认证而言是必需的。
CLIENT_PRIVATE_KEY_password	是		用于连接到 DataPower 设备 XML 管理接口端口的密钥文件的密码。此参数对于相互认证而言是必需的。如果未使用任何密码，该值可以是“Unset”。
CLI_file	是	Unset	包含在 DomainZipFile.zip 中的 CLI 文件的名称。此 CLI 在域安装和 WSRR 服务器配置的末尾运行。

SOA Policy Gateway Advanced Runtime 模式的 SOA Policy Gateway 2.0.0.0 - Security 脚本配置参数

必须先配置没有缺省值的必需参数，才能部署该模式。

表 30. 可配置的参数

参数名称	必需	缺省值	描述
SCP_zip_location	是		DomainZipFile.zip 文件的 URI 位置；例如，/files/DomainZipFile.zip。
SCP_host	是		包含 DomainZipFile.zip 文件的 SCP 服务器的主机名。
SCP_user	是		用于连接到 SCP 服务器的用户名。
SCP_password	是		用于登录 SCP 服务器的密码。
确认密码	是		确认 SCP_password 的用户输入。

表 30. 可配置的参数 (续)

参数名称	必需	缺省值	描述
CLIENT_PUBLIC_KEY_file	是		用于连接到 DataPower 设备 XML 管理接口端口的 PEM 证书文件的名称。
CLIENT_PUBLIC_KEY_password	是		用于连接到 DataPower 设备 XML 管理接口端口的客户机证书的密码。此参数对于相互认证而言是必需的（如果可用）。如果未使用任何密码，该值可以是“Unset”。
CLIENT_PRIVATE_KEY_file	是		用于连接到 DataPower 设备 XML 管理接口端口的 PEM 密钥文件的名称。此参数对于相互认证而言是必需的。
CLIENT_PRIVATE_KEY_password	是		用于连接到 DataPower 设备 XML 管理接口端口的密钥文件的密码。此参数对于相互认证而言是必需的。如果未使用任何密码，该值可以是“Unset”。
CLI_file	是	Unset	包含在 `DomainZipFile.zip` 中的 CLI 文件的名称。此 CLI 在域安装和 WSRR 服务器配置的末尾运行。

第 5 章 使用 IBM SOA Policy Gateway Pattern

IBM SOA Policy Gateway Pattern 针对生成产品的拓扑的可重复部署提供模式定义。每个模式都在 IBM SOA Policy Gateway Pattern 中提供一个特定功能，并且包含多个映像以支持各个模式。在部署前，必须根据业务需求配置模式。

在部署过程中，需要配置部分参数。有关更多信息，请参阅第 56 页的『部署模式』。

相关任务:

第 9 页的第 3 章，『IBM SOA Policy Gateway Pattern 入门』
此模式使用 WebSphere DataPower 来控制使用 WSRR 中的受管策略和服务定义的消息。请查看本部分中的主题，以了解此场景中涉及的内容、企业可能想要采用此场景的原因、涉及的用户角色以及通过产品交付的功能的概述。

规划模式配置和模式先决条件

IBM SOA Policy Gateway Pattern 提供一种方式以快速可靠地供应环境，用于监管服务定义和策略以及执行这些策略。确定所需的监管需求和资源。

要部署环境，请准备 DataPower 设备进行远程管理，并收集与设备安全通信所需的资产。可通过部署 SOA Policy Gateway Basic Runtime Sample 来完成测试环境，这将确认环境是否已正确配置以进行部署并演示策略的执行情况。在验证环境之后，使用 WSRR 最佳实践决定期望的 IBM SOA Policy Gateway Pattern 监管和运行时配置。模式部署自 Governance Master 开始，后跟与期望配置匹配的运行时模式。

准备和部署 IBM SOA Policy Gateway Pattern

准备 DataPower 并收集安全性文件:

1. 准备 DataPower 设备进行远程管理。有关更多信息，请参阅第 48 页的『为 IBM SOA Policy Gateway Pattern 配置 DataPower』。
2. 如果 DataPower 设备受到保护，请阅读 DataPower 的安全性部分，然后收集与其进行通信所需的 DataPower 安全性文件。
3. 确认云环境中的系统 DataPower 可以与设备进行通信，并且设备可以与已部署的系统进行通信。

在创建生产部署之前，SOA Policy Gateway Basic Runtime Sample 可用于演示模式的功能。如果需要使用 Basic Runtime Sample，请完成以下步骤:

1. 在 Linux 上提供可通过云中已部署系统进行访问的 SCP 服务器。SCP 是安全复制命令。 SCP 服务器提供一种方式来托管模式外部的安全性文件，因此无需对每个安全性配置更改模式。
2. 提供 LDAP 服务器来托管 DataPower 中实施的样本应用程序所使用的安全性标识。有关更多信息，请参阅第 55 页的『为样本配置 LDAP』。
3. 部署 SOA Policy Gateway Basic Runtime Sample 模式以验证基础结构。有关更多信息，请参阅第 57 页的『部署 SOA Policy Gateway Basic Runtime Sample 模式』。
4. 样本使用完成时，将不需要 LDAP 服务器。

准备生产部署:

1. 确定部署需要的规模。为 Governance Master 和运行时部署确定集群大小。

   注: 在部署集群时，不能使用另一个集群成员扩展该集群。
2. 定义 Governance Master 的单元名、管理用户标识和密码。
3. 在 SCP 服务器上托管 DataPower 安全性 `DomainZipFile.zip` 文件。有关更多信息，请参阅第 49 页的『创建安全性 `DomainZipFile.zip`』。

为生产环境部署 Governance Master:

1. 部署 SOA Policy Gateway Governance Master 模式。等待该部署完成，然后再部署生产环境运行时模式。有关更多信息，请参阅第 58 页的『部署 SOA Policy Gateway Governance Master 模式』。

部署生产环境运行时模式:

1. 确定需要集群环境还是独立环境。
2. 如果需要多个 DataPower 域，请克隆 Basic Runtime 模式或 Advanced Runtime 模式，并为每个所需域将 DataPower 脚本程序包添加到克隆项。

   注: 完成该配置后，将不能添加额外的 DataPower 域。
   有关更多信息，请参阅第 63 页的『使用多个 DataPower 域进行部署』。
3. 使用 Governance Master 模式信息配置运行时模式。有关更多信息，请参阅第 59 页的『SOA Policy Gateway Governance Master 部署信息』。
4. 确定运行时将为登台运行时、生产运行时还是其他运行时。
5. 部署 Basic Runtime 或 Advanced Runtime 模式。有关更多信息，请参阅第 60 页的『部署 SOA Policy Gateway Advanced Runtime 模式』或第 59 页的『部署 SOA Policy Gateway Basic Runtime 模式』。
6. 等待直至完全部署，然后再部署另一个运行时

。

部署运行时完成后:

1. 不再需要 SCP 文件服务器。
2. 可以通过缺省的安全性配置更新 WSRR 和 WebSphere 安全性。有关更多信息，请参阅第 49 页的『安全管理』。
3. DataPower 域已准备好进行网关配置。

为 IBM SOA Policy Gateway Pattern 配置 DataPower

在运行 SOAPolicy 脚本之前，请完成以下 DataPower 配置步骤。

过程

1. 以管理员身份登录到受支持的 DataPower 设备。
2. 搜索 `XML 管理界面`。
3. 确保其状态为已启用。
4. 确保以下项处于活动状态，并且受到正确保护:
   - SOAP 管理 URI
   - SOAP 配置管理
   - SOAP 配置管理 (v2004)

- AMP 端点
- SLM 端点
- WS 管理端点
- WSDM 端点
- UDDI 预订
- WSRR 预订

IBM SOA Policy Gateway Pattern 模式的安全性

客户需要 WSRR 和 DataPower 之间不同级别的安全性，尤其是 SSL 区域。当使用 SOA Policy Gateway Basic Runtime、 SOA Policy Gateway Basic Runtime Sample 和 SOA Policy Gateway Advanced Runtime 模式时，IBM SOA Policy Gateway Pattern 在配置脚本和 DataPower 之间支持 3 级 SSL 通信。

如果不需要 SSL

如果不需要使用 SSL，那么不会提供 curl 客户机的公用密钥和专用密钥，并保留为“取消设置”。

注: 如果未使用 SSL，那么发送给 DataPower 的所有数据都未加密，包括用户和密码信息。这就存在一个安全漏洞问题。针对 DataPower 的 SOMA 调用中使用的密码不支持加密，因此，被传输到未加密的 DataPower 设备。所以，至少使用服务器端认证以确保安全性。

DataPower 应用程序与 Basic 和 Advanced 模式中脚本之间的相互认证

如果您要求在 DataPower 应用程序与 Basic 和 Advanced 模式中脚本之间相互认证:

- 必须提供 curl 客户机的公用密钥和专用密钥。

安全管理

模式中使用的 WSRR 映像和 WebSphere Application Server 映像仅具有适当的缺省安全性。要生成真正安全的环境，您需要使用标准的 WebSphere 安全性技术保证其安全。

请参阅位于以下链接的 WebSphere Network Deployment V8.0 信息中心:

- WebSphere Application Server Network Deployment（分布式平台和 Windows）V8.0: IBM WebSphere Application Server Network Deployment（分布式平台和 Windows）V8.0 信息中心
- 应用程序安全性: IBM WebSphere Application Server Network Deployment（分布式平台和 Windows）V8.0 信息中心 - 确保应用程序及其环境的安全性
- 端到端的安全性路径: IBM WebSphere Application Server Network Deployment（分布式平台和 Windows）V8.0 信息中心 - 确保应用程序及其环境的安全性

创建安全性 DomainZipFile.zip

为 SOA Policy Gateway Basic Runtime 模式、SOA Policy Gateway Advanced Runtime 模式和 SOA Policy Gateway Basic Runtime Sample 创建安全性 `DomainZipFile.zip`。

过程

使用以下规则创建 DomainZipFile.zip:

1. DomainZipFile.zip 的结构必须如下所示:

   注: 仅需要目录结构，各文件名可以遵循您选择的命名。然而，所有证书和密钥文件都必须采用 PEM 格式。

   注: 在路径中使用 DataPower 主机名将允许将不同的证书用于不同的 DataPower 设备。

表 31. Basic 和 Advanced 模式所需的文件

文件名，相对于根目录的位置	Notes®
CurlClientPublicKeyFile.crt	仅当使用相互认证才需要。仅限 PEM 格式。
CurlClientPrivateKeyFile.key	仅当使用相互认证才需要。
/*dataPowerHostName*/certificate1.crt	要上载至 WSRR 的 DataPower 证书。它要求整个证书链都采用 PEM 格式。要上载至 WSRR 的 DataPower 证书。必须仅包含以下内容: ------BEGINCERTIFICATE---- to -----END CERTIFICATE----- 文件扩展名必须为 .crt 或 .pem。
/*dataPowerHostName*/certificate2.crt	文件扩展名必须为 .crt 或 .pem
/*dataPowerHostName*/certificate3.crt	文件扩展名必须为 .crt 或 .pem

2. 仅针对 SOA Policy Gateway Advanced Runtime 模式，添加要运行的 cli 文件（可选）:

表 32. Advanced 模式所需的其他文件

文件名，相对于根目录的位置	注释
/cli.cli	将在 DataPower Domain 配置的末尾运行的单个 CLI 文件

3. 将 DomainZipFile.zip 放置在您的 SCP 服务器位置上。 由于该文件的敏感性，建议在配置后删除该文件。模式配置脚本将从您 SCP 环境删除从 DomainZipFile.zip 获取的任何文件以及使用 SCP 创建的 DomainZipFile.zip 的副本。
4. 请注意以下 SCP 服务器信息:
   - SCP 主机名
   - DomainZipFile.zip 的 SCP 路径
   - SCP 用户和密码

使用 DomainZipFile 文件

针对模式中不同级别安全性的 DomainZipFile 文件的用例。

可以在 Basic Runtime、Basic Runtime Sample 和 Advanced Runtime 模式中使用 DomainZipFile.zip 文件。

无需使用 SSL 将模式脚本程序包连接到 DataPower 设备。如果不使用 SSL，那么无需创建 DomainZipFile.zip 文件，除非您需要 cli 脚本来定制由模式创建的 DataPower 域。在本案例中，如果不使用服务器认证作为最低限制，那么将不会对数据进行加

密。由于在通过 http 连接对客户机进行脚本编制期间会将用户和密码信息传递至 DataPower，并且通过 DomainZipFile.zip 文件中的证书对其进行保护，因此这是一个安全风险。

如果 DataPower 主机未配置为验证客户机证书，那么无需在脚本客户机和 DataPower 设备之间使用相互认证。建议您至少使用服务器认证。

本主题中的案例场景描述不同级别的安全性。

该产品支持以下案例场景:

案例 1: 无需任何 SSL

案例 2: 无需任何 SSL，但需要 cli 脚本来定制域

案例 3: 需要通过脚本客户机对 DataPower 证书进行服务器认证

案例 4: 需要对 DataPower 设备进行相互认证

案例 1: 无需任何 SSL

出于概述的安全性原因，建议仅将该选项用于开发场景。如果不希望使用任何 SSL:

1. 请将 SCP_host 的参数设置为“Unset”。如果正在使用 Basic Runtime 或 Advanced Runtime 模式，那么 SCP_host 位于 SOA Policy Gateway 2.0.0.0 - Security 程序包脚本中。如果正在使用 Basic Runtime Sample 模式，那么 SCP_host 位于 SOA Policy Gateway 2.0.0.0 脚本中。这会在模式中设置脚本，因此不会使用 SCP 检索 DomainZipFile.zip 文件。
2. 在来自步骤 1 的相同脚本程序包中，将以下参数设置为“Unset”:
   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PUBLIC_KEY_password
   - 确认密码
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - 确认密码

案例 2: 无需任何 SSL，但需要 cli 脚本来定制域

出于概述的安全性原因，建议仅将该选项用于开发场景。如果不想使用 SSL 但需要 cli 脚本:

1. 请将 SCP_host 的参数设置为“Unset”。如果正在使用 Basic Runtime 或 Advanced Runtime 模式，那么 SCP_host 位于 SOA Policy Gateway 2.0.0.0 - Security 程序包脚本中。如果正在使用 Basic Runtime Sample 模式，那么 SCP_host 位于 SOA Policy Gateway 2.0.0.0 脚本中。这会在模式中设置脚本，因此不会使用 SCP 检索 DomainZipFile.zip 文件。
2. 在来自步骤 1 的相同脚本程序包中，将以下参数设置为 Unset:
   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PUBLIC_KEY_password
   - 确认密码
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password

- 确认密码

注: 如果 SCP_host 为“Unset”，那么无需 DomainZipFile.zip 文件，除非您具有希望在 Basic Runtime 和 Advanced Runtime 模式中运行的 cli 脚本。

3. 将要使用的 cli 脚本文件放置在 DomainZipFile.zip 文件的根目录中。DomainZipFile.zip 文件的示例结构如下所示:

   ```
   /cli.cli
   ```

   将在 DataPower Domain 脚本程序包的末尾运行该文件。cli.cli 是一个示例文件名。文件名不能包含任何空格。

案例 3: 需要通过脚本客户机对 DataPower 证书进行服务器认证

您必须提供保护 XML 管理接口的 DataPower 证书链的所有证书。要找到这些证书，请完成以下步骤:

1. 检查 XML 管理接口的 SSL 代理概要文件，并找到加密概要文件。加密概要文件将包含身份凭证，而这些身份凭证包含用于保护 XML 管理接口的证书。
2. 将这些证书添加到 DomainZipFile.zip 文件。

   格式如下:

   - dataPowerHostName/certificateChainMember1.crt
   - dataPowerHostName/certificateChainMember2.pem
   - dataPowerHostName/certificateChainMember(n).crt

   如果正在使用多域场景，那么文件可具有两个不同的 dataPowerHostName 目录，具有针对每个 DataPower 证书链的以下文件:

   - clientCertificate.crt clientKeyFile.key
   - dataPowerHostName/certificateChainMember1.crt
   - dataPowerHostName/certificateChainMember2.pem
   - dataPowerHostName/certificateChainMember(n).crt
   - dataPowerHostName2/certificateChainMember1a.crt
   - dataPowerHostName2/certificateChainMember2a.pem
   - dataPowerHostName2/certificateChainMember2(n).crt

   注: DataPower 证书链文件必须具有类型 .crt 或 .pem，并且必须仅包含证书本身。此处使用的 .crt 或 .pem 文件名为示例。文件名不能包含任何空格。

3. 可选: 如果仅针对 Basic Runtime 和 Advanced Runtime 模式所使用的 SOA Policy Gateway 2.0.0.0 - Security 程序包脚本或 Basic Runtime Sample 模式中的 SOA Policy Gateway 2.0.0.0 - Sample 脚本需要服务器认证，请对这些脚本中的以下参数使用“Unset”作为值:

   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PUBLIC_KEY_password
   - 确认密码
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password

- 确认密码

4. 可选: 如果需要 cli 脚本:

   将要使用的 cli 脚本文件放置在 DomainZipFile.zip 文件的根目录中。DomainZipFile.zip 文件的示例结构如下所示:

   ```
   /cli.cli
   ```

   将在 DataPower Domain 脚本程序包的末尾运行该文件。cli.cli 是一个示例文件名。文件名不能包含任何空格。

案例 4: 需要对 DataPower 设备进行相互认证

在本案例中，客户机和 DataPower 服务器需要验证另一方的证书。只有当在 XML 管理接口的 SSL 代理概要文件中配置了 DataPower 主机来验证客户机的证书时，才需要此项。

1. 将这些证书添加到 DomainZipFile.zip 文件。

   格式如下:

   - clientCertificate.crt
   - clientKeyFile.key
   - dataPowerHostName/certificateChainMember1.crt
   - dataPowerHostName/certificateChainMember2.pem
   - dataPowerHostName/certificateChainMember(n).crt
   - dataPowerHostName2/certificateChainMember1a.crt
   - dataPowerHostName2/certificateChainMember2a.pem
   - dataPowerHostName2/certificateChainMember2(n).crt

   注: DataPower 证书链文件必须具有类型 .crt 或 .pem，并且必须仅包含证书本身。此处使用的 .crt 或 .pem 文件名为示例。文件名不能包含任何空格。

   客户机证书和客户机密钥文件可以包含该证书或密钥文件中显示以下内容的行之前的数据: -----BEGIN CERTIFICATE-----。

2. 可选: 如果针对 Basic Runtime 和 Advanced Runtime 模式所使用的 SOA Policy Gateway 2.0.0.0 - Security 程序包脚本或 Basic Runtime Sample 模式中的 SOA Policy Gateway 2.0.0.0 - Sample 脚本需要服务器认证，请对这些脚本中的以下参数使用“Unset”作为值:

   - CLIENT_PUBLIC_KEY_file
   - CLIENT_PRIVATE_KEY_file
   - CLIENT_PRIVATE_KEY_password
   - 确认密码

3. 如果公用密钥文件没有任何密码，那么以下项的值可以为“Unset”:

   - CLIENT_PUBLIC_KEY_password
   - 确认密码

4. 脚本程序包所使用的 curl 命令假设文件类型为 .pem，因此缺省情况下，会将 **--key-type** 和 **--cert-type** 设置为 PEM。证书和密钥文件可以包含特定证书或密钥文件中 -----BEGIN CERTIFICATE----- 之前的内容。
5. 可选：如果需要 cli 脚本，使用 Basic Runtime 或 Advanced Runtime 模式：

   将要使用的 cli 脚本文件放置在 DomainZipFile.zip 文件的根目录中。DomainZipFile.zip 文件的示例结构如下所示：

   ```
   /cli.cli
   ```

   将在 DataPower Domain 脚本程序包的末尾运行该文件。cli.cli 是一个示例文件名。文件名不能包含任何空格。

通过选择案例，您已配置适当级别的安全性（使用或不使用 DomainZipFile.zip 文件）。

要上载至 WSRR 的 DataPower 证书

您可以提供 DomainZipFile.zip 文件的 dataPowerHostName 目录中证书的目录。可以将此上载至 WSRR 部署管理器服务器或 WSRR 独立服务器。

提供您自己的机制以下载 DomainZipFile.zip 文件

您可以提供自己的 DomainZipFile.zip，而不使用“安全脚本软件包”中的 SCP 服务器。

过程

要使用其他方法将文件放入环境，您必须执行以下操作：

1. **SCP_host** 参数必须设置为 Unset。
2. 您必须创建定制的脚本软件包，以在 /tmp 目录中创建 DomainZipFile.zip，然后才能运行任何 SOA Gateway 模式脚本。
3. 对于高级模式，在 /tmp/security/RetrieveDomainFiles 目录中创建 DomainZipFile.zip 文件。
4. 对于含样本的基本模式，在 /installSample/Retrieve_Domain_Files 目录中创建 DomainZipFile.zip 文件。

   注：如果未提供 DomainZipFile.zip 文件，那么在参数指示将使用证书或密钥时，脚本可能失败。

证书中的 CN 值

作为 DomainZipFile.zip 文件一部分提供的证书必须考虑证书中的 CN 值。

当您选择使用 SSL 时主机名验证始终处于活动状态，因此在脚本程序包中使用证书时需要注意以下方面：

- 对于客户机证书（公用和专用/密钥），您无法获知运行脚本的 WSRR 服务器或 WSRR 部署管理器将位于的确切主机。因此，CN 值必须足够通用才能在 IBM Workload Deployer 环境中的任何可能的客户机主机上运行；例如，*clientname*.yourcompany.com。
- DataPower 机器的证书位于 DomainZipFile.zip 文件中的个别目录中；例如：

```
dpHost1/cert1.crt
dpHost2/certb.crt
dpHost2/certbc.pem
```

- 证书（DataPower 主机链中的最终证书）的 CN 值必须对该主机名有效；例如，`dp1.yourcompany.com` 或 `*dp*.yourcompany.com`。

为样本配置 LDAP

样本需要具有一些特定条目的轻量级目录访问协议 (LDAP)。

关于此任务

必须在配置 LDAP 时定义元素和属性。

注: 请勿更改这些密码。

作为手工配置步骤的备用步骤，请解压缩 `.zip` 文件 soaSamples.zip 的内容，该 zip 文件包含两个具有该任务中所提供配置详细信息的 LDIF 文件，然后使用这些文件更新 LDAP 服务器。

过程

利用以下元素创建 LDAP:

1. 定义后缀:

   ```
   dc=ibm.com
   ```

2. 利用以下属性定义域 `dc=ibm.com`:

   ```
   dn: dc=ibm.com
   dc: ibm.com
   objectclass: domain
   objectclass: top
   ```

3. 定义容器:

   a. 定义容器组:

      ```
      dn: cn=groups,dc=ibm.com
      objectclass: container
      objectclass: top
      cn: groups
      ```

   b. 定义容器用户:

      ```
      dn: cn=users,dc=ibm.com
      objectclass: container
      objectclass: top
      cn: users
      ```

4. 定义以下用户:

   a. 具有以下属性的用户 ConsumerA:

      ```
      dn: uid=ConsumerA,cn=users,dc=ibm.com
      uid: ConsumerA
      objectclass: inetOrgPerson
      objectclass: organizationalPerson
      objectclass: person
      objectclass: top
      sn: ConsumerA
      cn: ConsumerA
      userpassword: passw0rd
      ```

   b. 具有以下属性的用户 ConsumerB:

```
dn: uid=ConsumerB,cn=users,dc=ibm.com
uid: ConsumerB
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
sn: ConsumerB
cn: ConsumerB
userpassword: passw0rd
```

c. 具有以下属性的用户 ConsumerX:

```
dn: uid=ConsumerX,cn=users,dc=ibm.com
uid: ConsumerX
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
sn: ConsumerX
cn: ConsumerX
userpassword: passw0rd
```

5. 定义以下组:

a. 利用以下属性定义组 MANAGER:

```
dn: cn=MANAGER,cn=groups,dc=ibm.com
objectclass: groupOfNames
objectclass: top
cn: MANAGER
member: uid=ConsumerX,cn=users,dc=ibm.com
```

b. 利用以下属性定义组 Clerk:

```
dn: cn=Clerk,cn=groups,dc=ibm.com
objectclass: groupOfNames
objectclass: top
cn: Clerk
member: uid=ConsumerA,cn=users,dc=ibm.com
```

c. 利用以下属性定义组 Customer:

```
dn: cn=Customer,cn=groups,dc=ibm.com
objectclass: groupOfNames
objectclass: top
cn: Customer
member: uid=ConsumerB,cn=users,dc=ibm.com
```

6. 确保在运行样本前收集有关 LDAP 的以下信息:

- 专有名称 (DN); 例如, `cn=root`。
- 密码; 例如, `passw0rd`。
- 非安全端口; 例如, 389。
- LDAP 主机名; 例如, `ldap.customer.com`。

部署模式

在云中使用 IBM Workload Deployer 3.1.0.2 或 IBM SOA Policy Gateway Pattern 部署模式将提供一个运行的 IBM PureApplication System环境。您可以使用 IBM SOA Policy Gateway Pattern 映像部署预定义的模式，或者部署创建的模式。

开始之前

要部署模式，必须首先具有预定义的模式或者完整的新模式，并且配置了所有必需的部件。

关于此任务

部署模式会创建一个虚拟系统，或者新供应的 IBM SOA Policy Gateway Pattern 运行时环境（在云中运行）。

过程

要部署 IBM SOA Policy Gateway Pattern 以在私有云中运行，请完成以下步骤:

1. 从“虚拟系统模式”窗口的模式列表中，选择要部署的模式。
2. 单击**部署**图标。
3. 完成必填字段以部署模式。在窗口中，输入虚拟系统的名称，并输入任何其他必需的信息。每个项目旁边的选中表明该项不需要进一步配置。在部署模式之前，您可以通过单击部件名称打开部件的编辑器，更改配置的部件的参数。这样会按照需要的顺序创建并启动虚拟机。

结果

部署过程会创建并启动定义的部件的虚拟机，并提供指向所需控制台的链接。部署时间取决于要部署的模式的复杂性。部署的模式是虚拟系统或新供应的 IBM SOA Policy Gateway Pattern 运行时环境。

下一步做什么

您可以从“虚拟系统实例”窗口查看实例的状态，以了解部署何时完成以及何时开始管理。

相关信息:

IBM Workload Deployer: 管理虚拟系统模式

IBM PureApplication System: 管理虚拟系统模式

部署 SOA Policy Gateway Basic Runtime Sample 模式

部署 SOA Policy Gateway Basic Runtime Sample 模式将创建模式的运行虚拟系统实例。

开始之前

必须在部署模式之前完成这些先决条件:

- 为样本配置 DataPower; 请参阅第 48 页的『为 IBM SOA Policy Gateway Pattern 配置 DataPower』。
- 为样本配置安全性; 请参阅 第 49 页的『IBM SOA Policy Gateway Pattern 模式的安全性』。
- 设置 SCP 服务器以托管安全性文件。
- 为样本配置 LDAP; 请参阅第 55 页的『为样本配置 LDAP』。

关于此任务

部署模式将创建在云中运行的虚拟系统实例。

过程

要部署 SOA Policy Gateway Basic Runtime Sample 模式，请完成以下步骤:

1. 单击**模式 > 虚拟系统**。
2. 从“虚拟系统模式”列表中，选择 **SOA Policy Gateway 2.0.0.0 - Basic Runtime 示例**。
3. 单击“部署”图标。
4. 完成必填字段以部署模式。 每个项目旁边的选中表明该项不需要进一步配置。
   a. 在**虚拟系统名称**框中，输入实例的唯一名称。
   b. 配置虚拟模式。单击**配置虚拟部件**，然后单击部件名称以打开部件和脚本的编辑器:

      注: 此模式的所有密码（DataPower_admin_id 参数除外）都缺省为 `password`。

      - 第 23 页的『SOA Policy Gateway Basic Runtime Sample 模式的 DB2 Enterprise 部件配置参数』.
      - 第 35 页的『SOA Policy Gateway Basic Runtime Sample 模式的 WSRR 独立服务器部件配置参数』
      - 第 42 页的『SOA Policy Gateway Basic Runtime Sample 模式的 SOA Policy Gateway 2.0.0.0 - Sample 脚本配置参数』
5. 单击**确定**以部署模式。

下一步做什么

要验证部署，请参阅第 62 页的『验证部署』。

部署 SOA Policy Gateway Governance Master 模式

部署 SOA Policy Gateway Governance Master 模式将创建模式的运行虚拟系统实例。

关于此任务

部署模式将创建在云中运行的虚拟系统实例。

过程

要部署 SOA Policy Gateway Governance Master 模式，请完成以下步骤:

1. 单击**模式 > 虚拟系统**。
2. 从“虚拟系统模式”列表，选择 **SOA Policy Gateway 2.0.0.0 - Governance Master**。
3. 单击“部署”图标。
4. 完成必填字段以部署模式。 每个项目旁边的选中表明该项不需要进一步配置。
   a. 在**虚拟系统名称**框中，输入实例的唯一名称。
   b. 配置虚拟模式。单击**配置虚拟部件**，然后单击部件名称以打开部件的编辑器。
      - 第 31 页的『SOA Policy Gateway Governance Master 模式的 DB2 Enterprise HADR Primary 部件配置参数』
      - 第 36 页的『SOA Policy Gateway Governance Master 模式的 WSRR 部署管理器部件配置参数』

- 第 38 页的『SOA Policy Gateway Governance Master 模式的 WSRR 定制节点部件配置参数』
- 第 33 页的『SOA Policy Gateway Governance Master 模式的 DB2 Enterprise HADR Standby 部件配置参数』

5. 单击**确定**以部署模式。

下一步做什么

要验证部署，请参阅第 62 页的『验证部署』。

SOA Policy Gateway Governance Master 部署信息

必须在部署 SOA Policy Gateway Basic Runtime 或 SOA Policy Gateway Advanced Runtime 模式之前部署 Governance Master。

关于此任务

需要使用 Governance Master 实例中的部署信息，作为针对运行时模式的部署值的输入。

过程

要从 Governance Master 实例中查找必需值，请执行以下操作:

1. 浏览至**实例 > 虚拟系统**。
2. 选择部署 Governance Master 实例。
3. 展开**虚拟机**。
4. 展开名为 ***WSRRDMGR*** 的虚拟机。
5. 请注意以下事项:
   - 在**硬件和网络**部分中，记下主机名和 IP 地址。主机名为**网络接口 0** 值。
   - 在 **WebSphere 配置**部分中，记下单元名称。

   注: 需要使用部署 Governance Master 实例期间使用的主机名或 IP、单元名称及 WebSphere 管理用户名和密码，作为针对 SOA Policy Gateway Basic Runtime 或 SOA Policy Gateway Advanced Runtime 模式中以下参数的输入:
   - WSRR_GOV_DMGR_hostname
   - WSRR_GOV_DMGR_cellname
   - WSRR_GOV_admin_user
   - WSRR_GOV_admin_password

部署 SOA Policy Gateway Basic Runtime 模式

部署 SOA Policy Gateway Basic Runtime 模式将创建模式的运行虚拟系统实例。

开始之前

请在部署 Basic Runtime 模式之前完成以下操作:

- 为 IBM SOA Policy Gateway Pattern 配置 DataPower; 请参阅第 48 页的『为 IBM SOA Policy Gateway Pattern 配置 DataPower』。
- 为 IBM SOA Policy Gateway Pattern 配置安全性; 请参阅 第 49 页的『IBM SOA Policy Gateway Pattern 模式的安全性』。

- 设置 SCP 服务器以托管安全性文件。
- 获取 Governance Master 部署信息; 请参阅 第 59 页的『SOA Policy Gateway Governance Master 部署信息』。

关于此任务

部署模式将创建在云中运行的虚拟系统实例。

注: 如果正在使用“监管支持概要文件”(GEP), 那么不能在 SOA Policy Gateway Basic Runtime 模式和 SOA Policy Gateway Advanced Runtime 模式中同时部署登台和生产环境。这是因为它会导致提升属性配置过程中出现冲突。请先部署登台环境, 然后再部署生产环境。

过程

要部署 SOA Policy Gateway Basic Runtime 模式, 请完成以下步骤:

1. 单击**模式 > 虚拟系统**。
2. 从“虚拟系统模式”列表, 选择 **SOA Policy Gateway Basic Runtime 2.0.0.0**。
3. 单击“部署”图标。
4. 完成必填字段以部署模式。 每个项目旁边的选中表明该项不需要进一步配置。
   a. 在**虚拟系统名称**框中, 输入实例的唯一名称。
   b. 配置虚拟模式。单击**配置虚拟部件**, 然后单击部件名称以打开部件和脚本的编辑器:
      - 第 22 页的『SOA Policy Gateway Basic Runtime 模式的 DB2 Enterprise 部件配置参数』
      - 第 34 页的『SOA Policy Gateway Basic Runtime 模式的 WSRR 独立服务器部件配置参数』
      - 第 45 页的『SOA Policy Gateway Basic Runtime 模式的 SOA Policy Gateway 2.0.0.0 - Security 脚本配置参数』
      - 第 40 页的『SOA Policy Gateway Basic Runtime 模式的 SOA Policy Gateway 2.0.0.0 - Promotion 脚本配置参数』
      - 第 39 页的『SOA Policy Gateway Basic Runtime 模式的 SOA Policy Gateway 2.0.0.0 - DataPower Domain 脚本配置参数』
5. 单击**确定**以部署模式。

下一步做什么

要验证部署, 请参阅第 62 页的『验证部署』。

部署 SOA Policy Gateway Advanced Runtime 模式

部署 SOA Policy Gateway Advanced Runtime 模式将创建模式的运行虚拟系统实例。

开始之前

请在部署 Advanced Runtime 模式之前完成以下操作:

- 为 IBM SOA Policy Gateway Pattern 配置 DataPower; 请参阅第 48 页的『为 IBM SOA Policy Gateway Pattern 配置 DataPower』。

- 为 IBM SOA Policy Gateway Pattern 配置安全性；请参阅 第 49 页的『IBM SOA Policy Gateway Pattern 模式的安全性』。
- 设置 SCP 服务器以托管安全性文件。
- 获取 Governance Master 部署信息；请参阅 第 59 页的『SOA Policy Gateway Governance Master 部署信息』。

关于此任务

部署模式将创建在云中运行的虚拟系统实例。

注：如果正在使用“监管支持概要文件”(GEP)，那么不能在 SOA Policy Gateway Basic Runtime 模式和 SOA Policy Gateway Advanced Runtime 模式中同时部署登台和生产环境。这是因为它会导致提升属性配置过程中出现冲突。请先部署登台环境，然后再部署生产环境。

过程

要部署 SOA Policy Gateway Advanced Runtime 模式，请完成以下步骤：

1. 单击**模式 > 虚拟系统**。
2. 从“虚拟系统模式”列表中，选择 **SOA Policy Gateway 2.0.0.0 - Advanced Runtime**。
3. 单击“部署”图标。
4. 完成必填字段以部署模式。 每个项目旁边的选中表明该项不需要进一步配置。
   a. 在**虚拟系统名称**框中，输入实例的唯一名称。
   b. 可选： 选择环境，安排部署。
   c. 配置虚拟模式。单击**配置虚拟部件**，然后单击部件名称以打开部件和脚本的编辑器：
      - 第 25 页的『SOA Policy Gateway Advanced Runtime 模式的 DB2 Enterprise HADR Primary 部件配置参数』
      - 第 36 页的『SOA Policy Gateway Advanced Runtime 模式的 WSRR 部署管理器部件配置参数』
      - 第 45 页的『SOA Policy Gateway Advanced Runtime 模式的 SOA Policy Gateway 2.0.0.0 - Security 脚本配置参数』
      - 第 41 页的『SOA Policy Gateway Advanced Runtime 模式的 SOA Policy Gateway 2.0.0.0 - Promotion 脚本配置参数』
      - 第 39 页的『SOA Policy Gateway Advanced Runtime 模式的 SOA Policy Gateway 2.0.0.0 - DataPower Domain 脚本配置参数』
      - 第 37 页的『SOA Policy Gateway Advanced Runtime 模式的 WSRR 定制节点部件配置参数』
      - 第 32 页的『SOA Policy Gateway Advanced Runtime 模式的 DB2 Enterprise HADR Standby 部件配置参数』
5. 单击**确定**以进行部署。

下一步做什么

要验证部署，请参阅第 62 页的『验证部署』。

验证部署

在部署模式后，验证部署是否成功。

过程

1. 检查虚拟系统部署历史记录中的部署日志以查找任何错误。有关更多信息，请参阅第 101 页的『对部署问题进行故障诊断』。
2. 可选: 如果部署了 SOA Policy Gateway Basic Runtime Sample，那么按照教程，使用提供的样本应用程序发送某些样本消息，以便测试部署的实例。 请参阅第 66 页的『运行样本测试用例』。

场景: 将额外的运行时添加到模式

“监管支持概要文件”随附包含以下四个不同环境的预定义环境分类系统: 开发、测试、登台和生产。

关于此任务

登台和生产环境也已编入 SOA 生命周期中，该生命周期定义了能力版本（如服务版本）的生命周期。这意味着存在特定于登台和生产环境的状态和转换，从而允许通过在提升配置文件中定义目标系统来以受控方式提升到这些运行时中。如果贵组织以相同方式定义环境（将登台作为生产前环境，以允许先进行测试，再允许打开能力版本以进行普遍使用），那么这是比较适合的。但是，许多组织需要额外环境，因此需要在概要文件中进行修改以容纳这些差异。本部分描述了可将新运行时环境添加到 WSRR“监管支持概要文件”中的一种方式。

有关规划部署环境的更多信息，请参阅第 47 页的『规划模式配置和模式先决条件』。

过程

1. 部署预定义的 SOA Policy Gateway Governance Master。有关更多信息，请参阅第 58 页的『部署 SOA Policy Gateway Governance Master 模式』。
2. 可选: 修改 WSRR“监管支持概要文件”。有关更多信息，请参阅IBM WebSphere Service Registry and Repository V8.0 信息中心 - 教程: 定制运行时环境。
3. 使用 Governance Master 详细信息配置 SOA Policy Gateway Basic Runtime 或 SOA Policy Gateway Advanced Runtime 模式。有关更多信息，请参阅第 59 页的『SOA Policy Gateway Governance Master 部署信息』。

   注: 必须将提升环境值设置为“Unset”。
4. 部署预定义的 SOA Policy Gateway Basic Runtime 或 SOA Policy Gateway Advanced Runtime。有关更多信息，请参阅第 59 页的『部署 SOA Policy Gateway Basic Runtime 模式』和第 60 页的『部署 SOA Policy Gateway Advanced Runtime 模式』。

克隆和定制 IBM SOA Policy Gateway Pattern

不能编辑 IBM SOA Policy Gateway Pattern。如果 IBM SOA Policy Gateway Pattern 虚拟系统模式提供的拓扑未提供您需要的功能，那么可以克隆模式，然后编辑以创建新模式。

关于此任务

您可以通过以下方式定制模式:

- 添加其他 DataPower 域。有关更多信息，请参阅『使用多个 DataPower 域进行部署』。
- 增加缺省集群大小。有关更多信息，请参阅 IBM Workload Deployer V3.1 信息中心。

  注: 在扩展集群大小时，请同时增加 WSRR 部署管理器的内存大小。
- 允许您选择获取服务器上压缩的安全性文件的方式。有关更多信息，请参阅第 49 页的『安全管理』。
- 允许您定义和锁定自己的缺省值；例如，DataPower 管理员标识。有关锁定参数的更多信息，请参阅 IBM Workload Deployer V3.1 信息中心。
- 允许您使用自己的机制下载 `DomainZipFile.zip` 文件。有关更多信息，请参阅第 54 页的『提供您自己的机制以下载 `DomainZipFile.zip` 文件』。

过程

要克隆模式以进行编辑和创建新模式，请完成以下步骤:

1. 在模式创建的左侧面板中，选择要克隆的模式。
2. 单击“克隆”图标并提供新模式的名称。您还可以提供其他信息，如描述。
3. 选择新模式并单击“编辑”图标以更改配置。您可以添加和除去部件并对它们进行配置，增加或减少某些部件的数目，或更改某些部件的部署顺序。

下一步做什么

确保您具有针对您创建的模式类型正确配置的所有所需部件。当您完成配置后，可以部署模式。

相关信息:

IBM Workload Deployer: 管理虚拟系统模式

IBM PureApplication System: 管理虚拟系统模式

使用多个 DataPower 域进行部署

可以克隆和定制 SOA Policy Gateway Basic Runtime 和 SOA Policy Gateway Advanced Runtime 模式，以包含多个 DataPower 域。

过程

1. 克隆 SOA Policy Gateway Basic Runtime 或 SOA Policy Gateway Advanced Runtime 模式。 有关更多信息，请参阅第 62 页的『克隆和定制 IBM SOA Policy Gateway Pattern』。
2. 要编辑模式，请单击**编辑**。
3. 展开**脚本**部分。
4. 对于每个要添加的额外域，请将 **SOA Policy Gateway 2.0.0.0 DataPower Domain** 脚本程序包拖放到 Advanced Runtime 模式的 WSRR 部署管理器部件上，或拖放到 Basic Runtime 模式的 WSRR 独立部件上。
5. 单击**已完成编辑**。
6. 部署模式，为每个添加的域输入以下信息:
   - DataPower_hostname
   - DataPower_XML_mgmt_port

- DataPower_admin_id
- DataPower_admin_password
- 确认密码
- New_DataPower_domain
- securityFileCleanUp

  注: 使用多个域时，最后一个域必须将 securityFileCleanUp 值设置为 **true**，所有其他域必须将值设置为 **false**。

有关部署模式的更多信息，请参阅第 59 页的『部署 SOA Policy Gateway Basic Runtime 模式』或第 60 页的『部署 SOA Policy Gateway Advanced Runtime 模式』。

样本应用程序

样本应用程序是可配置的 DataPower Domain 和一组可用于演示模式功能的 WSRR 工件。

样本应用程序中的基本场景是针对店铺（仓库）的库存应用程序。存在具有以下三个操作的 Store Web service:

- purchase
- findInventory
- returnProduct

基本服务级别定义 (SLD) 包含两个调解策略:

- 根据 Store.wsdl 进行验证。这假设 DataPower 验证已关闭。
- 如果在 90 秒内存在 5 条以上的消息，那么拒绝。这是轻松演示的下限阈值。

此服务的消费者当前有两个服务级别协议 (SLA): Gold 和匿名。如果 HTTP 头中的客户上下文为 Gold，会将使用者立即路由至备用端点。如果他们是匿名的（即当前非 Gold），他们将转至 Store Mock 服务端点，在该端点中商品的价格不同。

该场景还将根据用户组成员资格对 findInventory 操作执行授权。第 65 页的图 5 显示了应用程序流，其中每个框表示不同的 DataPower 网关。

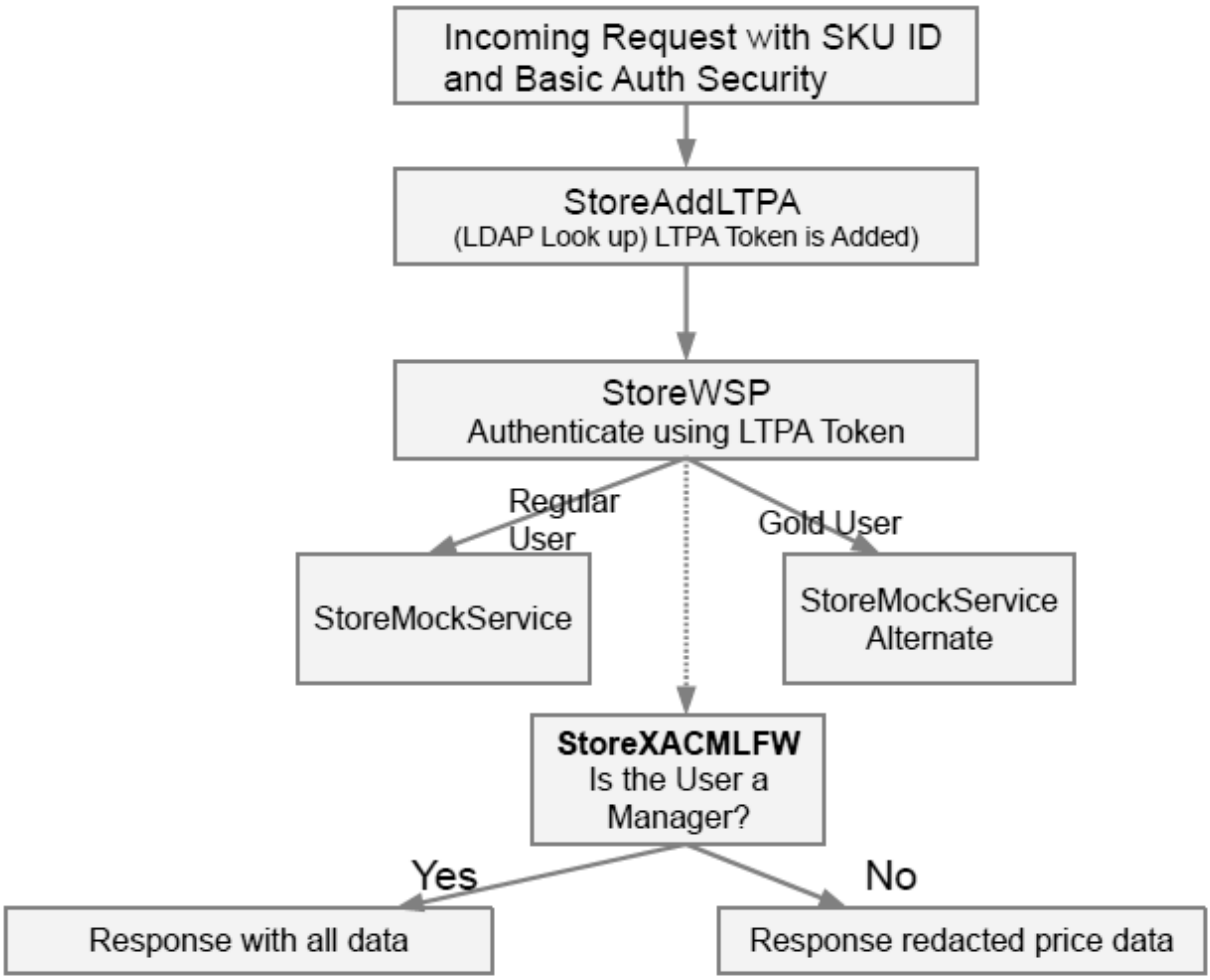


图 5. 样本应用程序流程图

相关任务:

第 62 页的『克隆和定制 IBM SOA Policy Gateway Pattern』
不能编辑 IBM SOA Policy Gateway Pattern。如果 IBM SOA Policy Gateway Pattern 虚拟系统模式提供的拓扑未提供您需要的功能，那么可以克隆模式，然后编辑以创建新模式。

样本中 WSRR 工件的概述

WSRR 工件描述了仓储操作。

存在针对仓库的基本业务能力，这是范围更大的 Bob's Warehouse 组织的一部分。服务版本 Store V1.0 表示存储服务。Store 服务级别定义 (SLD) 具有两个服务级别协议 (SLA)；一个针对 Gold 用户，用于将这些用户路由至备用首选服务；另一个是匿名用户 SLA，针对所有其他用户，仅在发出请求的 DataPower 上记录通知。Store SLD 还附加了两个其他样本策略：第一个策略在 90 秒内的 5 条消息之后拒绝消息，第二个策略根据 Store.wsdl 模式执行验证。

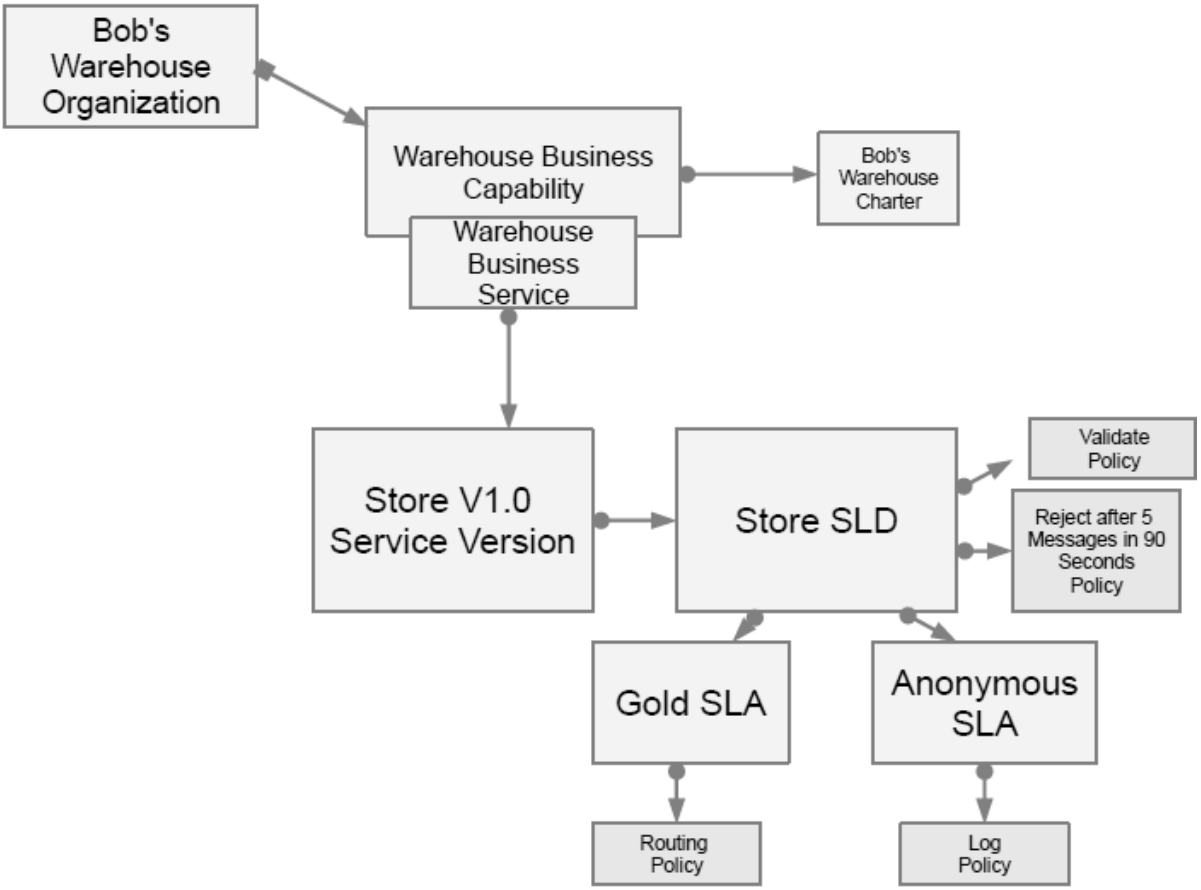


图 6. 样本域

运行样本测试用例

您可以使用样本 Web 应用程序或命令行测试已部署 SOA Policy Gateway Basic Runtime Sample 上的样本应用程序。有六个命令行测试变体可在样本应用程序上运行。

要部署 Basic Sample Runtime，请参阅第 57 页的『部署 SOA Policy Gateway Basic Runtime Sample 模式』。

注: 可在 SOA Policy Gateway Basic Runtime Sample 的日志中找到以下 XML 样本中所使用的 `SamplePolicySample_starting_port` 的值。

运行样本 Web 应用程序测试用例

要运行 Web 应用程序测试用例，请执行以下操作:

1. 通过打开已部署的“虚拟系统实例”，找到已部署 WSRR 环境的主机名。要执行此操作，请展开**虚拟机**部分，并选择 WSRR 独立服务器的虚拟机以查看虚拟机详细信息。在**硬件和网络**部分，主机名为**网络接口 0** 值。
2. 在 Web 浏览器中打开 URL: `http://<wssrHostName>:9080/SoaPolicyTester`
3. 将显示在 DataPower 中实施的样本应用程序的测试屏幕。
4. 选项为:

- **发送标准** - 将 findInventory 请求发送至存储服务。上下文标识为“Silver”用户。成功的结果为: `Part: SKU10 Price: 461.73`。
- **发送已路由** - 将 findInventory 请求发送至存储服务。上下文标识为“Gold”用户，因此请求将路由至服务的 Gold 实施。成功的结果为: `Part: GOLDSKU10 Price: 461.73`。
- **发送无效** - 发送具有无效内容的请求。验证策略需要 DataPower 来验证该请求，成功的结果将是来自 DataPower 的响应消息: `"Internal Error (from client)"`。
- **用户标识 = ConsumerA** - 对于 UserID 为 ConsumerA 的调用，将执行 XACML 策略，以便只有经理才可以查看价格。将编辑响应消息中 Price 的值。成功的结果包含 `Price: 0.0`。
- **许多标准请求** - 如果在 90 秒内执行 5 个以上请求，那么将执行拒绝策略。演示所执行策略的成功响应为: `Rejected: "Rejected (from client)"`。

5. 打开 WSRR 控制台，并浏览服务和策略。有关更多信息，请参阅。

使用命令行运行样本应用程序测试用例:

使用命令行通过“编辑”场景演示 XACML 许可/拒绝

可以将以下请求 XML 发送至 DataPower StoreAddLTPA 服务:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:stor="http://company.ibm.com/store">
  <soapenv:Header>
    <store:ConsumerIdentifier xmlns:store="http://store.com">CEO
    </store:ConsumerIdentifier>
    <store:ContextIdentifier xmlns:store="http://store.com">silver
    </store:ContextIdentifier>
  </soapenv:Header>
  <soapenv:Body>
  <stor:findInventory>
    <findInventoryReq>
      <sku>SKU10</sku>
    </findInventoryReq>
  </stor:findInventory>
  </soapenv:Body>
</soapenv:Envelope>
```

假定上面的示例请求 XML 包含在名为 `silver.xml` 的文件中，请运行以下 curl 命令:

```
curl -k --data-bin @./silver.xml -H "Content-Type: text/xml"
-u ConsumerX:passw0rd http://<yourDataPowerHostName>.com:<SamplePolicySample_starting_port+4>/Stor
```

在本示例中，ConsumerX 是一位经理，因此我们将看到完整的价格信息作为响应:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
<KD4NS:KD4SoapHeaderV2
xmlns:KD4NS="http://www.ibm.com/KD4Soap">AFIAAgAkZmExODgzNTQtY2Q1ZC0z
YjU0LWEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxN
mRhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2>
</soapenv:Header>
<soapenv:Body>
  <b:findInventoryResponse xmlns:a="http://company.ibm.com/"
     xmlns:b="http://company.ibm.com/store">
  <findInventoryRes>
<sku>SKU10</sku>
<price>461.73</price>
```

```
<inventory>460</inventory>
<msrp>923.46</msrp>
<supplierID>IBM</supplierID>
</findInventoryRes>
</b:findInventoryResponse>
</soapenv:Body></soapenv:Envelope>
```

使用命令行运行“编辑”场景

ConsumerA 不是经理，因此将看到不同的响应。运行 curl 命令:

```
curl -k --data-bin @./silver.xml -H "Content-Type: text/xml"
-u ConsumerA:passw0rd http://<yourDataPowerHostName>.com:<SamplePolicySample_starting_port+4>/Store/S
```

请注意，响应已编辑价格，为 0.0:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header><KD4NS:KD4SoapHeaderV2
xmlns:KD4NS="http://www.ibm.com/KD4Soap">AFIAAgAkZmExODgzNTQtY2Q1ZC0zYjU0L
WEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxNm
RhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2>
</soapenv:Header>
<soapenv:Body>
<b:findInventoryResponse xmlns:a="http://company.ibm.com/"
xmlns:b="http://company.ibm.com/store">
<findInventoryRes>
<sku>SKU10</sku>
<price>0.0</price>
<inventory>460</inventory>
<msrp>923.46</msrp>
<supplierID>IBM</supplierID>
</findInventoryRes>
</b:findInventoryResponse>
</soapenv:Body></soapenv:Envelope>
```

使用命令行测试路由策略

SLA ContextId 用于触发路由策略。在此情况下，针对 Gold 客户的 SLA 在 SLA 中具有值“Gold”。以下是将 Gold 作为 contextIdentifier 的样本请求的内容:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:stor="http://company.ibm.com/store">
<soapenv:Header>
  <store:ConsumerIdentifier xmlns:store="http://store.com">CEO
  </store:ConsumerIdentifier>
  <store:ContextIdentifier xmlns:store="http://store.com">Gold
  </store:ContextIdentifier>
</soapenv:Header><soapenv:Body>
<stor:findInventory><findInventoryReq>
  <sku>SKU10</sku>
  </findInventoryReq>
</stor:findInventory>
</soapenv:Body></soapenv:Envelope>
```

假定上面的示例请求 XML 包含在名为 gold.xml 的文件中，请运行以下 curl 命令:

```
curl -k --data-bin @./gold.xml -H "Content-Type: text/xml"
-u ConsumerX:passw0rd http://<yourDataPowerHostName>.com:<SamplePolicySample_starting_port+4>/Store/S
```

响应如下所示:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
  <KD4NS:KD4SoapHeaderV2
```

```
  xmlns:KD4NS="http://www.ibm.com/KD4Soap">AFIAAgAkZmExODgzNTQtY2Q1ZC0zYjU0L
  WEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxNm
  RhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2>
</soapenv:Header><soapenv:Body>
<b:findInventoryResponse xmlns:a="http://company.ibm.com/"
xmlns:b="http://company.ibm.com/store">
<findInventoryRes>
  <sku>GOLDSKU10</sku>
  <price>461.73</price>
  <inventory>460</inventory>
  <msrp>923.46</msrp>
  <supplierID>IBM</supplierID>
</findInventoryRes></b:findInventoryResponse>
</soapenv:Body>
</soapenv:Envelope>
```

请注意，返回响应将 GOLDSKU 作为 SKU 值，指示使用了 Gold 端点。

使用命令行测试模式的验证

验证策略会根据 Store.wsl 及其关联的 Company.xsd 检查请求的模式。

以下 XML badvalid.xml 显示由于主体包含名为 <skubad>（应该为 <sku>）的元素而无效的请求:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:stor="http://company.ibm.com/store">
<soapenv:Header>
<store:ConsumerIdentifier xmlns:store="http://store.com">CEO</store:ConsumerIdentifier>
<store:ContextIdentifier xmlns:store="http://store.com">silver</store:ContextIdentifier>
</soapenv:Header>
<soapenv:Body>
<stor:findInventory>
<findInventoryReq>
<skubad>SKU10</skubad>
</findInventoryReq>
</stor:findInventory>
</soapenv:Body></soapenv:Envelope>
```

如果我们运行以下 curl 请求:

```
curl -k --data-bin @./badvalid.xml -H "Content-Type: text/xml"
-u ConsumerX:passw0rd
http://<yourDataPowerHostName>.com:<SamplePolicySample_starting_port+4>/Store/Store
```

这将生成以下错误:

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
<env:Body>
<env:Fault><faultcode>env:Client</faultcode>
<faultstring>Internal Error (from client)</faultstring>
</env:Fault>
</env:Body>
</env:Envelope>
```

使用命令行在调解策略中测试拒绝

样本中包含的一个调解策略会测试消息计数在 90 秒内运行 5 次之后的拒绝。运行以下命令 6 次:

```
curl -k --data-bin @./silver.xml -H "Content-Type: text/xml" -u ConsumerX:passw0rd
http://<yourDataPowerHostName>.com:<SamplePolicySample_starting_port+4>/Store/Store
```

样本请求如下所示:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
<KD4NS:KD4SoapHeaderV2
xmlns:KD4NS="http://www.ibm.com/KD4Soap">AFIAAgAkZmExODgzNTQtY2Q1ZC0z
YjU0LWEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxN
mRhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2>
</soapenv:Header>
<soapenv:Body>
<b:findInventoryResponse xmlns:a="http://company.ibm.com/"
xmlns:b="http://company.ibm.com/store">
<findInventoryRes>
```

在本例中，ConsumerX 是一位经理，因此，针对前五次运行将显示完整价格信息，如下所示:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
<KD4NS:KD4SoapHeaderV2
xmlns:KD4NS="http://www.ibm.com/KD4Soap">AFIAAgAkZmExODgzNTQtY2Q1ZC0z
YjU0LWEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxN
mRhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2>
</soapenv:Header>
<soapenv:Body>
<b:findInventoryResponse xmlns:a="http://company.ibm.com/"
xmlns:b="http://company.ibm.com/store">
<findInventoryRes>
<sku>SKU10</sku>
<price>461.73</price>
<inventory>460</inventory>
<msrp>923.46</msrp>
<supplierID>IBM</supplierID>
</findInventoryRes></b:findInventoryResponse>
</soapenv:Body>
</soapenv:Envelope>
```

在第六次运行时，您将看到以下错误:

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope
xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
<env:Body>
<env:Fault>
<faultcode>env:Client</faultcode>
<faultstring>Rejected (from client)</faultstring>
</env:Fault>
</env:Body>
</env:Envelope>
```

注: 如果在 90 秒时间间隔内运行了其他测试，您将更早地看到该错误。

使用命令行在调解策略中测试通知

在 contextId 不为“Gold”的情况下，不会映射 SLA，并将利用匿名 SLA。匿名 SLA 的调解策略是进行记录或通知。这需要为样本域启用调试方式。运行以下命令:

```
curl -k --data-bin @./silver.xml -H "Content-Type: text/xml" -u ConsumerX:passw0rd
http://<yourDataPowerHostName>.com:<SamplePolicySample_starting_port+4>/Store/Store
```

在本例中，ConsumerX 是一位经理，因此，我们将看到完整价格信息，如下所示:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
<KD4NS:KD4SoapHeaderV2
xmlns:KD4NS="http://www.ibm.com/KD4Soap">AFIAAgAkZmExODgzNTQtY2Q1ZC0zYjU0L
WEyMzItZGM3MmEzNWY0MTAzACRmYWVjYjA1Mi1jMWUxLTMyODEtOWY3Ni0wY2IxNm
RhMDc4MjkAAw==</KD4NS:KD4SoapHeaderV2></soapenv:Header><soapenv:Body><b:fin
dInventoryResponse xmlns:a="http://company.ibm.com/"
xmlns:b="http://company.ibm.com/store">
<findInventoryRes>
<sku>SKU10</sku>
<price>461.73</price>
<inventory>460</inventory>
<msrp>923.46</msrp>
<supplierID>IBM</supplierID>
</findInventoryRes>
</b:findInventoryResponse>
</soapenv:Body>
</soapenv:Envelope>
```

以下消息是域的缺省日志中的输出:

```
Notify action triggered ('operation_38_2_sla1-1-filter_1-notify') from source policy ('LogEveryTim
```

注: 必须将日志记录设置为调试才能查看该消息。如果未这样设置，请单击 DataPower Web 控制台中的“故障诊断”图标。在“日志记录”部分中，将日志级别值更改为“调试”，然后单击**设置日志级别**。

要找到该日志，请选择**文件**和**文件管理 > 文件管理**。该日志位于 logtemp 文件夹中，名为 default-log。由于日志合并，在运行测试之前，您可能需要将日志文件放入 Web 浏览器窗口中，并在运行测试之后刷新浏览器中的选项卡。

相关任务:

第 57 页的『部署 SOA Policy Gateway Basic Runtime Sample 模式』
部署 SOA Policy Gateway Basic Runtime Sample 模式将创建模式的运行虚拟系统实例。

扩展样本应用程序

可通过修改“绑定”样式表和 XSL 样式表来修改样本应用程序。

对“绑定”样式表的修改

变量 xacml-subjects 已添加到样式表 apil-xacml-binding-new.xsl。它涉及创建请求的 subjects 部分。以后会在 sendToPDP.xsl 中访问此变量。

```
<xsl:variable name="xacml-subjects">
<xacml-context:Subject SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subje
<!--
************************************************
Starting here, use the MC result as subject.
************************************************
```

sendToPDP.xsl

该样式表使用 url-open 调用 StoreXACMLFW。该调用针对另一个 XML 防火墙，因此不使用 SSL 代理概要文件。如果期望将策略决策点 (PDP) 移至另一个 DataPower 框，可能已创建 SSL 代理概要文件并通过 url-open 调用进行使用。

```
<xsl:param name="resource" />
<!--
<xsl:variable name="incoming_resource">
<xsl:value-of select="$resource" />
</xsl:variable>
<xsl:message dp:priority="debug">
********** ABOUT TO CALL PDP for RESOURCE equal **********
<xsl:value-of select="$incoming_resource" />
</xsl:message>
-->
- <!--
building the XACML request for masking
-->
<xsl:variable name="customized-request">
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header />
<soapenv:Body>
<xacml-context:Request xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:soap="http://schemas.xm
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os" xmlns:ws="http://docs.oasis-open
wss-wssecurity-secext-1.0.xsd">
- <!--
copy in the subjects saved from AAA request processing
-->
<xsl:copy-of select="dp:variable('var://context/snip/xacml/xacmlSubjects')/*" />
<xacml-context:Resource>
<xacml-context:ResourceContent>
<xsl:copy-of select="./soap:Envelope/soap:Body" />
</xacml-context:ResourceContent>
<xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
<xacml-context:AttributeValue>PriceInfo</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Resource>
<xacml-context:Action>
<xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
<xacml-context:AttributeValue>View</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Action>
<xacml-context:Environment>
<xacml-context:Attribute AttributeId="ContextId" DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="http://security.tivoli.ibm.com/policy/distribution">
<xacml-context:AttributeValue>StorePriceData</xacml-context:AttributeValue>
</xacml-context:Attribute>
</xacml-context:Environment>
</xacml-context:Request>
</soapenv:Body>
</soapenv:Envelope>
</xsl:variable>
- <!--
Use set-variable so that it is visible in Probe, which is convenient
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlRequest'" value="$customized-request" /
- <!--
Report the XACML-REQUEST to the debug log
-->
<xsl:message dp:priority="debug">
<XACML-REQUEST>
<xsl:copy-of select="$customized-request" />
</XACML-REQUEST>
</xsl:message>
<xsl:variable name="headers">
<header name="SOAPAction">xacml:authorization</header>
</xsl:variable>
- <!--
Call the XACML PDP for decision
-->
```

```
<xsl:variable name="rtss-response">
<xsl:variable name="StoreGWURL">
<xsl:value-of select="concat('http://','127.0.0.1',':',$StoreGWPort,'/rtss/authz/services/AuthzSer
</xsl:variable>
<dp:url-open target="{$StoreGWURL}" http-headers="$headers" response="responsecode">
<xsl:copy-of select="$customized-request" />
</dp:url-open>
</xsl:variable>
- <!--
Use set-variable so that it is visible in Probe, which is convenient
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlResponse'" value="$rtss-response" />
- <!--
Report the XACML-RESPONSE to the debug log
-->
<xsl:message dp:priority="debug">
<XACML-RESPONSE>
<xsl:value-of select="$rtss-response" />
</XACML-RESPONSE>
</xsl:message>
</xsl:template>
</xsl:stylesheet>
```

如果我们检查 sendToPDP.xsl 文件，应该会注意到以下项:

1. 该样式表从 soavars.xsl 获取 XACMLFW 的端口。
2. 变量 rtssResponse 预期完全采用 Runtime Security Services 将使用的格式，转而采用 DataPower on-box PDP 可以处理的格式。
3. 该样式表构造 SOAP 请求:
   - 主题信息通过较早的 apil-binding.xsl 样式表来构造，并通过以下选择请求副本来获取:

     ```
     <xsl:copy-of select="dp:variable('var://context/snip/xacml/xacmlSubjects')/*" />
     ```
4. 该操作仅用于查看操作: `<xacml-context:AttributeValue>View</xacml-context:AttributeValue>`
5. 环境为 StorePriceData，在 IBM Tivoli® Security Policy Manager 或 Runtime Security Services 术语中称为“应用程序”对象。

让我们检查要编辑的策略样式表。

StorePrivateDataXACML.xml

```
<PolicySet PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-over
PolicySetId="RPS:StorePrivateData:policy:dc703409-d408-49b3-acc1-16c89c844fce:rolec4a9f664-a0af-45
1cafdb9fd9f0:role:2884ab77-58d1-4b1d-8728-7d528169d608" Version="1.0">
<Target>
<Subjects>
<Subject>
<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">MANAGER</xacml:AttributeValue>
<SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
DataType="http://www.w3.org/2001/XMLSchema#string" SubjectCategory="urn:oasis:names:tc:xacml:1.0:s
/>
</SubjectMatch>
</Subject>
</Subjects>
</Target>
<Policy PolicyId="PPS:StorePrivateData:dc703409-d408-49b3-acc1-16c89c844fce:c4a9f664-a0af-451b-b80
a0af-451b-b80b-1cafdb9fd9f0:pps" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-a
Version="1.0">
<Target>
```

```
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">PriceInfo</xacml:AttributeValue>
<ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" />
</ResourceMatch>
</Resource>
</Resources>
<Actions>
<Action>
<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">View</xacml:AttributeValue>
<ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string" />
</ActionMatch>
</Action>
</Actions>
</Target>
<Rule Effect="Permit" RuleId="PPS:StorePrivateData:dc703409-d408-49b3-acc1-16c89c844fce:c4a9f664-a0a
1cafdb9fd9f0:c4a9f664-a0af-451b-b80b-1cafdb9fd9f0:pps:rules:0">
<Target />
</Rule>
</Policy>
</PolicySet>
</PolicySet>
```

请注意以下事项:

- “角色”必须是 Manager:

  ```
  <xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string" xmlns:xacml="urn:oasis:na
  ```

- “资源”必须是 PriceInfo:

  ```
  <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
   xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">PriceInfo</xacml:AttributeValue>
  ```

- “操作”必须是 View:

  ```
  <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
   xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">View</xacml:AttributeValue>
  ```

修改样本 XSL 样式表

您可以在多个点修改应用程序中使用的 .xsl 脚本。

过程

要修改样本 XSL 样式表，您可以:

1. 修改 AZ 的凭证映射。

   打开 rgxacml.xsl 样式表，并完成以下 XSL 语句:

   ```
   <!-- Specify your LDAP Server -->
   <xsl:variable name="server"><xsl:copy-of select="$LDAPHost"/></xsl:variable>
   <xsl:variable name="bindDN"><xsl:copy-of select="$LDAPCN"/></xsl:variable>
   <xsl:variable name="bindPassword"><xsl:copy-of
   select="$LDAPPassword"/></xsl:variable>
   <xsl:variable name="port"><xsl:copy-of select="$LDAPPort"/></xsl:variable>
   ```

   在 soavars.xsl 样式表中定义以下变量:

```
<xsl:variable name="LDAPHost" select='"yourldap.something.com"' />
<xsl:variable name="LDAPPort" select='"389"' />
<xsl:variable name="LDAPCN" select='"cn=root"' />
<xsl:variable name="LDAPPassword" select='"passw0rd"' />
<xsl:variable name="StoreGWHost" select='"yourDatapowerName"' />
<xsl:variable name="StoreGWPort" select='"62151"' />
```

该样本包含 LDAP 服务器的未加密密码，这是您可能想要定制提供的样式表以解密加密时使用的密码。

```
<!-- Specify base DN to begin search -->
<xsl:variable name="baseDN">dc=ibm.com</xsl:variable>
```

The baseDN is hard coded as dc=ibm.com。如果为 LDAP 配置了不同的后缀、baseDN，请更改改行以定制样本。

2. 修改编辑样式表。

   noPriceInfo.xsl 样式表包含以下代码，这将使任何价格值归零。您可以向编辑逻辑添加其他字段，或者添加含计算的更复杂变换以确定字段值。

```
<!-- private access only fields -->
<xsl:template match="price">
<price>0.0</price>
</xsl:template>
<xsl:template match="Price">
<Price>0.0</Price>
</xsl:template>
```

   然后，该样式表会对所有其他元素执行标识变换。

样本的进一步研究

要了解有关样本的更多信息，可以在 DataPower 上配置 XACML 策略决策点 (PDP) 并编辑策略文档。

在 DataPower 上更改 XACML PDP

您可以浏览如何在 DataPower 中更改用于安全性策略决策点 (PDP) 的 XACML，以了解有关通过 XACML 进行访问控制的更多信息。

过程

要更改或添加 PDP:

1. 在 DataPower 控制面板中，搜索 XACML PDP。
2. 单击现有 PDP，或者单击**添加**。
3. 输入 URL；例如，local:///storePrivateDataXACML.xml。
4. 添加支持策略所需的任何从属文件或目录文件。

   注：如果直接在文件系统上编辑 XACML 策略文件，那么必须返回至 PDP 定义，并重新输入 URL 或更改的任何项，或者重新启动域以使更改生效。

编辑策略文档

使用 Business Space 用户界面编辑策略文档。

开始之前

配置 SOA 监管空间。有关更多信息，请参阅第 87 页的『为首次使用配置 Business Space』。

过程

1. 创建具有所需条件和操作的调解策略；例如，“5 分钟内消息计数 > 5 条消息”的条件以及拒绝操作。 有关创建调解策略的更多信息，请参阅第 97 页的『编写新策略』。
2. 单击**完成**。 此时将显示“浏览”视图
3. 监管调解策略。 有关监管策略文档的更多信息，请参阅第 98 页的『管理策略的生命周期』。
   a. 单击“服务注册表导航器”中的策略文档，或者在搜索窗口小部件中进行搜索。这将在“策略文档编辑器”中显示操作。
   b. 单击**建议规范**。
   c. 单击**核准规范**。

   此时将核准策略。您可以重新定义、替换或否决策略以管理生命周期或编辑现有定义。

相关任务:

第 97 页的『编写新策略』
在 Business Space 用户界面中编写调解策略时，为策略指定条件和操作。

第 98 页的『管理策略的生命周期』
可以使用 Business Space 用户界面在监管状态之间转换策略。

相关信息:

IBM WebSphere Service Registry and Repository V8.0 信息中心 - 使用 Business Space 用户界面

DataPower 样本域

该模式提供样本 DataPower 域，该域支持您开始使用该模式。作为 DataPower 开发者，您可以将现有网关用作自己应用程序的模板。样本环境包含五个网关。有一个主网关用于“存储”服务，四个支持网关为要调用的“存储网关”提供示例后端，为编辑场景提供 XACML 支持，并提供一个前端以提供额外的安全性功能。

Store Web Service 代理

Store Web Service 代理 (WSP) 是应用程序域的主网关。它通过附加的 LTPA 令牌接收请求。

在请求时，请求的处理规则完成以下操作:

1. 根据验证策略的请求，对请求进行验证。有关更多信息，请参阅第 65 页的『样本中 WSRR 工件的概述』。
2. 如果服务级别协议 (SLA) 为“Gold”，那么将请求路由至备用端点。
3. 对请求进行认证、完成授权和记帐 (AAA)。这包含以下操作:
   a. 通过 LTPA 令牌对用户进行认证。

b. 针对 LDAP 服务器映射凭证，该服务器提供有关客户属于哪些组的信息。这些组包含经理、职员和客户。

c. 将提供的输入变换为 XACML 策略决策点 (PDP) 可以理解的请求对象。

d. 通过可以在 IBM Tivoli Security Policy Manager 中创建的 XACML 策略文档，在 DataPower 框上使用 XACML PDP 完成授权。该策略的条件是用户必须是经理、客户或职员。对于 findInventory 操作，退货需要经理或职员执行，而购买可以由客户执行。

4. 使用 XSL 脚本设置 ConsumerID 值。
5. 从请求中除去整个 HTTP 安全性头。
6. 调用存储服务后端。

在处理请求时，响应处理规则将完成以下操作:

1. 调用在场景中充当 PDP 的 StoreXACMLFW 网关。
2. 基于响应，将根据用户是否具有“经理”角色来编辑（清零）价格信息字段。

样本中的 XML 防火墙

在样本中定义了以下 XML 防火墙。

StoreAddLTPA XML 防火墙

StoreAddLTPA XML 防火墙的功能是提供带有端口的前端，用户仅使用基本认证（例如，无 LTPA 或类似项）即可调用该前端。请求处理规则:

1. 通过基本认证进行识别。
2. 通过非常简单的 LDAP 查找进行认证。
3. 在后处理过程中添加 LTPA 令牌。
4. 将请求转发至现已附加 LTPA 信息的 StoreWSP 安全策略。

StoreMockService XML 防火墙

StoreMockService 是一个示例服务，它将 XML 防火墙用作实施。 findInventory、购买和退货操作全部受支持。响应值是静态的。在无法将 WebSphere Application Server 包含在模式中时，创建了此示例服务。策略的三个请求规则使用匹配操作来确定请求操作，并根据匹配项通过静态 SOAP 响应做出响应。静态 SOAP 响应是根据请求操作而非完整的服务实施来提供的。

StoreMockServiceAlternate XML 防火墙

StoreMockServiceAlternate 是一个示例服务，它将 XML 防火墙用作实施。findInventory、购买和退货操作全部受支持。此服务用于演示所执行的路由策略。

StoreXACMLFW 防火墙

本场景根据基于 XACML 的许可/拒绝机制的结果来执行编辑。在 DataPower 中，无法调用响应流中的个别 AAA 操作。创建了单独的网关以包含 XACML 策略决策点 (PDP)。此 PDP 封装在 StoreXACMLFW 的请求规则的 AAA 操作中。

StoreXACMLFW 是 DataPower 中的 XML 防火墙网关。由于这是一种提供功能的简单方式，因此使用了此实施。 StoreXML 防火墙使用相同的 WSDL 接口作为 Tivoli Runtime Security Services 服务器。StoreWSP 网关创建请求对象，并将其（使用 SSL 进行保护）发送到 StoreXMLFW 网关。

StoreXML 防火墙的请求规则执行以下操作:

1. 通过将 SSL 信息用于认证来执行 AAA。
2. 通过使用 on-box XACML PDP 来执行授权。PDP 使用的策略最初在 IBM Tivoli Security Policy Manager 中编写，但可以使用标准编辑器进行重新创建，而模式则在 XACML 规范中进行定义。
3. 不需要在此授权处理中对请求进行任何变换。
4. 如果 XACML 请求有效，那么请求处理规则会访存“许可”响应并返回到客户机。否则，将抛出异常，该异常将由异常处理规则处理，并将“拒绝”响应返回到客户机。

注: 此“许可/拒绝/不确定”仅是示例级别的响应。在特定于客户的流中可能包含其他错误信息。

XACML 安全策略

此主题描述如何创建 XACML 文档。

样本中使用的 XACML 文档是通过 IBM Tivoli Security Policy Manager 策略编辑器创建的，但您可以使用任何文本或 XML 编辑器手动创建此类文档。要构造或修改现有的 XACML 策略，请参阅 OASIS 规范: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml。

样本中使用的 XACML 安全策略包含在 `storeSWPXACML.xml` 和 `storePrivateDataXACML.xml` 中。将利用这些策略来评估传入策略决策点 (PDP) 的请求。该请求由四个关键元素组成:

1. Subjects 部分 - 包含请求调用者的专有名称的详细信息以及调用者所属的组。
2. resource 部分 - 包含调用者希望有权访问的文档。样本中使用了两种类型的资源; 第一种是对 Web Service 的操作，第二种是对响应中数据（在本例中，为 priceInfo 资源）的授权。
3. Environment 部分 - 包含有关请求的环境的信息。
4. 操作 - 用户希望通过授权的材料执行的操作。在编辑场景中，操作只是查看 priceInfo 数据。

StoreWSP 安全策略

`storeSWPXACML.xml` 文件中的安全策略会将组映射到 Web Service 操作。

示例安全策略如下所示:

```
<PolicySet PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:denyoverrid
PolicySetId="RPS:Store:policy:aed2df4e-4159-4df0-ada2-f148d9b56cef:roled200c213-27f9-
4d17-8305-b0d3ca8fcf54:role:09b60522-76b8-4280-9c1a-31d026441164" Version="1.0">
<Target>
<Subjects>
<Subject>
<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:x500Name-equal">
<xacml:AttributeValue DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">CN=MANAGER, CN=groups,
DC=ibm.com</xacml:AttributeValue>
```

```
<SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:group-id"
DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"
SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" />
</SubjectMatch>
</Subject>
<Subject>
<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">MANAGER</xacml:AttributeValue>
<SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
DataType="http://www.w3.org/2001/XMLSchema#string"
SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" />
</SubjectMatch>
</Subject>
</Subjects>
</Target>
<Policy PolicyId="PPS:StoreSOAP:findInventory:aed2df4e-4159-4df0-ada2-f148d9b56cef:d200c213-27f9-
4d17-8305-b0d3ca8fcf54:d200c213-27f9-4d17-8305-b0d3ca8fcf54:pps"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable"
Version="1.0">
<Target>
<Resources>
<Resource>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">{http://company.ibm.com/store}findInve
cml:AttributeValue>
<ResourceAttributeDesignator AttributeId="urn:ibm:xacml:profiles:web-services:1.0:wsdl:1.1:operati
DataType="http://www.w3.org/2001/XMLSchema#string" />
</ResourceMatch>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">{http://company.ibm.com/store}StoreSOA
ml:AttributeValue>
<ResourceAttributeDesignator AttributeId="urn:ibm:xacml:profiles:web-services:1.0:wsdl:1.1:port"
DataType="http://www.w3.org/2001/XMLSchema#string" />
</ResourceMatch>
<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os">{http://company.ibm.com/store}Store</x
ibuteValue>
<ResourceAttributeDesignator AttributeId="urn:ibm:xacml:profiles:web-services:1.0:wsdl:1.1:service
DataType="http://www.w3.org/2001/XMLSchema#string" />
</ResourceMatch>
</Resource>
</Resources>
</Target>
```

注: 在 subjects 部分中，将对 x500 名称或主题角色 Manager 进行匹配。如果检查整个策略 .xml 文件，您将看到存在针对客户和职员的类似映射。您将看到已授权 findInventory 操作使用所有三个组，而 returnProduce 和 purchase 操作仅限于特定组。

编辑网关

有关 storeCallPDP.xsl 样式表的详细信息。

如果检查 storeCallPDP.xsl 样式表，那么您将注意到以下事项:

1. storeSendToPDP.xsl 样式表包含的内容。这是具有用于调用 storeXAMLFW 的逻辑的样式表。
2. 对 storeSendToPDP 内的模板 call_PDP 的调用。
3. 从调用的响应中抽取决策，例如“许可”。
4. 将 var:/context/response/displayfilter 值设置为 allData.xsl 或 noPriceInfo.xsl 样式表。

5. 仔细检查用于编辑的 XACML storePrivateDataXACML.xml，结构几乎与 StoreWSP 场景中所使用的结构相同。差异在于只有“经理”角色具有访问权。

storeCallPDP.xsl

```
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:dp="http://www.c
extension-element-prefixes="dp" exclude-result-prefixes="dp">
  <xsl:include href="storeSendToPDP.xsl" />
    <xsl:template match="/">
      <xsl:call-template name="call_PDP">
        <xsl:with-param name="resource" select="'StorePrivateData'" />
      </xsl:call-template>
      <xsl:variable name="decision">
        <xsl:copy-of select="dp:variable('var://context/snip/xacml/BacksideXacmlResponse')/*[local-na
        response']/*[local-name()='Envelope']/*[local-name()='Body']/*[local-name()='Response']/*[loc
        Decision']" />
      </xsl:variable>
      <xsl:message dp:priority="debug">
        <DECISION-FROM-RTSS>
          <xsl:value-of select="$decision" />
        </DECISION-FROM-RTSS>
      </xsl:message>
      <xsl:choose>
      <xsl:when test="$decision = 'Permit'">
        <xsl:message dp:priority="debug">****** SETTING THE PRIVATE FILTER ********</xsl:message>
        <dp:set-variable name="'var://context/response/displayFilter'" value="'local:///allData.xsl'
      </xsl:when>
      <xsl:otherwise>
        I<dp:set-variable name="'var://context/response/displayFilter'" value="'local:///noPriceInfo
      </xsl:otherwise>
    </xsl:choose>
  </xsl:template>
</xsl:stylesheet>
```

在 SOA Policy Gateway Basic Runtime Sample 中创建的 WSRR 工件

在 SOA Policy Gateway Basic Runtime Sample 模式中创建的 WSRR 工件及样本如何使用这些工件。

表 33. 为 SOA Policy Gateway Basic Runtime Sample 模式创建的 WSRR 工件

对象	描述
组织	Bob’s Warehouse。
业务能力	Bob’s Warehouse 组织所拥有的仓库。
服务版本	Store 1.0 使用 Store Web Service、Store 服务级别定义 (SLD) 和仓库业务能力。
WSDL	Store.wsdl
XSD	Company.xsd
策略	• Validate.xml • RouteForGold.xml • LogEveryTime.xml • RejectAfter5MsgIn90Seconds.xml

表 33. 为 SOA Policy Gateway Basic Runtime Sample 模式创建的 WSRR 工件 (续)

对象	描述
策略附件	• Anonymous Users_GenericObject_Anonymous Users_LogEveryTime.xml - 将 LogEveryTime 策略附加到匿名用户服务级别协议 (SLA)。 • Gold SLA_GenericObject_Gold SLA_RouteForGold.xml - 将 RouteForGold 策略附加到 Gold SLA。 • Store_GenericObject_Store_urn :RejectAfter5MsgIn90Seconds.xml - 将 RejectAfter5MsgIn90Seconds 策略附加到 Store SLD。 • Store_GenericObject_Store_urn:Validate.xml - 将验证策略附加到 Store SLD。
SLD	Store SLD - 供 Store 1.0 服务版本使用。
SLA	Gold SLA - 如果 ContextId 为“Gold”，那么路由至 Gold 端点。
匿名 SLA	匿名用户 - 使用 LogEveryTime 策略通知，并在 ContextId 不是“Gold”时执行。

WSRR 工件的样本应用程序使用

StoreWSP 使用 WSRR 预订来检索 WSDL 和策略工件。每当通过 StoreWSP 处理请求时，都将执行以下操作:

1. Store 1.0 服务版本将连接到 Store SLD，后者附加了两个直接策略: Validate 和 RejectAfter5MsgIn90Seconds。策略的运行顺序不确定。
   a. 如果在过去 90 秒内已发生 5 个请求，将拒绝该请求。
   b. 将根据 Store.wsdl 及其关联的 Company.xsd 对请求进行验证。
2. Store 1.0 服务使用 Store SLD，后者有两个 SLA: 用于 Gold 用户的 Gold SLA 和针对所有其他用户的匿名用户 SLA。如果 ContextId 属性为“Gold”，会将请求路由至 StoreMockServiceAlternate XML 防火墙，否则，如果该属性为“Silver”或其他任何值，匿名用户 SLA 将接管，并将运行 LogEveryTime 策略。这会将一条通知放入样本域的 `default.log` 中。仅当对该域启用调试方式时，才能看到此通知。然后，会将该消息路由至 StoreMockService XML 防火墙。

在 SOA Policy Gateway Basic Runtime Sample 中创建的 DataPower 工件

在 SOA Policy Gateway Basic Runtime Sample 中创建的 DataPower 工件

表 34. 为 SOA Policy Gateway Basic Runtime Sample 模式创建的 DataPower 工件

类型	名称	目的
WebService 代理	StoreWSP	主体服务。
XML 防火墙	StoreAddLTPA	认证和添加 LTPA 令牌。
	StoreMockService	非 Gold 客户的服务提供者
	StoreAlternateMockService	Gold 客户的服务提供者
	StoreXACMLFW	检查对 PriceInfo 的访问权。

表 34. 为 SOA Policy Gateway Basic Runtime Sample 模式创建的 DataPower 工件 (续)

类型	名称	目的
WSRR 服务器	WSRRSVR	到 WSRR 的连接。
WSRR 预订	StoreSub	为 WSRR 名称空间和对象等提供搜索信息。
AAA 策略	StoreAddLTPA	LDAP 的基本认证标识。 查找认证。 向请求添加 LTPA 令牌。
AAA 策略	StoreWSDLAAA	LTPA 标识和认证。 针对授权的组映射。 XACML 授权。
AAA 策略	StoreXACMLFWAZ	针对 PriceInfo 的 XACML 授权。
SSL 代理概要文件	WSRRPP	针对 WSRR 服务器的 SSL 代理概要文件。
加密概要文件	WSRRCP	针对 WSRR 服务器的加密概要文件。
验证凭证	WSRRVC	验证凭证包含加密证书 WSRRCERT。所有其他设置都是缺省值。
加密证书	WSRRCERT	WSRRCERT 使用签署者证书。此证书是从 NodeDefaultKeyStore（单台服务器的缺省证书）或 CMSKeyStore 缺省证书（针对 IBM HTTP Server 所存在的 ND 环境）中抽取的。

StoreWSP Web Service 代理处理规则

样本的中心网关是 StoreWSP。该网关的策略包含请求和响应规则。

请求规则

StoreWSP_default_request-rule 的主策略操作称为 AAA。在 AAA 操作中，将验证 LTPA 令牌，检索用户组，执行授权以查看用户是在经理、职员还是客户 LDAP 组中。当 AAA AZ 步骤在 DataPower 设备上调用 StoreWSDLPDP 策略决策点 (PDP) 时，将执行此操作。此 PDP 使用 storeWSPXACML.xml XACML 策略。

响应规则

在响应规则 StoreWSP_default_response-rule 中，变换将调用 StoreXACMLFW XML 防火墙服务。

此变换将根据用户是否为经理组的成员来确定是否授权用户访问价格信息。如果是该组成员，*var:///context/response/displayFilter* 变量将设置为 `local:///allData.xsl`。如果不是经理 LDAP 组的成员，*var:///context/response/displayFilter* 变量将设置为 `local:///noPriceInfo.xsl`。

然后，变换将在响应时执行样式表操作。

StoreXAMLFW 处理规则

定制样式表 storeSendToPDP.xsl 对本地 XML FW StoreXACMLFW 进行调用。在此防火墙中使用了两个处理规则。StoreXACMLFW_request 包含使用 allData.xsl 变换的单个 AAA 策略操作。此 AAA 操作 StoreXACMLFWAZ 反过来将调用 XACML PDP StorePDP 操作。通过使用 storePrivateDataXACML.xml XACML 策略，将确定是否授权用户访问价格信息。

样本 XSL 样式表

样本应用程序包含以 .xsl 结尾的以下样式表，这些样式表位于已安装域的本地目录中。

表 35. 样本应用程序中的样式表

样式表	目的
allData.xsl	身份样式表，用于将所有数据从源复制到目标。它用于编辑功能和对 XACML XML 网关的调用。
apil-xacml-binding-new.xsl	使用凭证映射信息创建可由 DataPower 设备“策略决策点”(PDP) 处理的 SOAP 请求。此样式表是对 DataPower 设备的存储目录中提供的 tspm-xacml-binding-sample.xsl 样式表的修改。此改编脚本提供的关键功能是添加外部可访问的变量，以使 XACML 请求的主题信息对编辑样式表可用。
noPriceInfo.xsl	此样式表将 price 元素设置为值 0.0。
rgxacml.xsl	此样式表是对 DataPower 设备的存储目录中 tspm-retrieve-groups.xsl 样式表的定制。此样式表的主要目的是提供 LDAP DN、主机名、密码、端口等，以便可以查找入局用户并检索其组信息。
soavars.xsl	此样式表是仅作为示例的样式表，它在 rgxacml.xsl 样式表所使用的变量中定义 LDAP 信息。在本示例中，密码未加密，这不是生产中的做法。
storeCallPDP.xsl	此样式表具有用于调用 XACML 网关的代码，处理许可/拒绝决策，并设置过滤器变量以运行 allData.xsl 或 noPriceInfo.xsl。
storeSendToPDP.xsl	此样式表构造将发送至 XACML 网关的 SOAP 请求。它包含资源信息、操作信息、环境信息以及在 apil-xacml-binding-new.xsl 样式表中获取的主题信息。

使用 XSL 样式表的 DataPower 对象

DataPower 对象使用随样本应用程序提供的一些 XSL 样式表。

表 36. 使用 XSL 样式表的 DataPower 对象

样式表	目的
allData.xsl	在 storeCallPDP.xsl 样式表中内部使用。该样式表在 AAA 策略 StoreXACMLFWAZ 中用作定制变换。
apil-xacml-binding-new.xsl	在 StoreWSDLAAA AAA 策略 AZ 步骤中用作定制样式表。
noPriceInfo.xsl	在 storeCallPDP.xsl 样式表中内部使用。
soavars.xsl	在 rgxacml.xsl 样式表中内部使用。
storeCallPDP.xsl	作为 Store_default-response 规则中的变换进行调用。
storeSendToPDP.xsl	在 storeCallPDP.xsl 样式表中内部使用。

第 6 章 使用已部署的实例

当已部署 IBM SOA Policy Gateway Pattern 映像时，您可以注册自己的服务定义并将自己的策略附加到定义。您还可以查看和管理您的部署系统。要查看部署实例的列表，请单击**实例 > 虚拟系统**。

查看实例详细信息

可以通过选择“虚拟系统实例”窗口的实例列表中的实例查看部署实例的详细信息。虚拟系统实例详细信息显示在右侧。这些详细信息包括由下列各项组成的列表：在云基础结构上为该部署供应的虚拟机、IP 地址、虚拟机状态和角色状态。角色是一个由虚拟机上的虚拟应用程序中间件执行的功能单元。还可查看虚拟机角色运行状况状态信息。例如，当虚拟机上的 CPU 很关键时，红色复选框位于绿色状态箭头之上。

要查看实例的供应和部署状态，请参阅详细信息视图中的**当前状态**值。

要查看供应期间虚拟机和脚本的状态，请展开详细信息视图中的**历史记录**部分。

要查看虚拟机和脚本日志的详细信息，请展开详细信息视图中的**虚拟机**部分。系统的主机和 IP 地址是**硬件和网络**部分中的**网络接口 0** 值。展开正在运行的虚拟机以查看**脚本软件包**部分中的脚本日志和链接以访问**控制台**部分中使用的虚拟机。

管理已部署的实例

在部署虚拟系统模式之后，可以查看和管理创建的虚拟系统实例以查看您的 IBM SOA Policy Gateway Pattern 环境。

开始之前

要查看虚拟系统实例，必须首先已部署虚拟系统模式。

关于此任务

部署模式将创建虚拟系统实例或新供应的 IBM SOA Policy Gateway Pattern 运行时环境。在部署完成时，虚拟系统实例即开始运行。

过程

要管理 IBM SOA Policy Gateway Pattern 虚拟系统实例，请完成以下步骤：

1. 单击**实例 > 虚拟系统**以访问“虚拟系统实例”窗口。
2. 从“虚拟系统实例”窗口的实例列表中，选择部署的实例。
3. 如果该实例正在运行，可以从虚拟系统视图中的控制台链接登录到虚拟系统的组件。可用的组件取决于您创建的模式。例如，您可以：
   - 启动并登录到部署管理器的管理控制台，然后查看创建的集群。
   - 启动流程中心，然后下载流程设计器以编写流程应用程序。
   - 设置 IBM Integration Designer 并连接到流程中心以进行流程编写。

连接到 WSRR - 业务空间

使用业务空间用户界面管理策略。

关于此任务

使用 WSRR 系统的主机地址访问业务空间用户界面。

过程

1. 单击**实例 > 虚拟系统**以访问“虚拟系统实例”窗口。
2. 从“虚拟系统实例”窗口的实例列表中，选择部署的实例。 这样会显示实例详细信息。
3. 使用业务空间用户界面访问 WSRR 系统:
   - 在**控制台**部分，单击 **WSRR 业务空间**，以连接至正在 WSRR 系统上运行的业务空间。
   - 或者，在外部 Web 浏览器中:
     a. 查找 WSRR 的主机名和端口号。展开**虚拟机**部分并选择 WSRR 独立服务器的虚拟机以查看虚拟机详细信息。在**硬件和网络**部分，主机名为**网络接口 0** 值。
     b. 输入业务空间 URL:
        – 对于已启用安全性的 WSRR 独立服务器: `https://<hostname>:9443/BusinessSpace`
        – 对于集群: `http://<hostname>/BusinessSpace`

        其中，*<hostname>* 和 *port* 是 WSRR 服务器的主机名和端口值。

结果

显示业务空间，可以用业务空间添加、删除或除去策略。

下一步做什么

如果第一次使用 WSRR 系统上的业务空间，请参阅 第 87 页的『为首次使用配置 Business Space』 并遵循创建操作空间的步骤。

相关信息:

IBM WebSphere Service Registry and Repository V8.0 信息中心

连接到 WSRR - 服务注册表控制台

使用“服务注册表控制台”以对服务版本分类。

关于此任务

使用 WSRR 系统的主机地址访问“服务注册表控制台”用户界面。

过程

1. 单击**实例 > 虚拟系统**以访问“虚拟系统实例”窗口。
2. 从“虚拟系统实例”窗口的实例列表中，选择部署的实例。 这样会显示实例详细信息。
3. 访问 WSRR 系统:

- 在**控制台**部分，单击 **WSRR_Web_UI** 以连接至正在 WSRR 系统上运行的业务空间。
- 或者，在外部 Web 浏览器中:
  a. 查找 WSRR 的主机名和端口号。展开**虚拟机**部分并选择 WSRR 独立服务器的虚拟机以查看虚拟机详细信息。在**硬件和网络**部分，主机名为**网络接口 0** 值。
  b. 输入服务注册表控制台 URL: http://*hostname*/ServiceRegistry

     其中，*hostname* 是 WSRR 服务器的主机名。

相关信息:

IBM WebSphere Service Registry and Repository V8.0 信息中心

为首次使用配置 Business Space

必须创建“SOA 管理”空间，才能将 Business Space 用户界面用于创建策略。

开始之前

有关访问 Business Space 的信息，请参阅第 86 页的『连接到 WSRR - 业务空间』。

关于此任务

要使用 Business Space 窗口小部件，必须创建空间。空间是为特定角色定义的。策略编写最适合在“SOA 管理”空间中使用。如果尚未创建“SOA 管理”空间，必须进行创建。要根据“SOA 管理的服务注册表”模板创建空间，请完成以下步骤:

过程

1. 单击页面顶部的**管理空间**。将显示“空间管理器”对话框。
2. 单击**创建空间**。将显示“创建空间”对话框。
3. 在“空间名称”字段中输入名称; 例如，SOA 管理。（可选）输入描述。
4. 从**使用模板创建新空间**列表中选择 **SOA 管理的服务注册表**，然后单击**保存**。
5. 新空间将显示在**空间管理器**列表中。单击新空间以打开到该空间。

结果

将创建“SOA 管理”空间。要打开“SOA 管理”空间:

1. 单击页面顶部的**转至空间**。这样会显示“转至空间”对话框。
2. 单击针对“SOA 管理”用户的空间。具体名称将取决于创建空间时指定的内容。

下一步做什么

您可以向“服务注册表操作”窗口小部件添加额外操作:

1. 在 Business Space 中，单击**编辑页面**。
2. 在“服务注册表操作”窗口小部件中，单击**编辑设置**。
3. 选择以下要显示的操作:
   - 创建服务级别定义
   - 创建服务版本

- 创建服务级别协议
- 创建业务能力

4. 在“服务注册表操作”窗口小部件中，单击**保存并关闭**。
5. 单击**完成编辑**。

部署模式后的配置

在部署模式之后，必须配置安全性和其他设置。

样本应用程序的 LDAP 设置更改

如果正在使用 SOA Policy Gateway Basic Runtime Sample 并且需要更改 LDAP 服务器的安全性设置（例如，密码或用户名），那么您需要在两个位置中更改这些值。

要进行更改的位置有:

- AAA 策略 StoreAddLTPA 的“AAA 策略认证”部分 - 要查找该策略，请使用 DataPower 管理 Web 用户界面的搜索窗口，并搜索 AAA。选择正确的 AAA 策略，并更改“认证”选项卡中的值。
- soavars.xsl 文件 - 使用 DataPower Web 管理用户界面中的“文件管理”部分。打开 DataPower 设备上通过 SOA Policy Gateway Basic Runtime Sample 模式创建的域，并浏览本地目录中的 soavars.xsl 文件。根据需要更改 LDAPHost、LDAPPort、LDAPCN 和 LDAPPassword 变量。

  注: 您可能需要重新启动该域以使这些更改生效。

DataPower 证书的证书 DN 值

将 SSL 与提供的 IBM SOA Policy Gateway Pattern 一起使用时，DN 主机验证比缺省的 WebSphere Application Server 安全性更严格。

缺省情况下，WebSphere Application Server 中未启用 DN 主机验证。但是，在 IBM SOA Policy Gateway Pattern 所使用的脚本程序包中，将开启并且不能禁用 DN 主机验证。在缺省的 WebSphere Application Server 和 DataPower 之间工作的非常具体的证书可能无法用于与 IBM SOA Policy Gateway Pattern 一起使用的“SOA Policy Gateway 2.0.0.0 - Security”脚本程序包和“SOA Policy Gateway 2.0.0.0 - Sample”脚本程序包；例如，缺省情况下，WebSphere Application Server 可以接受 DN myserver.yourcompany.com，但这些脚本程序包无法接受该 DN。要添加或除去用于部署的 DataPower 证书，请参阅第 89 页的『在 WSRR 信任库中除去或添加 DataPower 证书』。

更改 LTPA 密钥

此过程描述如何更改 LTPA 密钥。LTPA 密钥在 Basic 中的所有单元间共享。它不用于 SOA Policy Gateway Basic Runtime Sample 模式。 LTPA 密钥从 Governance Master 中导出，并导入运行时环境，例如，登台、生产或取消设置。

过程

1. 从 Governance Master WSRR Dmgr 导出新的 LTPA 密钥。
2. 将 LTPA 密钥导入运行时 WSRR 实例（Dmgr 或 Stand Alone）。

3. 如果运行时实例为 Advanced ND 环境，请按顺序完成以下操作:
   a. 同步所有节点。
   b. 停止 WSRR 集群。
   c. 停止节点代理程序。
   d. 停止 Dmgr。
4. 如果环境为 Advanced，那么必须按相反顺序重新启动:
   a. 启动 Dmgr。
   b. 启动节点代理程序。
   c. 启动 WSRR 集群。
5. 如果 WSRR 为独立服务器，那么必须停止并重新启动以使 LTPA 密钥更改生效。

在 WSRR 信任库中除去或添加 DataPower 证书

此任务描述如何添加或除去 DataPower 证书。执行此任务的优点在于，简化了 WSRR 和 DataPower 之间为策略更新而同步更新功能的未来设置。

关于此任务

DataPower 证书属于 curl 工具所使用的模式。DataPower 调用将上载到节点或单元缺省信任库。这简化了未来在 WSRR 和 DataPower 之间为策略更新而使用同步更新功能的设置。如果不需要此功能，以下过程描述如何除去 DataPower 证书。此过程还描述如何添加新的 DataPower 证书（如果需要更改证书）。

过程

1. 登录到 Dmgr 或 Stand Alone WSRR: `http://hostname:9060/admin`。输入用户和密码。
2. 浏览至**安全性**、**SSL 证书和密钥管理**。
3. 单击**密钥库和证书**。
4. 如果选择基本模式，请单击 **NodeDefaultTrustStore**，或者，如果选择高级模式，请单击 **CellDefaultTruststore**。
5. 单击**签署者证书**。
6. 选中想要除去的任何证书的复选框。
7. 单击**删除**。
8. 单击**保存**。
9. 可选: 如果需要添加新的 DataPower 证书，请单击**添加**以添加新证书。

配置策略执行点

DataPower 设备是 IBM SOA Policy Gateway Pattern 的“策略执行点”(PEP)。在部署“应用程序域”时，可以创建该域的内容。

过程

创建 Web Service 代理 (WSP):

1. 从 DataPower 控制面板，单击 **Web Service 代理**。
2. 单击**添加**并输入代理的名称。

3. 打开 **WSRR 预订**选项卡。在 WSRR Server 列表中，单击 **WSRRSVR**。
4. 提供必需的其他信息，例如，前端处理程序、名称空间、对象名等，以创建 Web Service 代理的配置。

创建 WSP 的策略:

5. 打开 WSP 编辑器的**策略**选项卡。
6. 单击相应级别的**处理规则**。您可以创建新规则或编辑提供的缺省规则。要添加的关键策略操作是 **AAA 操作**。这用于处理对于模式至关重要的“标识”、“认证”和“授权”。

   对于 AAA 操作必须指定的关键内容包括输入和输出以及 AAA 策略。您可以在创建 AAA 策略操作的流程中创建策略，也可以在使用 AAA 编辑器之前创建。

   - “标识”是标识用户的步骤。在我们的示例中，使用两种格式的标识。在 StoreAddLTPA XML 防火墙中，通过基本认证执行标识。在 StoreWSP 防火墙中，由 LTPA 令牌提供标识。
   - 认证是证明用户是系统已知的用户的步骤。有多个选项可供选择。在样本中，我们向您展示两个示例；第一个使用 LDAP 查找用户，第二个接受有效的 LTPA 令牌。
   - 授权是向用户授予资源权限的步骤，在此示例中，即 Web Service 操作。需要指定以下关键元素以使用 XACML on-box PDP 授权:
     - 方法: **使用 XACML 授权**。
     - XACML 版本；例如，2.0。
     - PDP 类型；例如，基于拒绝的 PDP。
     - 使用 On box PDP: **On**
     - 已指定 XACML 的 PDP 的名称。
     - 配置 PDP。有关更多信息，请参阅第 75 页的『在 DataPower 上更改 XACML PDP』。
     - 要绑定 AAA 和 XACML 的定制 XSL 样式表: 使用 `apil-xacml-bindingnew.xsl` 作为起点。

要配置网关，请使用“编辑”:

7. 修改 XACML `.xml` 文件，以匹配想要针对编辑实施的特定安全策略。
8. 创建包含 AAA 操作的 XML 防火墙（遵循编辑样本）。
9. 修改上述 AAA 操作使用的 PDP 以指向用于实施编辑的样式表。
10. 复制并修改针对 XACML 服务创建 SOAP 有效内容的 `storeCallPDP.xsl` 样式表。尤其是，确保“操作”和“资源”匹配创建的 XACML 策略文档的需求。
11. 确保修改的样式表针对新的 XACML XML 防火墙调用正确的端口。

下一步做什么

除了在 SOA Policy Gateway Advanced Runtime 和 SOA Policy Gateway Basic Runtime 模式中创建域和设置 WSRR 服务器配置，还可以通过运行定制 CLI 脚本来扩展域。CLI 脚本应该位于 `DomainZipFile.zip` 结构的根目录中，例如，`/cli.cli`。CLI 可以运行任何标准 CLI 命令，但 CLI 引用的所有工件必须存在或者可供模式创建的 DataPower Domain 访问。在部署 SOA Policy Gateway Advanced Runtime 或 SOA Policy Gateway Basic Runtime 模式的实例时，将提示您提供 Security 程序包参数中的 CLI 文件名。

使用 SOA Policy Gateway Basic Runtime 模式

SOA Policy Gateway Basic Runtime 模式包含三大块功能: 检索 DataPower 与 WSRR 模式脚本之间的安全性所需的文件，在 DataPower 上配置域，最后配置提升。

当已完成以下操作时:

1. 新域存在于指定的 DataPower 设备上。
2. WSRR 服务器定义存在于域中。
3. 已针对 DataPower 域运行定制 CLI 脚本。
4. 配置 WSRR 服务器。
5. 客户提供的任何 DataPower 签署者证书已上载至 WSRR 单元的 NodeDefaultTruststore。
6. 已配置 SOA Policy Gateway Basic Runtime 模式 WSRR 单元和 SOA Policy Gateway Governance Master 单元之间的提升。
7. 已交换签署者证书。监管部署管理器的签署者证书放置在基本单元的 NodeDefaultTrustStore 中，基本单元部署管理器的签署者证书放置在监管单元的 CellDefaultTrustStore 中。
8. 已交换 LTPA 密钥。监管单元的 LTPA 密钥会导入基本单元中。
9. Governance Master WSRR 集群的每个主机会添加到基本单元的受信域。基本单元 WSRR 集群的每个主机会添加到 Governance Master 的受信域。
10. 如果单元指定为给定输入中的登台或生产环境，那么配置提升属性文件。

当您需要采取其他步骤才能完成完全安全的生产环境时，此时执行的配置将允许您执行以下操作:

1. 使用缺省 GEP 创建服务和策略，以及通过 WSRR 上的 SOA 策略生命周期对其进行监管（已提供登台和生产环境时）。
2. 创建可以使用预创建的 WSRR 服务器定义的 Web Service 代理来构建预订。

使用 SOA Policy Gateway Advanced Runtime 模式

SOA Policy Gateway Advanced Runtime 模式包含三大块功能: 检索 DataPower 与 WSRR 模式脚本之间的安全性所需的文件，在 DataPower 上配置域，最后配置提升。

当已完成以下操作时:

1. 新域存在于指定的 DataPower 设备上。
2. WSRR 服务器定义存在于域中。
3. 已针对 DataPower 域运行定制 CLI 脚本。
4. 将已创建和配置具有“n”节点的 WSRR 集群环境。
5. 客户提供的任何 DataPower 签署者证书将上载到 WSRR 单元的 CellDefaultTruststore。
6. 已配置 SOA Policy Gateway Advanced Runtime 模式 WSRR 单元和 SOA Policy Gateway Governance Master 单元之间的提升:
   a. 已交换签署者证书。监管部署管理器的签署者证书放置在高级单元的 CellDefaultTrustStore 中，高级单元部署管理器的签署者证书放置在监管单元的 CellDefaultTrustStore 中。

b. 将交换 LTPA 密钥。监管单元的 LTPA 密钥会导入高级单元中。

c. Governance Master WSRR 集群的每个主机会添加到高级单元的受信域。高级单元 WSRR 集群的每个主机会添加到 Governance Master 的受信域。

d. 如果单元指定为给定输入中的登台或生产环境，那么配置提升属性文件。

当前配置使您能够执行以下操作:

1. 使用缺省“监管支持概要文件”(GEP) 创建服务和策略，以及通过 WSRR 上的 SOA 策略生命周期对其进行监管（已提供登台和生产环境时）。
2. 创建可以使用预创建的 WSRR 服务器定义的 Web Service 代理来构建预订。

接下来，您必须执行额外步骤以完成完全安全的生产环境。有关更多信息，请参阅第 49 页的『IBM SOA Policy Gateway Pattern 模式的安全性』。

在 Basic Runtime 和 Advanced Runtime 模式下创建的 DataPower 对象

在 SOA Policy Gateway Basic Runtime 和 SOA Policy Gateway Advanced Runtime 模式下创建的 DataPower 对象及其功能的概述。

表 37. DataPower 模式对象

对象	描述
域	可用于用户应用程序的域。
WSRR 服务器	名为 WSRRSVR。配置了 SOAP URL、用户和密码以及具有验证凭证的 SSL 代理概要文件。
SSL 代理概要文件	名为 WSRRPP，它是一个转发（客户机）概要文件。它使用加密概要文件 WSRRCP。使用了所有其他缺省值。
加密概要文件	WSRRCP 包含验证凭证对象 WSRRVC，后者包含作为模式脚本一部分上载的签署者证书。
验证凭证	WSRR 验证凭证包含加密证书 WSRRCERT。所有其他设置都是缺省值。
加密证书	WSRRCERT 利用签署者证书。此证书是从 NodeDefaultKeyStore（单台服务器的缺省证书）或 CMSKeyStore 缺省证书（如果是 IBM HTTP Server 存在于的 ND 环境）抽取的。

Web Service 代理中 WSRR 服务器定义的示例用法:

1. 从 DataPower 控制面板，单击 **Web Service 代理**。
2. 单击**添加**并为代理提供**名称**。
3. 接下来，选择 **WSRR 预订**选项卡
4. 选择菜单中的“WSRR 服务器”。WSRRSVR 对象可用。
5. 提供其他所需信息（如前端处理程序、名称空间、对象名等）以创建 Web Service 代理的配置。

服务创建和监管

使用 WSRR Business Space 用户界面来创建和监管业务服务及其关联对象。

必须先在 Business Space 中创建 SOA 监管空间，然后才能创建策略。如果尚未创建 SOA 监管空间，请参阅第 87 页的『为首次使用配置 Business Space』，并遵循以下步骤创建空间。

有关创建新的受监管服务的更多信息，请参阅 IBM WebSphere Service Registry and Repository V8.0 信息中心 - 教程: 管理新服务。

有关监管现有服务的更多信息，请参阅 IBM WebSphere Service Registry and Repository V8.0 信息中心 - 教程: 管理现有服务。

相关任务:

第 86 页的『连接到 WSRR - 业务空间』
使用业务空间用户界面管理策略。

策略

在创建调解策略时，将 WSRR 用作策略编写点和将 WebSphere DataPower 用作策略执行点的实施详细信息。

WSRR 中的策略

WSRR 可以用于编写所有 SOA 策略，包括 SLA（服务级别协议）策略、调解策略、监控策略、定制策略和其他将在以后支持的策略域。使用业务空间用户界面，您可以在 WSRR 中创建、更新或删除策略文档。策略文档可以包含为特定策略域指定大量策略的策略表达式。或者，可以创建策略文档，以用于组装其他文档中的现有策略。可以使用策略标识来引用个别策略，在将策略添加到文档时可以指定策略标识。策略表达式表示策略的声明，相当于 WS-Policy 文档中的 `<wsp:Policy>` 元素。

要在 Business Space 中创建调解策略，请参阅第 97 页的『编写新策略』。

调解策略断言

服务级别协议 (SLA) 应来自于业务需求，即服务提供的服务质量必须满足指定标准。设计服务时，创建功能性需求以指导服务采用的逻辑。在该服务的分析和设计中，应同时指定非功能性需求，从而指定预计服务将提供的服务质量。例如，企业可能具有一项服务: 提供信息以对客户互联网查询做出响应。目标是在 3 秒内返回响应。在端到端事务工程中，确定此服务必须在 2 秒内返回其信息，以便满足企业非功能性需求。

当未满足 SLA 时，我们可以编写将对服务性能实施运行时检查的策略，并采取操作，以便保障服务满足其 SLA。例如，我们可能具有一个通常能够在 2 秒内提供服务响应（95% 的情况）的服务主端点。SOA 架构设计师在另一台服务器上创建次要端点，这通常是针对主端点停运而用作热备用，但当主端点无法满足事务负载时，也可以被授权用于处理溢出流量。当必需满足 SLA 时，我们可以编写策略，用于检查服务响应时间和重新路由流量。

通过运行时策略维护 SLA 的另一个示例是，服务对具有各种消费者且每个消费者具有不同级别优先级的事务做出响应的情况。例如，我们可能有“gold”和“bronze”客户，但只保障“gold”客户的特定服务质量。在本示例中，我们可以检查客户是否为“gold”客户，然后重新路由至次要端点，而继续以较慢的响应速度处理“bronze”客户。企业决定，由于“bronze”客户不能提供足够的收入增长额，从而牺牲响应时间以满足“gold”客户的 SLA。

在第三个示例中，我们可能遇到一种情况，服务将尽其所能，但当它确定处于超负荷时，它将对低优先级客户服务的消息采取排队甚至拒绝措施。其中一个例子是，当客户请求的批处理例程突然占满系统。为了保证服务质量，我们可以创建仅在办公时间有效的运行时策略，在此期间将拒绝所有批处理请求。

通常，调解策略允许在提供给服务器（提供者）之前，验证和转换客户机（消费者）的入局消息。

策略支持此类消息验证和转换。可以仅为提供者服务、特定消费者/提供者对或提供者服务的匿名消费者指定策略。针对匿名客户的策略提供一种用于定义缺省策略的方式，此缺省策略仅适用于未应用任何其他策略的消费者。使用此功能将为不标识自己的无赖消费者指定策略。这样此类消费者服务就可以拒绝其事务。这可以有助于防止充当消费者的黑客尝试使用事务占满系统以降低提供者服务质量的拒绝服务攻击。

调解策略条件

可以进行调解断言，这使运行时策略能够控制服务的 SLA、从消费者到提供者的消息转换，或验证消费者消息的消息模式。

SLA 策略条件（调解策略的特殊类型）实际上允许具有条件的典型 if-then-else 结构，然后根据条件求值情况来执行一组操作。指定条件为可选。如果未指定任何条件，那么它就相当于逻辑条件求值为 True，并将相应地执行任何指定的操作。

如果指定了条件，那么条件必须包含布尔表达式和/或调度规范。

调度

如果指定，那么调度标识策略生效时间。根据本地策略执行点对指定的日期和时间求值，使用的时区是该策略执行点的时区。如果未指定任何调度，那么策略在从策略编写点下载到策略执行点就开始执行，并一直继续。

调度可定义一个可选的开始日期和一个可选的停止日期、一个可选的每日期限以及一个可选的工作日列表。例如，可以定义调度有效期自 2012 年 10 月 1 日到 2012 年 10 月 30 日，在星期三和星期天从早上 8 点到下午 5 点。

可以指定的调度参数如下所示:

- **StartDate** - 此可选属性指定了调度生效日期（xs:date 格式）。StartDate 包含在内，如果该属性不存在，那么调度将在今天立即有效。

  注: 单击 xs:date 超链接以了解此行业标准。
- **StopDate** - 此可选属性指定调度停止有效的日期（xs:date 格式）。StopDate 不包含在内，并且所指定的日期应晚于开始日期。当终止日期早于或等于开始日期时，调度将永远无效。如果该属性不存在，那么调度将永久有效。
- **Daily** - 此可选元素指定调度有效的每日期限。如果该元素不存在，那么调度将全天有效。
  - **StartTime** – 如果指定 Daily，那么需要此属性。它指定调度每天开始的时间（采用 xs:time 格式）。（注: 单击 xs:time 超链接以了解此行业标准）。
  - **StopTime** - 如果指定 Daily，那么需要此属性。它指定调度每天停止的时间（采用 xs:time 格式）。StopTime 不包含在内，并且所指定的时间早于或与每天开始时间相同，那么调度会在次日指定的停止时间停止。

- **Weekdays** - 此可选元素指定调度中包含的每周天数。如果该元素不存在，那么调度中包含一周内的每一天。此元素仅影响日常时间表的开始，因为调度允许在午夜一直运行。例如，如果调度设置为在星期三晚上 11 点开始并运行 2 小时，那么调度实际上将在星期四凌晨 1 点结束。
  - **Days** - 如果指定了 Weekdays，那么需要此属性。它列出了调度中包含的工作日，名称列表之间用加号（“+”）隔开；例如，“Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday”。

调解策略条件表达式

条件表达式是指定布尔表达式的非重复元素（如果指定）。

表达式包含三个必需的参数（Attribute、Operator 和 Value）以及一个可选的 Interval 和 Limit。如果对 Attribute 和 Value 应用 Operator 以及 Interval 和 Limit（适当情况下），求值为 True，那么表达式求值为 True。限制元素仅与 HighLow 和 TokenBucket 运算符一起使用。如果未指定，那么 Limit 的值为 0。如果未指定 Interval，那么缺省值为 60 秒。

指定的表达式参数如下:

- **属性** - 下表概述了定义的属性及其类型。

表 38. 定义的属性

属性	描述和类型
ErrorCount	此监视时间间隔期间检测到的故障数。
MessageCount	监视时间间隔内拦截的实际消息数。
InternalLatency	内部等待时间（处理时间，秒）。
BackendLatency	设备到服务器等待时间（秒）。
TotalLatency	后端和内部等待时间之和（秒）。

- **运算符** - 下表概述了可用运算符及其含义:

表 39. 运算符

运算符	含义
GreaterThan	一个简单的数字算法，当属性大于定义的值时，为 True。
LessThan	一个简单的数字算法，当属性小于定义的值时，为 True。
TokenBucket	一种基于速率并允许脉冲串传输的算法。算法包含最大容量为限制令牌数的存储区。每个时间间隔之间以固定比率的值令牌填满存储区，而对于每个属性单元，除去令牌。当存储区中没有令牌时，该算法求值为 True，否则，求值为 False。这里有个示例可以帮助说明此算法：假设限制=100，值=5，时间间隔=1 秒，属性=MessageCount。 1. 使用最大容量为 100 个令牌填满存储区。 2. 当消息到达时，算法检查存储区是否包含任何令牌: a. 如果有，那么算法求值为 False，会从存储区中除去一个令牌。 b. 如果没有，那么算法求值为 True。 3. 同时，算法每秒钟会向存储区中添回 5 个令牌（如果空间允许）。

表 39. 运算符 (续)

运算符	含义
HighLow	一个算法，当属性达到指定为值的高阈值时，求值为 True，在属性达到指定为限制的低阈值之前，继续求值为 True。

- **Value** – 这是正整数元素。“0”有效。
- **Interval** - 此可选元素定义用作滑动窗口的时间间隔，以在对表达式求值时度量 wsme:Attribute，格式为 xs:duration。如果未指定，那么使用的时间间隔为 60 秒。如果指定，应指定一个合理值，将配置的策略执行点功能考虑在内。即，值越高，策略执行点跟踪属性需要的内存越多。

  注: 单击 xs:duration 超链接以了解此行业标准
- **Limit** - 此可选整数元素定义当 wsme:Operator 为 TokenBucket 或 HighLow 时所需的其他 Limit 参数。单位取决于指定的 wsme:Operator。

  当 wsme:Operator 为 HighLow 时，这定义低阈值，而 wsme:Value 定义高阈值。指定的阈值应该低于 wsme:Value 的值。当未指定时，缺省限制为 0。

  当 wsme:Operator 为 TokenBucket 时，这定义脉冲串传输的最大大小，或存储区中令牌的最大数，而值指定每个时间间隔令牌数填满存储区的速率。当未指定时，缺省限制为 0，TokenBucket 相当于 GreaterThan 操作。

调解策略操作

调解 Action 元素指定要采取的操作。尽管语法允许多种组合，它们并非都有意义，当指定冲突操作时（如要求对消息同时执行排队和拒绝操作），策略编写点将拒绝此行为。允许的调解策略操作为:

- **QueueMessage** – 此操作指定当满足逻辑条件时，事务将排队。将不会重新开始消息处理，直至不再满足逻辑条件。队列方法和任何相关的超时如示例 WebSphere DataPower 中策略执行点所定义。当在单个 Action 元素中指定多个操作时，QueueMessage 应该是第一个操作。
- **RejectMessage** – 此操作指定当满足逻辑条件时，将拒绝事务。将继续拒绝事务，直至不再满足逻辑条件。当拒绝事务时，会将 SOAP 故障返回至客户机（消费者）服务。当在单个 Action 元素中指定多个操作时，RejectMessage 应该是第一个操作。QueueMessage 和 RejectMessage 互斥。
- **Notify** - 此可选元素指定当满足逻辑条件时，将产生通知。对于 WebSphere DataPower，将消息写入 DataPower 系统日志。
- **RouteMessage** - 此可选元素指定当满足逻辑条件时，会将消息路由至指定的端点目标。将继续将消息路由至指定的端点，直至不再满足逻辑条件。
  - **EndPoint** – 当指定 RouteMessage 操作时，此参数为必需的。受支持的端点值可以是 IP 地址、主机名或虚拟主机；例如负载均衡器组。
- **ValidateMessage** - 此可选元素指定应根据指定的语法对消息进行验证。验证失败时应拒绝消息。如果指定了 ValidateMessage，那么必须将 XSD 或 WSDL 指定为子参数。SCOPE 可选，如果未指定，那么 SOAPBody 用于验证。
  - **XSD** - 指定将针对它包含的 URI 标识的 XML 模式，验证消息。
  - **WSDL** - 指定将针对它包含的 URI 标识的 Web service 描述 (WSDL)，验证消息。

– **SCOPE** - 指定将验证消息的哪一部分。下表列出了可能值及其含义:

表 40. ValidateMessage 元素

值	描述
SOAPBody	验证 SOAP 主体元素的内容，而不对 SOAP 故障进行特殊处理。（缺省值）
SOAPBodyOrDetails	对于 SOAP 故障，验证详细信息元素的内容，否则验证主体元素的内容。
SOAPEnvelope	验证包括信封在内的整个 SOAP 消息。
SOAPIgnoreFaults	如果消息是 SOAP 故障，那么不进行任何验证，否则验证 SOAP 主体元素的内容。

- **ExecuteXSL** - 指定将使用指定的 Stylesheet 和 Parameter 执行 XSL 转换。执行失败时，将拒绝事务。必须指定 Stylesheet 信息，而 Parameter 为可选，应根据指定的特定样式表的需要来指定。
  – **Stylesheet** - 指定转换操作将使用由包含的 URI 指定的样式表。样式表必须是 XSLT 文件。
  – **Parameter** - 此可选的重复元素指定要用于 ExecuteXSL 操作的样式表参数。
    - **Name** – 每个对应的 Parameter 参数都需要此属性，它指定了参数的名称。
    - **Value** - 每个对应的 Name 参数都需要此属性，它指定了参数的值。

编写新策略

在 Business Space 用户界面中编写调解策略时，为策略指定条件和操作。

开始之前

有关访问 Business Space 的信息，请参阅第 86 页的『连接到 WSRR - 业务空间』。

必须先创建 SOA 监管空间，然后才能创建策略。如果尚未创建 SOA 监管空间，请参阅第 87 页的『为首次使用配置 Business Space』，并遵循以下步骤创建空间。

关于此任务

使用 SOA 监管空间编写新策略。

过程

1. 打开 SOA 监管空间:
   a. 单击**转至空间**。这样会显示“转至空间”对话框。
   b. 单击针对“SOA 管理”用户的空间。具体名称取决于创建空间时指定的内容。
2. 在“概述”选项卡上，单击**创建调解策略**。
3. 输入有意义的名称，以及可选描述。
4. 根据需要添加条件和操作。 有关条件和操作的更多信息，请参阅第 93 页的『策略』和 IBM WebSphere Service Registry and Repository V8.0 信息中心 - 创建调解策略。
5. 单击**完成**。

结果

此时将创建策略并将其存储在 WSRR 中。要查看刚刚创建的策略的策略文档，请选择屏幕左下角的“服务注册表导航器”窗口小部件中的策略文档。或者，搜索指定的名称，尾部包含 .xml。策略文档将在右侧的“服务注册表详细信息”窗口小部件中显示。

相关概念:

第 93 页的『策略』

在创建调解策略时，将 WSRR 用作策略编写点和将 WebSphere DataPower 用作策略执行点的实施详细信息。

相关信息:

IBM WebSphere Service Registry and Repository V8.0 信息中心 - 创建调解策略

管理策略

可以使用“业务空间”用户界面编辑或除去策略。

开始之前

配置 SOA 监管空间。有关更多信息，请参阅第 87 页的『为首次使用配置 Business Space』。

过程

1. 要打开策略的策略文档，请在屏幕左下角的“服务注册表导航器”窗口小部件中选择策略文档。或者，搜索指定的名称，尾部包含 .xml。 策略文档将在右侧的“服务注册表详细信息”窗口小部件中显示。
2. 要更改策略详细信息:
   a. 单击此窗口小部件中的“编辑”图标以编辑策略文档。 此时将显示一个窗口，其中包含编辑策略详细信息选项。
   b. 如果策略具有任何条件或操作，将显示这些条件和操作。根据需要创建并修改条件和操作。
   c. 单击**完成**以保存并关闭策略编辑器。 “服务注册表详细信息”窗口小部件将刷新，以显示执行的更改。
3. 要删除策略:
   a. 将策略转换为监管状态，以允许编辑或删除策略文档。有关在 SOA 策略生命周期中转换策略的更多信息，请参阅『管理策略的生命周期』。
   b. 单击**操作 > 删除**。 “删除”选项位于菜单中。
   c. 选择**删除**以删除策略。
   d. 单击**是**以确认删除。

相关信息:

IBM WebSphere Service Registry and Repository V8.0 信息中心

IBM WebSphere Service Registry and Repository V8.0 信息中心 - 监管支持概要文件中的策略

管理策略的生命周期

可以使用 Business Space 用户界面在监管状态之间转换策略。

关于此任务

有关监管的更多信息，请参阅第 3 页的『SOA 策略生命周期』。

过程

要将策略转换为不同的生命周期状态，请完成以下步骤。根据需要多次重复这些步骤以进入期望的生命周期状态:

1. 在 Business Space 中，通过在屏幕左下角的“服务注册表导航器”窗口小部件中选择策略文档，打开策略的策略文档。或者，搜索指定的名称，尾部包含 .xml。 策略文档将在右侧的“服务注册表详细信息”窗口小部件中显示。**监管状态**属性显示概要文件的最新监管状态。
2. 单击**操作**。 可能的生命周期转换列表将随其他可能的操作一起显示。
3. 选择所需的生命周期转换以将策略移至所需的状态。 这样会更新策略的**监管状态**属性以显示新的生命周期状态。

相关概念:

第 3 页的『SOA 策略生命周期』
使用 SOA 策略生命周期监管调解策略。 这将使策略从最初识别，一直到部署到生产中，最后在不再需要时弃用。

相关信息:

IBM WebSphere Service Registry and Repository V8.0 信息中心 - SOA 策略生命周期

附加到服务的策略

可以使用 WSRR 将策略附加到服务。

有关更多信息，请参阅IBM WebSphere Service Registry and Repository V8.0 信息中心 - 策略附加任务。

第 7 章 故障诊断

获得您在部署模式之前、期间和之后遇到的诊断问题的援助。

使用以下链接以查找与模式问题相关的主题。

对部署问题进行故障诊断

当在 IBM SOA Policy Gateway Pattern 中部署模式时可以对常见问题进行故障诊断。

部署期间，无法连接到 DataPower

尝试以下解决方案:

- 检查 DataPower 管理员用户和密码是否有效:
  - 在 DataPower 中，通过转至**控制面板 > 管理用户帐户**验证存在此用户。
  - 检查帐户是否存在。
  - 检查用户是否有权使用 XML 管理界面；例如，系统管理员。
  - DataPower 管理员可能需要检查用户代理设置中是否启用了此用户帐户；例如，基本认证设置。
- 检查 DataPower 主机名是否正确
- 检查是否启用 DataPower XML 管理界面。
- 查看下面的 SSL 连接故障步骤以验证在 `DomainZipFile.zip` 和 DataPower 设备上正确安装证书。

对“相互认证”客户机认证的故障进行故障诊断

尝试以下解决方案:

- 检查正确的证书是否存在于 `DomainZipFile.zip` 中。
- 检查 XML 管理界面端口上的加密概要文件是否具有包含链中所有证书的验证凭证。
- 检查客户机公用密钥和客户机公用证书的密码是否正确。

对服务器认证的故障进行故障诊断

尝试以下解决方案:

- 检查链中所有证书是否都存在于所使用的 `DominZipFile.zip` 文件的 *`yourDataPowerHostName`* 目录中。
- 检查 SSL 代理概要文件是否具有包含证书链的身份凭证的反向加密概要文件。

对已存在域的错误进行故障诊断

尝试以下解决方案:

- 在 DataPower 控制面板上，打开应用程序域。检查域是否已存在。

对样本应用程序的端口重叠错误进行故障诊断

如果某个样本服务不可用，那么检查您域中的端口是否与其他域中的发生冲突。

尝试以下解决方案:

- 登录 DataPower，并切换至样本域。然后，打开“控制面板”，单击“XML 防火墙”图标。检查 XML 防火墙是否都处于“运行”状态。
- 搜索 HTTP 前端处理程序。检查单个 HTTP 前端处理程序是否处于“运行”状态。

对未能连接到 SCP 进行故障诊断

尝试以下解决方案:

- 检查 SCP 主机名是否正确。
- 检查 SCP 用户是否正确。
- 检查 SCP 密码是否正确。
- 通过提供的信息手动从 IBM Workload Deployer 或 IBM PureApplication System 环境中的节点测试 SCP。

对从 SCP 检索 DomainZipFile.zip 文档或调试缺失工件的故障进行故障诊断

尝试以下解决方案:

- 检查 DomainZipFile.zip 是否存在于 URI 中。
- 检查日志故障中的文件是否存在于 DomainZipFile.zip 文件中的正确位置。特别是，确保所需的证书位于正确目录中。

对提升故障进行故障诊断

提升过程中可能出现很多问题，包括部署期间连接到 Governance Master 的故障。

尝试以下解决方案:

- 检查参数:
  - 检查 Governance Master WSRRCELL 的用户。
  - 检查 Governance Master WSRR Cell 的用户密码。
  - 检查 WSRR Governance Master Cell 的主机名。
  - 检查 WSRR Governance Master Cell 的 CELL 名称。
- 检查签署者证书交换:
  - 请转至 Governance Master 单元的 Cell Default Trust Store，并确保存在运行时环境部署管理器或独立服务器、SOA Policy Gateway Basic Runtime 或 SOA Policy Gateway Advanced Runtime 的证书项。
  - 转至每个运行时环境: SOA Policy Gateway Basic Runtime 或 SOA Policy Gateway Advanced Runtime，并检查 CellDefaultTruststore（针对 ND 环境案例）或 NodeDefaultTrustStore（针对 WSRR 独立服务器），以确保 Governance Master 的部署管理器存在证书。
  - 使用相同密码导出单元中的 LTPA 密钥，并检查它们是否相同（例如，字节数）。
- 确保提升属性文件包含适当主机和端口的服务器部分，以及用户和密码信息。此信息可以在 Governance Master 的 ServiceRegistry 控制台中找到:

– 转至 GovernanceMasterDMgrHost 或 ServiceRegistry 并切换至配置透视图。在“操作”部分，找到**提升**并打开提升属性文件。对于每种环境，登台 WSRR 节点或集群中每个服务器都应有 XML 元素。如果存在生产集群或节点，那么每个都应存在 server:port 条目，另外，还应存在用户和密码信息。

- 检查服务版本和 SOAP 端点是否都存在登台和生产的分类。
  – 在“服务注册表控制台”中，选择“SOA 监管”透视图。打开“服务版本”，然后选择“分类”选项卡。必须启用登台和生产。

对定制的 CLI 故障进行故障诊断

尝试以下解决方案:

- 检查 DataPower 域中错误消息的缺省日志。
- 启用 CLI 调试并检查那些日志是否在 CLI 的其他运行之前。

对由于缺失 DataPower 证书而导致的 SSL 故障进行故障诊断

如果未在 `DomainZipFile.zip` 文件中提供针对 DataPower 证书目录的正确主机名，那么在 DataPower 主机上启用相互认证或服务器认证的情况下，脚本程序包将无法连接至 WSRR 服务器。

对 WSRR/DataPower 连接问题进行故障诊断

如果在 Web Service 代理中看到 WSDL 的状态为 Down 或 Synchronizing，从未更改为 Okay，请检查以下项:

1. 检查 WSRR 服务器 (WSRRSVR) 的加密证书是否有效。
2. 检查 DataPower 是否设置了正确的 DNS 以识别 WSRR 服务器或部署管理器的主机名。
3. 如果 DNS 不正确，临时的变通方法是用 IP 替换 WSRR 服务器定义中 URL 内的主机名，从而将该 URL 更改为直接指向该 IP。
4. 转至 WSRR 预订并执行手动同步:
   a. 查看 `default.log`，以了解与 WSRR 服务器连接相关的错误。
5. 确保所需证书与 DataPower 设备 XML 管理接口 SSL 代理概要文件的加密概要文件身份凭证中的证书匹配。

部署实例中的故障诊断问题

您可以对部署实例中的常见问题进行故障诊断。

无法连接至 LDAP

要对样本中的 LDAP 故障进行故障诊断，请尝试以下解决方案:

- 在 DataPower 控制面板故障诊断中，确保跟踪处于调试方式。
- 转至 StoreAddLTPA，打开探测器详细信息并启用探测器。
- 运行客户机测试。
- 查看探测器中的日志。查找 LDAP 绑定故障消息。
- 检查 LDAP 主机名。
- 检查 LDAP DN; 例如，cn=root，dc=ibm.com。

- 检查 LDAP 密码；例如，passw0rd。
- 检查 LDAP 端口是否为 389 且不安全。
- 检查 ConsumerX、ConsumerA、ConsumerB 的输入密码是否都为 passw0rd。确保 LDIF 文件导入已记录正确的密码。

到 LDAP 服务器或 DataPower StoreWSP 端口的连接失败

如果 DataPower 日志显示到 LDAP 或 StoreWSP 网关的连接错误，并且您正在使用主机别名，那么您的域设置可能有问题；例如，`xyz` 代替脚本程序包中以下一个参数的标准主机 `xyz.company.com` 名称:

- DataPower 主机名
- LDAP 主机名

尝试以下解决方案:

1. 在 DataPower 管理控制台中，切换至缺省域。
2. 搜索配置 `DNS` 设置。
3. 单击“搜索域”选项卡。
4. 确保您的域（例如 `company.com`）位于列表中。如果该域未在列表中，请单击添加，将其添加到列表中。

收集诊断信息

您可以使用日志来帮助查找和解决问题。日志存储在设备上并可从用户界面进行查看，也可以将其下载到本地文件系统。

过程

要收集诊断信息，请完成以下步骤:

1. 查看虚拟实例:
   a. 单击**实例 > 虚拟系统**。
   b. 从“虚拟系统实例”窗口的实例列表中选择实例。
2. 对于 WSRR 虚拟机:
   a. 在**虚拟机**部分中，展开 WSRR 虚拟机，然后检查**脚本包**部分中是否有任何错误。如果任何脚本包存在错误，请单击脚本包名称旁的 **remote_std_out.log** 和 **remote_std_err.log** 日志链接。
   b. 登录到 WSRR 实例，然后检查服务器错误。
   c. 请参考 WSRR 故障诊断指南: http://pic.dhe.ibm.com/infocenter/sr/v8r0/topic/com.ibm.sr.doc/cwsr_troubleshootingandsupport.html
3. 对于 DataPower:
   a. 检索由模式创建的域的 **default.log** 文件。
   b. 检索缺省域的 **default.log** 文件。

第 8 章 维护和支持

您可以执行维护功能，例如，应用紧急修订。

将紧急修订添加到目录

作为紧急修订应用于虚拟系统实例的临时修订和修订包。您可以向要应用于虚拟映像的目录添加紧急修订。

开始之前

您必须分配*新建目录内容*许可权或具有完整许可权的 IBM Workload Deployer 设备*管理员*角色，才能执行这些步骤。

关于此任务

修订由 IBM 或映像提供者提供，并且必须下载。从 IBM Fix Central 下载新修订。然后，将修订上载至目录，而且可应用于所有适合的虚拟系统实例。

过程

完成以下步骤以将紧急修订添加至目录。

1. 从 Fix Central 查找并下载紧急修订。
2. 可选: 您一次可添加多个临时修订。要一次添加多个修订，请从 Fix Central 下载压缩文件，并将它们打包为单个压缩文件。
3. 从菜单中选择**目录 > 紧急修订**。
4. 单击左侧面板中的添加图标。
5. 输入要添加的修订的名称。您还可以选择添加要添加的修订的描述。修订在“紧急修订”窗口的左侧面板中显示，并且修订信息在右侧面板中显示。
6. 浏览至存储修订的位置，然后单击**上载**。出于安全原因，只能上载 .zip、tgz 和 pak 文件。Red Hat RPM 也受支持。
7. 填写有关修订的信息。您可以授予用户访问权并提供严重性评级。使用**适用于**字段指定要应用此修订的虚拟映像。

结果

紧急修订位于目录中，并且可应用于虚拟系统映像。

应用紧急修订

作为紧急修订应用于虚拟系统实例的临时修订和修订包。您可以将紧急修订应用于虚拟系统映像。

开始之前

必须为您分配针对虚拟系统实例的所有访问权，或者分配具有完整许可权的设备管理角色，才能完成这些步骤。必须针对要安排或应用的服务启动虚拟系统实例。必须先

将紧急修订添加到目录中，然后才能将该修订应用于虚拟系统。

关于此任务

添加新的紧急修订时，您需要定义该修订适用的虚拟映像。使用适合用于创建虚拟系统实例的虚拟映像的所有修订来构造调度服务请求时适用的修订列表。如果已将某个修订应用于虚拟系统，那么可以在**历史记录**列表中看到该修订并且它未包含在可用修订列表中。

过程

完成以下步骤以应用临时修订。

1. 从“虚拟系统实例”窗口中选择要应用修订的虚拟系统实例。
2. 单击『应用服务』图标。
3. 可选: 安排服务请求。缺省情况下，将立即应用修订。要安排在以后应用，请单击**安排服务**，并提供必要的信息。
4. 单击**选择服务级别或修订**。
5. 单击**应用紧急修订**以查看并选择要应用的修订。紧急修订应用于虚拟系统实例中的所有虚拟机。虚拟系统实例的状态表明服务已应用于虚拟系统。
6. 检查错误。 检查以下文件以确保在应用紧急修订的过程未发生任何错误:
   - Remote_std_out.log
   - Remote_std_err.log

   您可以从“虚拟系统实例”窗口访问日志文件。

第 9 章 Appendices

声明

本信息是为在美国提供的产品和服务编写的。IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。 有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，将由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

有关双字节（DBCS）信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

本条款不适用英国或任何这样的条款与当地法律不一致的国家或地区:

International Business Machines Corporation“按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。某些国家或地区在某些交易中不允许免除明示或暗含的保证。因此本条款可能不适用于您。

本出版物中可能包含技术方面不够准确的地方或印刷错误。 此处的信息将定期更改；这些更改将编入本资料的新版本中。IBM 可以随时对本资料中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本程序的被许可方如果要了解有关程序的信息以达到如下目的: （i）允许在独立创建的程序和其他程序（包括本程序）之间进行信息交换，以及（ii）允许对已经交换的信息进行相互使用，请与 IBM United Kingdom Laboratories 联系，地址为: MP151, Hursley Park, Winchester, Hampshire, England, SO21 2JN。只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际软件许可协议或任何同等协议中的条款提供。

商标

IBM、IBM 徽标和 ibm.com 是 International Business Machine Corp., 在全球许多司法区域注册的商标或注册商标。 其他产品和服务名称可能是 IBM 或其他公司的商标。Web 上的版权和商标信息（www.ibm.com/legal/copytrade.shtml）提供了 IBM 商标的最新列表。

将您的意见发送至IBM

您可以通过以下方式向 IBM 发送意见

请仅使用这些联系方式来发表您对文档的意见。

如果您需要特定的销售或服务帮助或者对 IBM 产品或系统的功能有具体意见，请与 IBM 代表联系。

您可以向 IBM 发送意见通过以下方式:

- 邮件:

  User Technologies Department (MP095)
  IBM United Kingdom Laboratories
  Hursley Park
  WINCHESTER,
  Hampshire
  SO21 2JN
  United Kingdom
- 传真:
  - 其他国家或地区 44-1962-816151
  - 英国: 01962-816151
- 电子邮件:
  - idrcf@hursley.ibm.com

无论您使用哪种方法，请确保包含下列信息:

- 这本书的标题。
- 主题引用和标题（如果您要对特定主题发表意见的话）。
- 您的姓名和联系方式，如果你想要一个答复。

细则

通过选择向 IBM 发送消息，即表明您承认您的消息中包含的所有信息（包括反馈数据，例如问题、意见、建议或类似数据）将视为非保密信息，并承认，IBM 关于此类信息不承担任何种类的义务并将可自由地、无限制地复制、使用、泄露该信息和向他人分发该信息。并且，IBM 将可自由地将此类信息中包含的任何构想、概念、专有技术或技巧用于任何用途，包括但不限于开发、制造和销售包含此类信息的产品。