IBM SOA
Policy Gateway Pattern

Índice

Capítulo 1. Visão Geral de SOA Policy. . 1
A Arquitetura SOA Policy 1
O Ciclo de Vida de SOA Policy 5
Padrões de Política 5

Capítulo 2. Visão Geral de Padrão . . . 9

Capítulo 3. Introdução ao IBM SOA Policy Gateway Pattern 13
Fazendo Download e Instalando os Padrões . . . 13
Verificando o Padrão Instalado 14
Aceitando Licenças 15
Configurando o Acesso de Usuário 16

Capítulo 4. Padrões, Partes e Pacotes de Scripts 19
Padrões. 19
SOA Policy Gateway Basic Runtime Sample (x86) 19
SOA Policy Gateway Governance Master . . . 21
SOA Policy Gateway Basic Runtime 22
SOA Policy Gateway Basic Runtime External DataPower 23
SOA Policy Gateway Advanced Runtime . . . 25
SOA Policy Gateway Advanced Runtime External DataPower 26
Serviço Compartilhado 28
System Monitoring for SOA Policy Gateway . . 28
Partes 29
Parte do DB2 Enterprise 29
Parte de HADR Primário do DB2 Enterprise . . 31
Parte de HADR de Espera do DB2 Enterprise . . 33
Parte do Servidor Independente do WSRR . . . 35
Parte do Gerenciador de Implementação do WSRR 36
Parte de Nós Customizados do WSRR 36
Parte do DataPower 37
Pacotes de Scripts 38
Script: SOA Policy Gateway 2.5.0.0 - Domínio do DataPower 38
Script: SOA Policy Gateway 2.5.0.0 - Promoção 39
Script: SOA Policy Gateway 2.5.0.0 - Amostra . . 40
Script: SOA Policy Gateway 2.5.0.0 - Segurança 42
Script: SOA Policy Gateway 2.5.0.0 - Monitoramento do DataPower (apenas x86) . . 42
Script: SOA Policy Gateway 2.5.0.0 - Monitoramento Externo do DataPower 43

Capítulo 5. Trabalhando com o IBM SOA Policy Gateway Pattern 45
Planejando a Configuração do Padrão e Pré-requisitos do Padrão 45
Configurando um Dispositivo DataPower para os IBM SOA Policy Gateway Patterns. 46
Segurança para os Padrões IBM SOA Policy Gateway Pattern. 46
Implementando Padrões 47
Implementando o Serviço Compartilhado de Monitoramento do Sistema 48
Implementando o Padrão de Amostra de Tempo de Execução Básico 49
Implementando o Padrão de Controle Principal 50
Implementando um Padrão de Tempo de Execução Básico 52
Implementando um Padrão de Tempo de Execução Avançado. 53
Atualizando o DataPower na Instância Implementada 54
Verificando a Implementação 55
Incluindo um Ambiente de Tempo de Execução Adicional 55
Incluindo Instâncias do DataPower em um Padrão 56
Excluindo Instâncias do DataPower a Partir de um Padrão 56
Implementando os Padrões do DataPower Externo Básico e Avançado 57
O Aplicativo de Amostra 58
Visão Geral de Artefatos do WSRR na Amostra 60
Executando os Casos de Teste de Amostra . . . 61
Estendendo o Aplicativo de Amostra 68
Exploração Adicional da Amostra 71
O Domínio de Amostra do DataPower 72

Capítulo 6. Trabalhando com a Instância Implementada 81
Acessando Instâncias Implementadas. 81
Conectando ao WSRR - Business Space 82
Conectando ao WSRR - UI da Web do WSRR . . 84
Conectando ao Console Administrativo do WebSphere Application Server 85
Conectando ao Console de um DataPower Virtual 85
Conectando ao Console de Monitoramento . . . 86
Parando e Iniciando a Instância Implementada . . 86
Configuração de Padrão de Pós-implementação . . 87
Configurando o Policy Enforcement Point . . . 87
Certificar Valores de DN para Certificados do DataPower 89
Removendo ou Incluindo Certificados do DataPower no Armazenamento Confiável do WSRR 90
Alterando as Chaves LTPA 90
Criação e Controle de Serviço 91
Políticas 92
Criação de Novas Políticas de Mediação. . . . 97
Criação de Novas Políticas de Monitoramento . . 98
Gerenciando Políticas 99
Gerenciando o Ciclo de Vida da Política . . . 100

Políticas Anexadas a um Serviço 100

Capítulo 7. Resolução de Problemas 101
Resolução de Problemas com a Implementação . . 101
Resolução de Problemas na Instância Implementada 102
Coletando Informações sobre Diagnóstico 103

Capítulo 8. Manutenção e Suporte . . 105
Incluindo uma Correção Emergencial no Catálogo 105
Aplicando uma Correção Emergencial 106

Capítulo 9. Appendices 107
Avisos 107
Informações sobre a Interface de Programação 109
Marcas Comerciais 109
Enviando seus comentários para a IBM. 109

Capítulo 1. Visão Geral de SOA Policy

O gerenciamento de política desempenha uma função-chave no controle de políticas de uma forma estruturada e consistente. As políticas podem ser usadas para permitir melhor controle em qualquer ambiente orientado a serviços.

Uma política é um elemento independente que pode ser aplicado a um ou vários recursos, incluindo serviços diferentes. A designação da política e quaisquer metadados associados, especialmente em um ambiente distribuído, pode ocorrer em vários pontos de execução e pontos de decisão.

A Arquitetura SOA Policy

A arquitetura SOA Policy descreve a interação do Policy Administration Point (PAP), do Policy Enforcement Point (PEP), do Policy Decision Point (PDP), do Policy Information Point (PIP) e do Policy Monitoring Point (PMP). No padrão, o PAP é fornecido por WSRR, o PEP é fornecido por WebSphere DataPower e o PMP por meio do componente de monitoramento do DataPower.

A organização da arquitetura de política básica e a definição desses pontos principais são:

- **Policy Administration Point**. Fornece recursos de política para a criação de uma política, o gerenciamento e o controle da política e a sua designação a recursos e administração dos resultados da política durante o tempo de execução. O PAP inclui um repositório para armazenar políticas. O PAP é fornecido por WSRR.
- **Policy Enforcement Point**. Um Policy Enforcement Point é um ponto funcional que é executado no middleware. Ele executa as ações a seguir:
  - Impinge políticas.
  - Recebe atualizações de política de execução e as deixa prontas ou as converte para uso.
  - Fornece métricas de execução para o Policy Monitoring Point.
  - Fornece resultados e analítica da política de execução para o Policy Administration Point e os Policy Monitoring Points.
  - Altera os locais em que as políticas são aplicadas e impingidas, dependendo do estágio do ciclo de vida:
    - Durante o tempo de design, o próprio WSRR é o ponto de aplicação.
    - Durante o tempo de execução, as políticas são geralmente impingidas pelo sistema intermediário subjacente (middleware) que conecta os provedores de serviços aos clientes.

  Nesse padrão, o PEP é fornecido por WebSphere DataPower.
- **Policy Decision Point**. Um Policy Decision Point avalia solicitações dos participantes com relação às políticas ou contratos e atributos relevantes. O PDP renderiza uma decisão de autorização, eligibilidade ou validação para fornecer resultados calculados.
- **Policy Information Point**. Um Policy Information Point fornece informações externas para o Policy Decision Point, tal como informações sobre o atributo LDAP, ou os resultados de um banco de dados, com informações que devem ser avaliadas para a tomada de uma decisão política.

- **Policy Monitoring Point**. Um componente funcional que fornece a função de monitoramento de política detalhada para a arquitetura geral; por exemplo, a visão geral da política no ambiente distribuído. Ele executa as ações a seguir:
  - Recebimento de atualizações de política de monitoramento e deixá-las prontas ou convertê-las para uso.
  - Capturando a coleta em tempo real e a análise de estatísticas para exibição.
  - Correlacionando, analisando e visualizando os dados que são alimentados por vários coletores em tempo real, incluindo Policy Enforcement Points.
  - Um console de gerenciamento que fornece visibilidade no gerenciamento da rede distribuída de pontos de execução de política e o status dessas execuções.
  - Criar log, agregar medidas e destacar eventos significantes conforme especificado pela política de monitoramento.
  - Fornecer analítica de política de monitoramento para o Policy Administration Point e os Policy Enforcement Points.

  Nesse padrão, o PMP é fornecido pelo componente de monitoramento do DataPower.

O consumidor e o provedor interagem com o middleware, que, por sua vez, interage com o repositório e qualquer software de monitoramento.

Como a Arquitetura SOA Policy Funciona Junto

O fluxo padrão do SOA Policy é mostrado em Figura 1 na página 3.

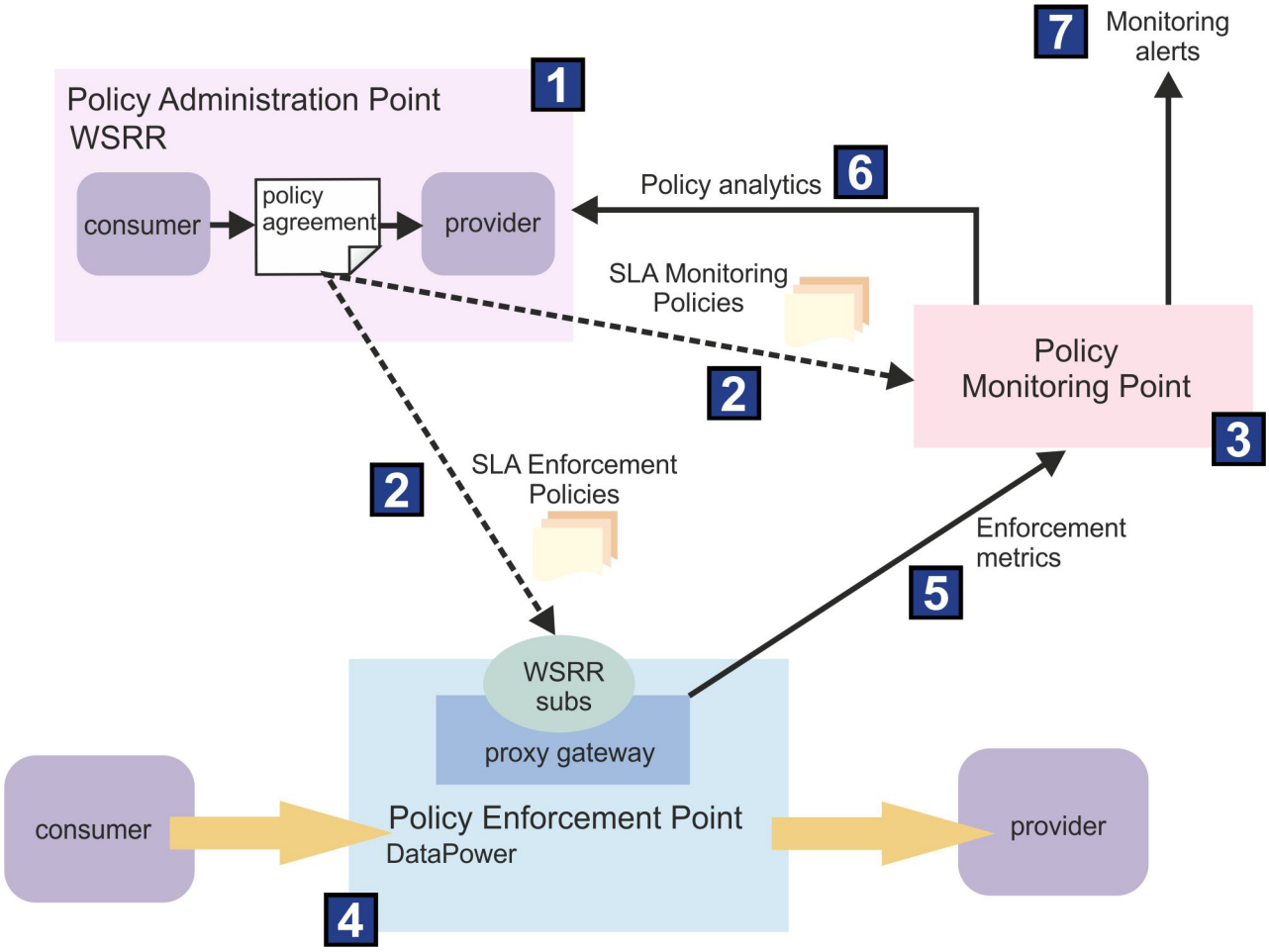


Figura 1. Política de Acordo de Nível de Serviço (SLA) - O Modelo de Implementação SOA

1 As políticas são criadas e, em seguida, anexadas aos serviços que requerem essa política. Geralmente, têm a seguinte ordem:

1. O conjunto de serviços é carregado ou criado no repositório de serviço. Essa ação faz parte do Policy Administration Point.
2. O conjunto de políticas necessário é criado no Policy Administration Point usando o ciclo de vida da política:
   - As políticas são anexadas aos serviços que requerem essas políticas – no nível de serviço, operação ou terminal, conforme necessário.

2 Publicação/assinatura automatizada de políticas a partir do Policy Administration Point até os Policy Enforcement Points e o Policy Monitoring Point:

1. Como parte da configuração, o serviço de monitoramento assina a política de monitoramento do WSRR. Essa ação ocorre apenas uma vez.
2. Como parte da configuração, os gateways de proxy são criados em cada dispositivo WebSphere DataPower (ou dispositivo virtual) que possui transações de serviço com execução de políticas. Essa ação ocorre apenas uma vez e é incluída ou alterada, conforme necessário.

3. Como parte da configuração, cada gateway de proxy no dispositivo assina políticas do WSRR para serviços pelos quais ele é responsável. Essa ação ocorre apenas uma vez e é incluída ou alterada, conforme necessário.
4. Como parte da configuração, o WebSphere DataPower é configurado de modo que as políticas possam ser compartilhadas por outros dispositivos em um cluster. Essa ação ocorre apenas uma vez e é incluída ou alterada, conforme necessário.
5. O Policy Monitoring Point faz download das políticas de monitoramento à medida que elas são publicadas.
6. O Policy Monitoring Point converte as políticas na representação interna chamadas políticas de situação.
7. O WebSphere DataPower faz download dos WSDLs para os serviços pelos quais ele é responsável por transacionar.
8. O WebSphere DataPower faz download das políticas para os serviços pelos quais ele responsável quando notificado pelo WSRR.
9. O WebSphere DataPower converte as políticas para a representação interna do WebSphere DataPower na forma de objetos SLM.

Monitoramento de políticas SOA com relatório e notificação de operações:

1. As políticas de monitoramento estão ativas na Política de Situação do Policy Monitoring Point.
2. O Policy Monitoring Point recebe informações de monitoramento e coloca essas informações em áreas de trabalho.

Execução de Políticas SOA:

1. As políticas de execução estão ativas nos vários dispositivos WebSphere DataPower.
2. O WebSphere DataPower recebe transações de serviço e aplica políticas para esse serviço de cliente e serviço de provedor.

O Policy Enforcement Point envia estatísticas de SOA Policy Enforcement para o Policy Monitoring Point.

O Policy Monitoring Point envia eventos de monitoramento para o Policy Administration Point:

1. Os eventos são configurados no Policy Administration Point que requer monitoramento do Policy Monitoring Point. Essa ação ocorre apenas uma vez e é incluída ou alterada, conforme necessário.
2. À medida que as políticas de situação são avaliadas como verdadeiras, os eventos são enviados ao Policy Authoring Point a partir do Policy Monitoring Point.

Monitoramento de alertas:

- As políticas de situação são executadas periodicamente e tomam uma ação operacional, conforme especificado na política. O padrão é a cada 5 minutos.

O Ciclo de Vida de SOA Policy

As políticas são controladas pelo ciclo de vida de SOA Policy. O ciclo de vida faz com que a política seja inicialmente identificada, até ser implementada na produção e, finalmente, ser descontinuada quando não for mais necessária.

Para obter mais informações sobre as transições do ciclo de vida e os estados no ciclo de vida da Política SOA, consulte Centro de Informações do IBM® WebSphere Service Registry and Repository Versão 8.0 - SOA policy lifecycle.

Padrões de Política

Os grupos de comunidades técnicas da web, W3C e OASIS, criaram padrões para definir as políticas aplicáveis aos serviços da web.

- **WS-Policy**: O domínio Web Services Mediation Policy 1.0 define um conjunto de asserções de política para descrever os requisitos de mediação para um serviço.
- **Web Services Policy 1.5 - Estrutura**: Define uma estrutura e um modelo para expressar políticas que se referem a recursos específicos do domínio, requisitos e características gerais de entidades em um sistema baseado em serviços da web.

Exemplos de especificações que definem asserções de política específica do domínio:

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

Para obter informações adicionais sobre WS-MediationPolicy, consulte ftp://public.dhe.ibm.com/software/solutions/soa/pdfs/WSMediationPolicy1.7-20130506.pdf.

O Modelo de Dados WS-Policy inclui as seguintes entidades:

- **Política**: Uma coleção não ordenada de “alternativas de política”.
- **Alternativa de Política**: Uma alternativa de política é uma coleção de “asserções de política”.
- **Asserção de Política**: Representa uma preferência individual; por exemplo, um requisito ou um recurso.
- **Parâmetros de Política**: A carga útil opaca de uma “asserção de política”.
- **Assunto de Política**: Uma entidade à qual uma expressão de política pode estar ligada. Essa entidade é usada em um documento WS-PolicyAttachment.

O seguinte exemplo, Figura 2 na página 6, mostra uma expressão de política de segurança que usa asserções definidas em WS-Security e em WS-SecurityPolicy:

```
(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">  <!-- expressão de política -->
(02)   <wsp:ExactlyOne>
(03)     <wsp:All>    <!-- alternativa de política nº1 -->
(04)       <sp:SignedParts>;   <!-- asserção de política -->
(05)         <sp:Body>   <!-- parâmetro de asserção de política -->
(06)       </sp:SignedParts>
(07)     </wsp:All>
(08)     <wsp:All>    <!-- alternativa de política nº2 -->
(09)       <sp:EncryptedParts> <!-- asserção de política -->
(10)         <sp:Body/>   <!-- parâmetro de asserção de política -->
(11)       </sp:EncryptedParts>
(12)     </wsp:All>
(13)   </wsp:ExactlyOne>
(14) </wsp:Policy>
```

As linhas (03-07) representam uma alternativa de política para assinar um corpo de mensagem.

As linhas (08-12) representam uma segunda alternativa de política para criptografar um corpo de mensagem.

As linhas (02-13) mostram o operador de política `ExactlyOne`. Os operadores de política agrupam asserções de política em alternativas de política. Uma interpretação válida da política é que uma chamada de um serviço da web assina ou criptografa o corpo da mensagem, mas não ambos.

Figura 2. Uso de Web Services Policy com Asserções de Política de Segurança.

Figura 3 mostra uma definição de política.

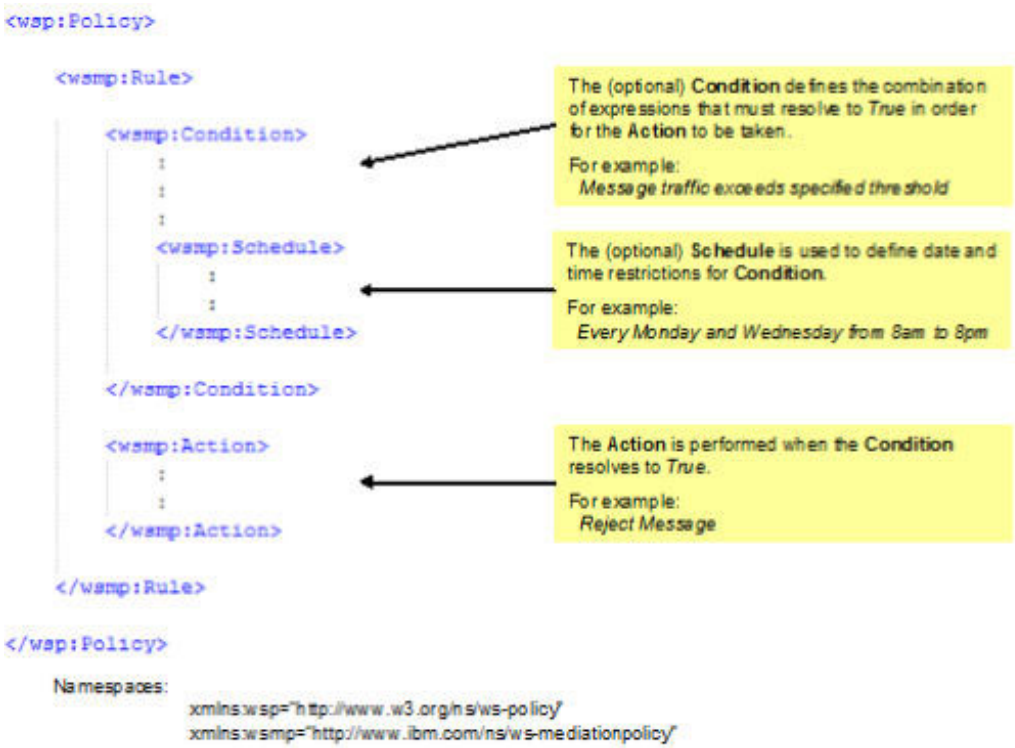


Figura 3. Visão Geral da Estrutura de Política

Anexo sobre a Política

A função Documentar de Anexo sobre a Política é associar um conjunto de políticas WS-Policy a um ponto de anexo de serviço específico para execução, como um ponto de anexo de serviços da web.

Por exemplo, as plataformas de Serviços da Web podem suportar pontos de anexo que são baseados em:

- Elementos de WSDL Element URI 1.1
- Elementos de WS-Addressing

A sintaxe é definida na especificação WS-PolicyAttachment:

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


    </wsp:AppliesTo>
    <wsp:Policy>


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

Figura 4. Especificação WS-PolicyAttachment

O WSRR expõe interfaces REST para adquirir os anexos sobre a política apropriados em um modelo SLA. As informações sobre o par Consumidor/ Provedor ao qual a política se aplica são passadas para o ESB no formato WS-PolicyAttachment. A sintaxe é definida na especificação WS-PolicyAttachment: Filtros de Conteúdo da Mensagem.

A política pode ser especificada para um serviço de provedor apenas, para um par de consumidor/provedor específico ou para consumidores Anônimos. Consumidores anônimos fornecem uma maneira de definir uma política padrão que se aplica apenas aos consumidores aos quais nenhuma outra política se aplica.

No Figura 4, o assunto da política específica do domínio ao qual a política se aplica (o provedor) está contido na seção `<wsp:AppliesTo>`. Ele é seguido pelo filtro de contexto do consumidor ao qual a política se aplica (consumidor). Em seguida, na seção `<wsp:Policy>`, a política, ou políticas, são declaradas ou referenciadas.

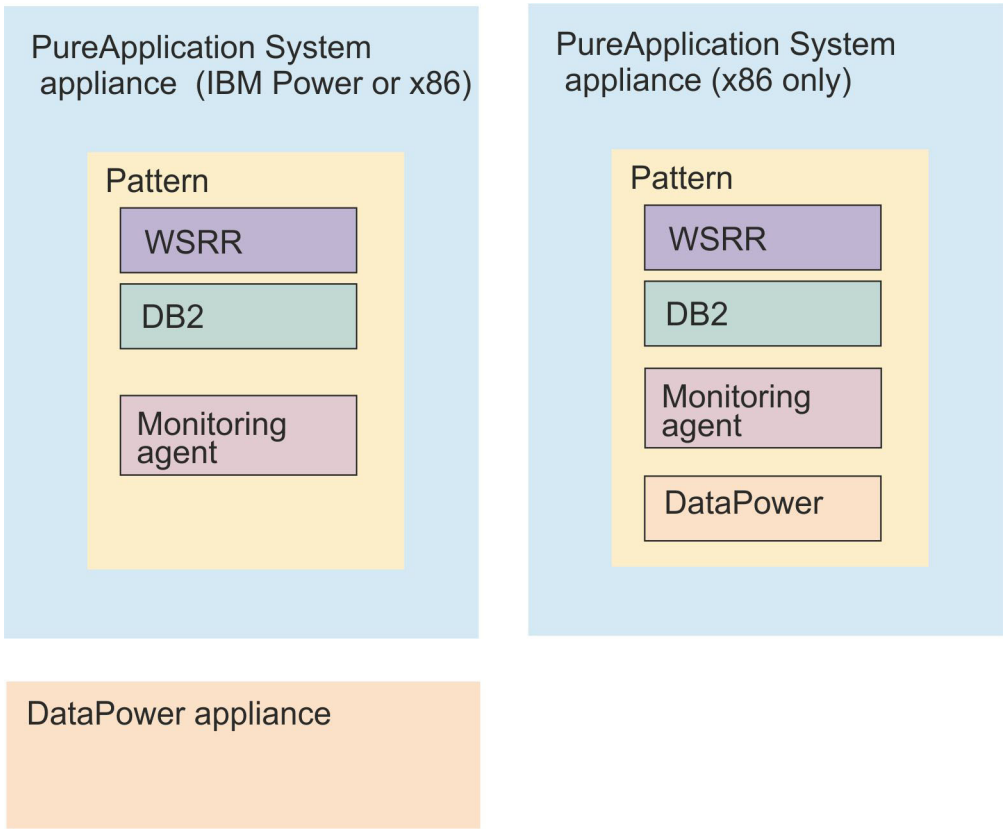
Capítulo 2. Visão Geral de Padrão

O IBM SOA Policy Gateway Pattern é um conjunto de padrões do sistema virtual que fornece um ponto de execução de política, um ponto de administração de política e um ponto de monitoramento de política.

É possível instalar o IBM SOA Policy Gateway Pattern em um dispositivo do IBM PureApplication System em um IBM Power ou em arquiteturas x86.

O ponto de administração de política é fornecido por padrões do sistema virtual que fornecem o WSRR em uma arquitetura multicamada, oferecendo um ambiente de produção e de temporariedade. O ponto de execução da política pode ser fornecido por um dispositivo do WebSphere DataPower. Ou então, em x86, o seu PureApplication System pode implementar uma imagem virtual do DataPower. Em qualquer um dos casos, um domínio é criado durante a implementação do padrão do sistema virtual. O ponto de monitoramento de política é fornecido por um complemento de monitoramento para o serviço de monitoramento do PureApplication System.

O diagrama a seguir ilustra os recursos que são derivados do IBM SOA Policy Gateway Pattern



Há exemplos de política em muitos, se não em todos os ambientes de Arquitetura Orientada a Serviços (SOA). Os produtores e consumidores de serviço concordam com os recursos, desempenho e características do serviço durante a fase de design.

Para implementar esses acordos, é possível usar Definições de Níveis de Serviço (SLDs) e Acordos de Nível de Serviço (SLAs). Use o padrão para definir políticas para SLDs e SLAs de uma maneira administrada, definida e controlada com eficiência. Os tipos de política que são usados neste padrão incluem as seguintes políticas:

- **Políticas de Mediação** -
  - Rejeição - Rejeita ou regula solicitações que chegam em uma taxa maior que a definida.
  - Registro - Cria uma mensagem de log com o ponto de execução de política quando um serviço é chamado.
  - Transformação.
  - Validação - Valida a chamada de serviço com relação à definição de serviço.
  - Roteamento - Com base na mensagem, roteia para um terminal específico.
- **Políticas de Segurança**: A amostra demonstra a execução de políticas de segurança de controle de acesso do XACML. Essas políticas não são controladas atualmente dentro do ponto de administração de política.
- **Políticas de Monitoramento**: É possível definir políticas de monitoramento em implementações do PureApplication System.

O IBM SOA Policy Gateway Pattern contém, os seguintes padrões do sistema virtual:

- SOA Policy Gateway Basic Runtime Sample (x86 apenas)
- SOA Policy Gateway Governance Master
- SOA Policy Gateway Basic Runtime
- SOA Policy Gateway Basic Runtime External DataPower
- SOA Policy Gateway Advanced Runtime
- SOA Policy Gateway Advanced Runtime External DataPower
- System Monitoring for SOA Policy Gateway Pattern 2.5 (um serviço compartilhado)

Os padrões do sistema virtual trabalham juntos para fornecer um ambiente de controle de serviços de vários estágios. O IBM SOA Policy Gateway Pattern fornece também o recurso de provisionar vários domínios do DataPower que são configurados para o ambiente de controle durante a implementação do padrão.

Para obter informações adicionais sobre Política SOA, consulte Capítulo 1, “Visão Geral de SOA Policy”, na página 1.

Conceitos relacionados:

Capítulo 1, “Visão Geral de SOA Policy”, na página 1
O gerenciamento de política desempenha uma função-chave no controle de políticas de uma forma estruturada e consistente. As políticas podem ser usadas para permitir melhor controle em qualquer ambiente orientado a serviços.

“SOA Policy Gateway Basic Runtime External DataPower” na página 23
O padrão SOA Policy Gateway Basic Runtime External DataPower é o mesmo que o padrão Tempo de Execução Básico, mas requer que os dispositivos DataPower externos sejam especificados na implementação.

“SOA Policy Gateway Basic Runtime Sample (x86)” na página 19
O SOA Policy Gateway Basic Runtime Sample provisiona um padrão de tempo de execução básico com uma interface de amostra e um aplicativo que demonstra as políticas que são atualmente suportadas nesta liberação.

"SOA Policy Gateway Governance Master" na página 21
O padrão SOA Policy Gateway Governance Master fornece um ambiente de controle em cluster para criar e gerenciar serviços e políticas. O ambiente é aprovisionado com o Perfil de Ativação de Controle padrão do WSRR configurado. O Perfil de Ativação de Controle padrão suporta dois destinos de promoção, Temporariedade e Produção.

"SOA Policy Gateway Advanced Runtime External DataPower" na página 26
O SOA Policy Gateway Advanced Runtime External DataPower é o mesmo que o padrão Tempo de Execução Avançado, mas requer que os dispositivos DataPower externos sejam especificados na implementação.

"System Monitoring for SOA Policy Gateway" na página 28
O serviço compartilhado System Monitoring for SOA Policy Gateway fornece os componentes de monitoramento para o SOA Policy Gateway.

Capítulo 3. Introdução ao IBM SOA Policy Gateway Pattern

Este padrão usa o WebSphere DataPower para controlar mensagens usando políticas controladas e definições de serviço no WSRR. Revise os tópicos nesta seção para entender como fazer o download e instalar o padrão, como verificar o padrão após a instalação, aceitar licenças e as funções de usuário envolvidas.

Fazendo Download e Instalando os Padrões

O IBM SOA Policy Gateway Pattern para uso com o IBM PureApplication System é compactado para download a partir do Passport Advantage.

Antes de Iniciar

Você faz download do IBM SOA Policy Gateway Pattern para um sistema provisório, que pode ser um sistema Linux ou Microsoft Windows. Em seguida, execute o instalador no sistema provisório para instalar os padrões no IBM PureApplication System.

Certifique-se de que haja 16 GB de espaço disponível para o arquivo `CIQ1LML.tar.gz` (Power de destino) ou o arquivo `CIQ1VML.tar.gz` (x86 de destino) e um extra de 40 GB para os arquivos extraídos. O Java™ Runtime Environment (JRE) Versão 6 também deve ser instalado antes de iniciar a instalação padrão. É possível fazer download do JRE para Linux dos seguintes endereços: http://www.ibm.com/developerworks/java/jdk/linux/download.html

Sobre Esta Tarefa

O IBM SOA Policy Gateway Pattern é compactado no arquivo `CIQ1LML.tar.gz` para um sistema Power de destino ou o arquivo `CIQ1VML.tar.gz` para um sistema x86 de destino. Esse archive contém os arquivos open virtual archive (OVA), arquivos de pacote de scripts e arquivos de definição de padrão.

Procedimento

Para fazer download das imagens do IBM SOA Policy Gateway Pattern a partir do Passport Advantage, conclua as etapas a seguir:

1. Acesse o website do Passport Advantage: Passport Advantage.
2. Faça download do archive que contém as imagens, os pacotes de scripts e os padrões a serem usados. O arquivo é chamado `CIQ1LML.tar.gz` (Power de destino) ou `CIQ1VML.tar.gz` (x86 de destino).
3. Abra um terminal no Linux ou uma janela de prompt de comandos no Windows e navegue até o diretório em que o archive foi transferido por download.
4. Extraia o conteúdo do archive em seu sistema de arquivos local. No Linux, o seguinte comando de extração é usado:

```
tar xvzf archive_file
```

   No Windows, use o software extra de extração de archive para extrair o conteúdo do archive.
5. Altere para o diretório `installer`:

```
cd installer
```

6. Para instalar o IBM SOA Policy Gateway Pattern no IBM PureApplication System, execute o instalador. O nome do comando é `installer.bat` no Microsoft Windows ou `installer` no Linux. Insira o seguinte comando: `installer -h <host> -u <username> -p <password>`, em que `<host>` é o IBM PureApplication System, e username e password são as credenciais do Administrador em Nuvem. Por exemplo:

```
./installer -h drivensnow.hillesden.ibm.com -u cbadmin -p cbadmin
```

7. Quando solicitado, aceite a licença do IBM SOA Policy Gateway Pattern.
   a. No Microsoft Windows: depois de aceitar o contrato de licença, se uma nova linha no terminal exibir `>>>`, digite `quit()` e pressione a tecla Enter. Repita a etapa 7.
8. Os padrões são importados. À medida que cada padrão é instalado, uma mensagem é exibida para indicar que ele foi instalado com êxito. Por exemplo:

```
Importando Padrão do "SOA Policy Gateway 2.5.0.0 - Controle Principal" ...
Importação do padrão "SOA Policy Gateway 2.5.0.0 - Controle Principal" bem-sucedida.
```

Resultados

Os padrões e scripts são carregados e os padrões de Sistema Virtual são criados.

Nota: Se existir um padrão de sistema virtual na versão correta que é usada no IBM SOA Policy Gateway Pattern no catálogo, ele não será sobrescrito.

O que Fazer Depois

Aceite licenças em IBM PureApplication System; consulte .

Para validar a instalação, consulte “Verificando o Padrão Instalado”.

Verificando o Padrão Instalado

É possível verificar se o padrão foi instalado com êxito.

Antes de Iniciar

Assegure-se de que todas as etapas de “Fazendo Download e Instalando os Padrões” na página 13 estejam concluídas.

Sobre Esta Tarefa

Depois de instalar o padrão, é possível verificar a instalação padrão para garantir que todas as partes tenham sido instaladas com êxito.

Procedimento

Para verificar a instalação do IBM SOA Policy Gateway Pattern, conclua as etapas a seguir:

1. Abra o Console de carga de trabalho no dispositivo em que o padrão foi instalado.
2. Verifique as Imagens Virtuais navegando para **Catálogo** > **Imagens Virtuais** e localize os seguintes itens:
   - DB2 Enterprise 10.1.0.2
   - WebSphere Service Registry and Repository 8.0.0.2

- WebSphere DataPower X152 Virtual Edition (apenas sistemas x86)

3. Navegue para **Catálogo** > **Pacotes de Scripts** e localize:
   - SOA Policy Gateway 2.5.0.0 - Domínio do DataPower
   - SOA Policy Gateway 2.5.0.0 - Monitoramento do DataPower (apenas x86)
   - SOA Policy Gateway 2.5.0.0 - Monitoramento do DataPower Externo
   - SOA Policy Gateway 2.5.0.0 - Promoção
   - SOA Policy Gateway 2.5.0.0 - Amostra (apenas x86)
   - SOA Policy Gateway 2.5.0.0 - Segurança
   - SOA Policy Gateway 2.5.0.0 - Add_Named_Queries
   - SOA Policy Gateway 2.5.0.0 - Derrubar

   Esses pacotes de scripts estão todos presentes em uma instalação bem-sucedida.
4. Navegue para **Padrões** > **Sistemas Virtuais**. Nos sistemas x86, localize:
   - SOA Policy Gateway 2.5.0.0 - Tempo de Execução Avançado
   - SOA Policy Gateway 2.5.0.0 - DataPower Externo de Tempo de Execução Avançado
   - SOA Policy Gateway 2.5.0.0 - Tempo de Execução Básico
   - SOA Policy Gateway 2.5.0.0 - DataPower Externo de Tempo de Execução Básico
   - SOA Policy Gateway 2.5.0.0 - Amostra de Tempo de Execução Básico
   - SOA Policy Gateway 2.5.0.0 - Controle Principal

   No Power Systems, localize:
   - SOA Policy Gateway 2.5.0.0 - Tempo de Execução Avançado
   - SOA Policy Gateway 2.5.0.0 - Tempo de Execução Básico
   - SOA Policy Gateway 2.5.0.0 - Controle Principal

   Esses padrões estão todos presentes em uma instalação bem-sucedida.
5. Navegue para **Nuvem** > **Tipos de Padrão** e localize o seguinte item:
   - System Monitoring for SOA Policy Gateway Pattern 2.5.0.0

   Este padrão está presente em uma instalação bem-sucedida.

Resultados

Você verificou a instalação do IBM SOA Policy Gateway Pattern.

O que Fazer Depois

Se você tiver uma instalação bem-sucedida, poderá prosseguir para aceitar licenças; consulte "Aceitando Licenças". Se sua instalação não foi bem-sucedida, repita a partir da etapa 7 do tópico "Fazendo Download e Instalando os Padrões" na página 13.

Aceitando Licenças

Você deve aceitar licenças para partes recém-instaladas para que possa trabalhar com os padrões.

Antes de Iniciar

Assegure-se de que todas as etapas de "Fazendo Download e Instalando os Padrões" na página 13 estejam concluídas.

Sobre Esta Tarefa

Para pode usar qualquer imagem virtual, você deve aceitar a licença necessária para ela.

Procedimento

Para aceitar licenças, conclua as seguintes etapas:

1. Abra o Console de carga de trabalho no dispositivo em que o padrão foi instalado.
2. Selecione **Catálogo** > **Imagens Virtuais**.
3. Localize as seguintes imagens na lista **Imagens Virtuais** e confirme se a licença foi aceita na área de janela de detalhes; caso contrário, clique em 'aceitar' para visualizar e aceitar a licença. Para sistemas x86:
   - WebSphere DataPower XI52 Virtual Edition, Versão 6.0.0.0 - Número de referência da imagem: XI52.6.0.0.0231528 (2013/06/16 14:14:19)
   - WebSphere Service Registry and Repository 8.0.0.2 - Número de referência da imagem: 201309062038
   - DB2 Enterprise 10.1.0.2 - Número de referência da imagem: 39
   - IBM OS Image for Red Hat Linux Systems, versão 2.0.0.3 - Número de referência da imagem: 136

   Para Power Systems:
   - WebSphere Service Registry and Repository 8.0.0.2 - Número de referência da imagem: 201309080001
   - DB2 Enterprise 10.1.0.2 - Número de referência da imagem: 50
   - IBM OS Image for AIX Systems version 2.0.0.2 - Número de referência da imagem: 126
4. Para aceitar uma licença, clique na imagem para visualizar seus detalhes. O status é exibido. Clique em **aceitar** para o Contrato de Licença e, em seguida, clique em quaisquer das licenças que devem ser aceitas para que a imagem virtual possa ser usada. O status exibe **Somente leitura** e o contrato de licença exibe **Aceito** quando concluído. Se uma licença não for aceita, o ícone da imagem conterá uma caixa vermelha com uma cruz.

Resultados

Você aceitou as licenças para o IBM SOA Policy Gateway Pattern.

O que Fazer Depois

Se você tiver uma instalação bem-sucedida e tiver aceitado todas as licenças, poderá trabalhar com o padrão; consulte Capítulo 5, “Trabalhando com o IBM SOA Policy Gateway Pattern”, na página 45. Se sua instalação não foi bem-sucedida, repita da etapa 7 em diante do tópico “Fazendo Download e Instalando os Padrões” na página 13.

Configurando o Acesso de Usuário

Para permitir que os usuários acessem as imagens e os padrões no dispositivo, o administrador do dispositivo deve primeiro permitir o acesso de usuário. É possível criar os usuários primeiro e incluí-los no grupo ou criar o grupo primeiro e, em seguida, criar os usuários e incluí-los no grupo.

Sobre Esta Tarefa

Os usuários administrativos, geralmente o administrador do dispositivo, podem incluir outros usuários para acessar e administrar os padrões. Eles fazem isso usando o console do sistema.

Procedimento

Para configurar o acesso de usuário, conclua as etapas a seguir:

1. Escolha uma das opções a seguir para configurar usuários e, opcionalmente, grupos de usuários:
   - Inclua e configure um usuário a partir da janela Usuários do console.
     a. No menu, clique em **Sistema** > **Usuários**.
     b. Clique no ícone **Incluir**.
     c. Forneça um nome abreviado, bem como o nome real do usuário, o endereço de email e as senhas, e clique em **OK**.
     d. Selecione o usuário que você incluiu no painel Usuários para configurar o acesso. Configure o acesso e as ações do usuário que você selecionou.
     e. Inclua o usuário em um ou mais grupos de usuários no campo **Grupos de Usuários**.
   - Criar um grupo de usuários.
     a. No menu, clique em **Sistema** > **Grupos de Usuários**.
     b. Clique no ícone **Incluir**. Forneça um nome e uma descrição para o grupo.
     c. Selecione o grupo que você incluiu no painel Grupos de Usuários para configurar o acesso.
     d. Inclua os membros no campo **Membros do Grupo** e forneça as permissões para aplicar ao grupo.
2. Opcional: Se você já incluiu as imagens virtuais, forneça acesso aos usuários ou ao grupo para as imagens virtuais. Alterne para o console de carga de trabalho e clique em **Padrões** > **Sistemas Virtuais** para abrir a janela Padrões do sistema virtual. Selecione uma imagem virtual do IBM SOA Policy Gateway Pattern para exibir seus detalhes. Inclua os usuários ou o grupo no campo **Acesso concedido**.

O que Fazer Depois

Se você ainda não tiver incluído as imagens virtuais, inclua-as e, em seguida, forneça aos usuários ou ao grupo acesso a elas.

Informações relacionadas:

IBM PureApplication System: Gerenciando Usuários e Grupos

Capítulo 4. Padrões, Partes e Pacotes de Scripts

Um padrão fornece uma definição de topologia para implementação repetida que pode ser compartilhada. As partes do IBM SOA Policy Gateway Pattern são os componentes funcionais do padrão. Cada parte representa uma única máquina virtual.

Os padrões descrevem a função que é fornecida por cada máquina virtual em um sistema virtual. Cada função é identificada como uma parte no padrão. Os padrões herdam as características de suas partes associadas. Por exemplo, quando uma parte do WSRR é colocada em um padrão, que é, então, implementado, o resultado é uma máquina virtual que possui uma instância do WSRR em execução.

Padrões

Quando as imagens virtuais são carregadas no IBM PureApplication System e o acesso é designado aos usuários, eles podem começar a trabalhar com os padrões.

Os padrões fornecem uma topologia repetida que pode ser implementada em uma nuvem. Padrões implementados são sistemas virtuais que são executados na nuvem. Os padrões, quer sejam predefinidos ou criados, contêm partes. Algumas partes são necessárias para que o padrão funcione quando implementado na nuvem como um sistema virtual.

SOA Policy Gateway Basic Runtime Sample (x86)

O SOA Policy Gateway Basic Runtime Sample provisiona um padrão de tempo de execução básico com uma interface de amostra e um aplicativo que demonstra as políticas que são atualmente suportadas nesta liberação.

O padrão SOA Policy Gateway Basic Runtime Sample está disponível apenas em sistemas x86.

O padrão SOA Policy Gateway Basic Runtime Sample possui as partes a seguir:

- Servidor Independente do WSRR
- DB2 Enterprise
- DataPower

O padrão SOA Policy Gateway Basic Runtime Sample instala um aplicativo de amostra no ambiente implementado. O padrão instala um domínio de amostra no DataPower que implementa um serviço de amostra, instala o WSDL de amostra e políticas anexadas no WSRR para o serviço, e fornece um aplicativo de teste para demonstrar as políticas forçadas. Para obter informações adicionais sobre o aplicativo de amostra, consulte “O Aplicativo de Amostra” na página 58. Ele instala um domínio de amostra no DataPower, instala o WSDL e Políticas de amostra no WSRR, e demonstra várias políticas com relação a um serviço.

O diagrama a seguir mostra a amostra de tempo de execução básico.

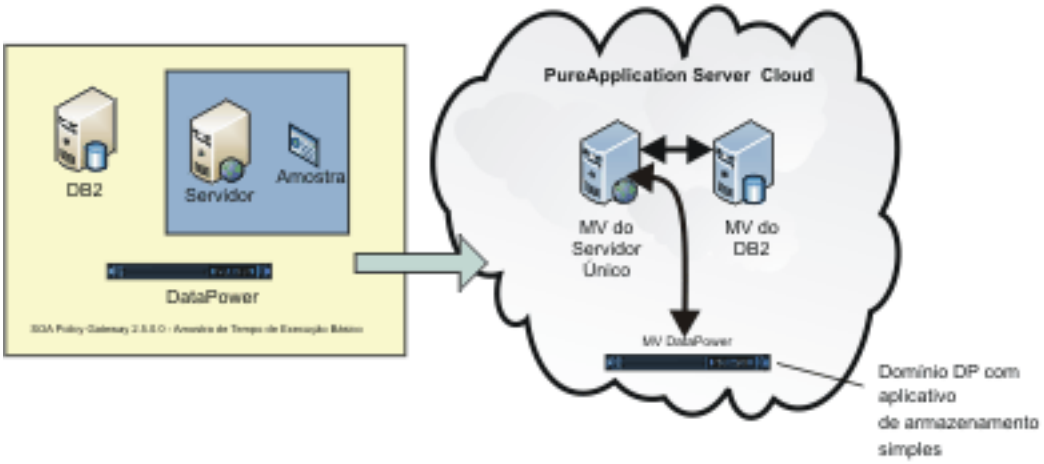


Figura 5. Configuração do Servidor PureApplication com VM DataPower (Apenas x86)

As políticas que são implementadas incluem:

Tabela 1. Políticas Inclusas no Basic Runtime com Padrão Sample

Tipo de política	**Descrição**
Criação de log	Com base em um ID de contexto de solicitações, registra a solicitação no DataPower.
Roteamento	Com base em um ID de contexto de solicitações, roteia a solicitação para um terminal especificado.
Validação	Valida a solicitação com relação ao WSDL de implementações de serviço.
Rejeição	Controla solicitações para um serviço com base na contagem de mensagens com as ações: rejeitar, enfileirar e outras.
Segurança AAA	Controla o acesso ao serviço usando autorização de usuário baseada em XACML. O XACML não é armazenado no WSRR.
Edição de Dados de Segurança	Edita os dados de partes da mensagem de resposta que é baseada em XACML. O XACML não é armazenado no WSRR.

Scripts e Opções Avançadas

O padrão requer os scripts a seguir.

Na parte do Servidor Independente do WSRR:
- SOA Policy Gateway 2.5.0.0 - Amostra

Visualize a parte e os parâmetros de script:
- “Parte do DB2 Enterprise” na página 29
- “Parte do Servidor Independente do WSRR” na página 35
- “Parte do DataPower” na página 37
- “Script: SOA Policy Gateway 2.5.0.0 - Amostra” na página 40

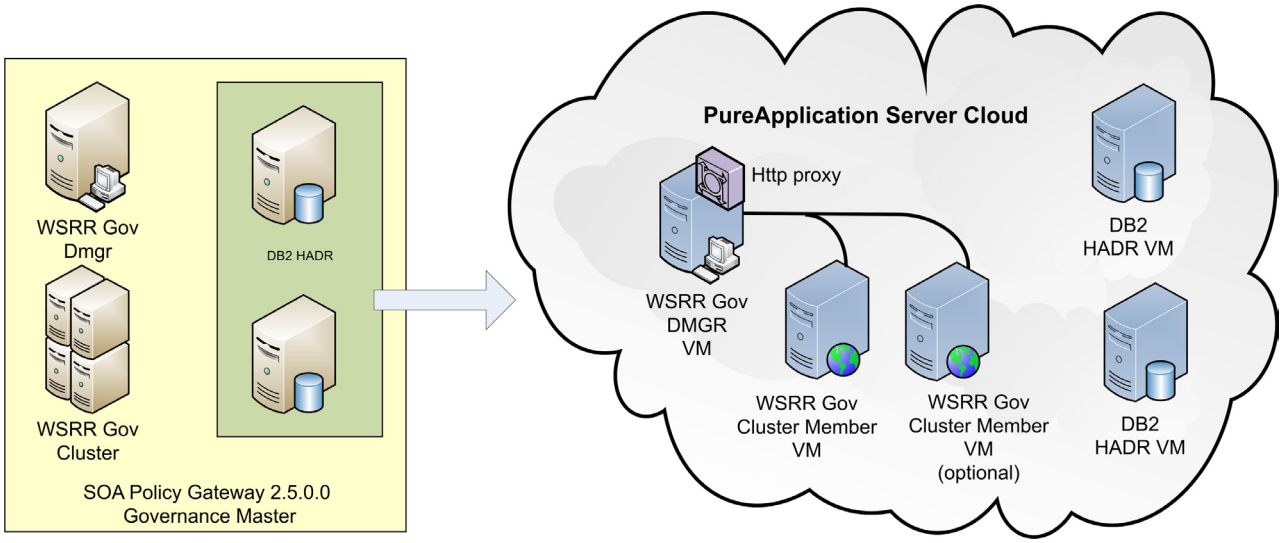
SOA Policy Gateway Governance Master

O padrão SOA Policy Gateway Governance Master fornece um ambiente de controle em cluster para criar e gerenciar serviços e políticas. O ambiente é aprovisionado com o Perfil de Ativação de Controle padrão do WSRR configurado. O Perfil de Ativação de Controle padrão suporta dois destinos de promoção, Temporariedade e Produção.

O padrão SOA Policy Gateway Governance Master requer as partes a seguir:

- HADR Primário do DB2
- HADR de Espera do DB2
- Gerenciador de Implementação do WSRR
- Nós Customizados do WSRR

Nota: O padrão de Controle Principal deve ser implementado antes de os padrões de tempo de execução serem implementados. Os parâmetros que são usados para configurar o padrão de Controle Principal são usados pelos padrões de tempo de execução para configurar ele próprio com o Controle Principal.



Parâmetros da Parte

Visualize os parâmetros da parte:

- “Parte de HADR Primário do DB2 Enterprise” na página 31
- “Parte de HADR de Espera do DB2 Enterprise” na página 33
- “Parte do Gerenciador de Implementação do WSRR” na página 36
- “Parte de Nós Customizados do WSRR” na página 36
- “Script: SOA Policy Gateway 2.5.0.0 - Segurança” na página 42
- “Script: SOA Policy Gateway 2.5.0.0 - Promoção” na página 39

Usando o Padrão Governance como um Controle Principal

O padrão SOA Policy Gateway Governance Master é implementado com o Perfil de Ativação de Controle do WSRR padrão que inclui dois estágios de promoção, Temporariedade e Produção. Para obter informações adicionais sobre o Perfil de Ativação de Controle no WSRR, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Governance Enablement

Profile. Os padrões de tempo de execução básico ou de tempo de execução avançado podem ser implementados nesta integração como destinos de promoção. Para obter informações adicionais sobre como configurar destinos de promoção, consulte “Incluindo um Ambiente de Tempo de Execução Adicional” na página 55.

Informações relacionadas:

Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Governance Enablement Profile

SOA Policy Gateway Basic Runtime

O padrão SOA Policy Gateway Basic Runtime é o meio mais simples de fornecer um tempo de execução SOA Policy Gateway; ele inclui duas instâncias DataPower (x86 apenas), uma instância WSRR independente, uma instância DB2 independente e uma instância do SO Base (para hospedagem dos agentes de monitoramento do DataPower).

Nota: Este tópico descreve o padrão disponível em x86. Para o padrão do IBM Power, consulte “SOA Policy Gateway Basic Runtime External DataPower” na página 23.

O padrão SOA Policy Gateway Basic Runtime requer as partes a seguir:

- Servidor Independente do WSRR
- DB2 Enterprise
- WebSphere DataPower X152 Virtual Edition
- Monitoramento SOA para DataPower (em uma parte principal do SO)

O diagrama a seguir mostra a configuração do padrão SOA Policy Gateway Basic Runtime.

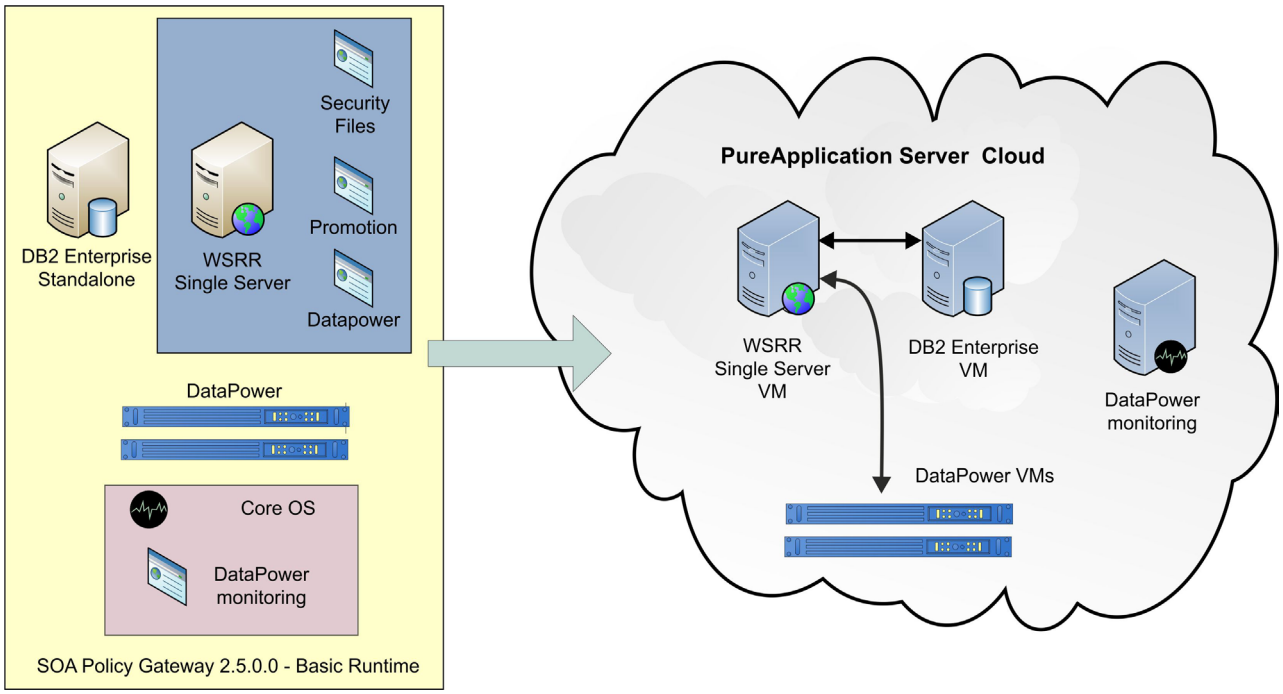


Figura 6. Configuração do Servidor PureApplication com VM DataPower

Scripts e Opções Avançadas

O padrão requer entrada do usuário para os scripts a seguir no momento da implementação.

Na parte do Servidor Independente do WSRR:
- SOA Policy Gateway 2.5.0.0 - Segurança
- SOA Policy Gateway 2.5.0.0 - Promoção
- SOA Policy Gateway 2.5.0.0 - Domínio do DataPower

Na parte principal do SO:
- SOA Policy Gateway 2.5.0.0 - Monitoramento do DataPower

Visualize a parte e os parâmetros de script:
- "Parte do Servidor Independente do WSRR" na página 35
- "Parte do DB2 Enterprise" na página 29
- "Parte do DataPower" na página 37
- "Script: SOA Policy Gateway 2.5.0.0 - Segurança" na página 42
- "Script: SOA Policy Gateway 2.5.0.0 - Promoção" na página 39
- "Script: SOA Policy Gateway 2.5.0.0 - Domínio do DataPower" na página 38
- "Script: SOA Policy Gateway 2.5.0.0 - Monitoramento do DataPower (apenas x86)" na página 42

Configurando o Tempo de Execução Básico com um Controle Principal

Quando um padrão de tempo de execução básico estiver configurado com um padrão de Controle Principal, ocorrerá o seguinte:
- A segurança de célula cruzada é configurada
- O arquivo `promotion.xml` no Controle Principal é atualizado com os dados da implementação para a implementação do tempo de execução básico.

Para configurar a promoção, você deve escolher uma das opções de estágio a seguir:
- produção
- temporariedade

Essas opções são alinhadas com os níveis fornecidos pelo Perfil de Ativação de Controle no WSRR. Para obter informações adicionais sobre o Perfil de Ativação de Controle no WSRR, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Governance Enablement Profile.

Nota: É possível usar esse padrão para provisionar um sistema independente, sem Controle Principal. Para fazer isso, especifique os parâmetros do Controle Principal como "Desconfigurado" ao implementar o padrão. Essas configurações farão com que o script de promoção gere um erro durante a implementação e a implementação será mostrada como **com falha**, mas você poderá ignorar o erro.

SOA Policy Gateway Basic Runtime External DataPower

O padrão SOA Policy Gateway Basic Runtime External DataPower é o mesmo que o padrão Tempo de Execução Básico, mas requer que os dispositivos DataPower externos sejam especificados na implementação.

Nota: Essa descrição é aplicável ao padrão nos sistemas IBM Power.

O padrão SOA Policy Gateway Basic Runtime External DataPower possui as partes a seguir:

- Servidor Independente do WSRR
- DB2 Enterprise
- Monitoramento SOA para DataPower (em uma parte principal do SO)

O diagrama a seguir mostra a configuração do padrão SOA Policy Gateway Basic Runtime External DataPower.

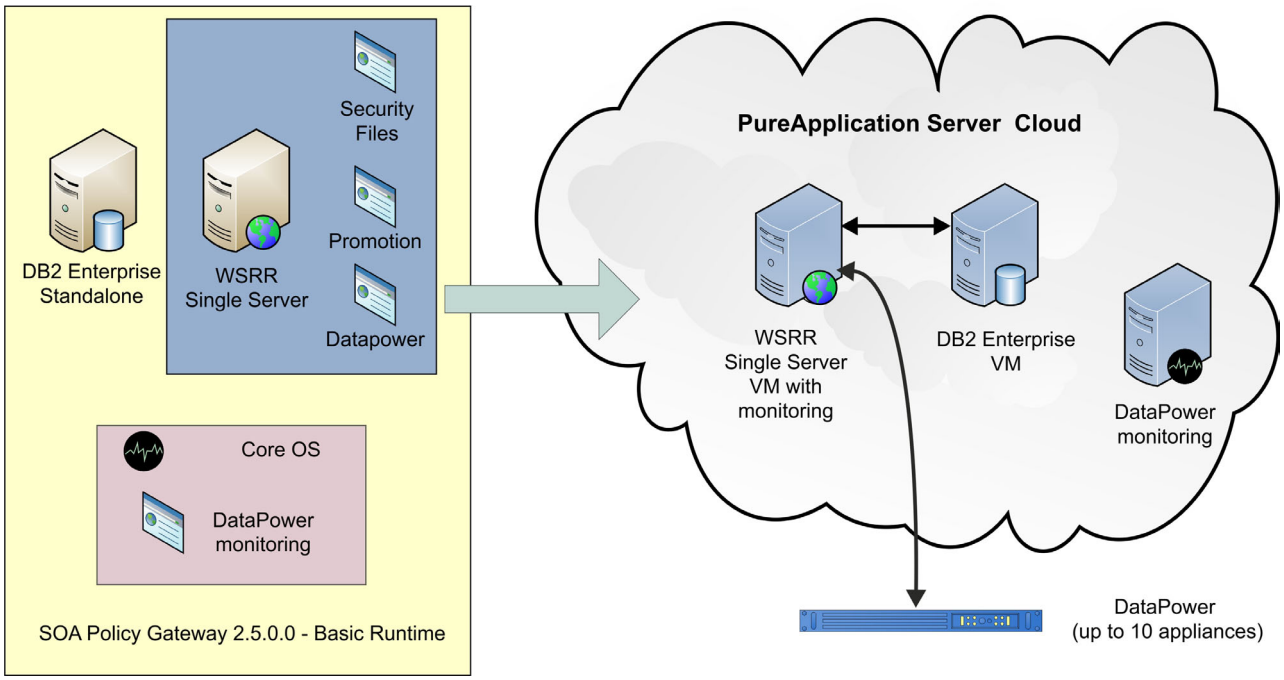


Figura 7. Configuração do Servidor PureApplication com o Dispositivo DataPower

Scripts e Opções Avançadas

O padrão requer entrada do usuário para os scripts a seguir no momento da implementação.

Na parte do Servidor Independente do WSRR:

- SOA Policy Gateway 2.5.0.0 - Segurança
- SOA Policy Gateway 2.5.0.0 - Promoção
- SOA Policy Gateway 2.5.0.0 - Domínio do DataPower

Na parte principal do SO:

- SOA Policy Gateway 2.5.0.0 - Monitoramento do DataPower

Visualize a parte e os parâmetros de script:

- “Parte do Servidor Independente do WSRR” na página 35
- “Parte do DB2 Enterprise” na página 29
- “Script: SOA Policy Gateway 2.5.0.0 - Segurança” na página 42

- "Script: SOA Policy Gateway 2.5.0.0 - Promoção" na página 39
- "Script: SOA Policy Gateway 2.5.0.0 - Domínio do DataPower" na página 38
- "Script: SOA Policy Gateway 2.5.0.0 - Monitoramento do DataPower (apenas x86)" na página 42

Configurando o Tempo de Execução Básico com um Controle Principal

Quando um padrão de tempo de execução básico estiver configurado com um padrão de Controle Principal, ocorrerá o seguinte:

- A segurança de célula cruzada é configurada
- O arquivo `promotion.xml` no Controle Principal é atualizado com os dados da implementação para a implementação do tempo de execução básico.

Para configurar a promoção, você deve escolher uma das opções de estágio a seguir:

- produção
- temporariedade

Essas opções são alinhadas com os níveis fornecidos pelo Perfil de Ativação de Controle no WSRR. Se o perfil de controle for diferente, "outro" será escolhido quando o perfil de controle Controles Principais for alterado. Para obter informações adicionais sobre o Perfil de Ativação de Controle no WSRR, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Governance Enablement Profile.

Nota: É possível usar esse padrão para provisionar um sistema independente, sem Controle Principal. Para fazer isso, especifique os parâmetros do Controle Principal como "Desconfigurado" ao implementar o padrão. Essas configurações farão com que o script de promoção gere um erro durante a implementação e a implementação será mostrada como **com falha**, mas você poderá ignorar o erro.

SOA Policy Gateway Advanced Runtime

O SOA Policy Gateway Advanced Runtime inclui duas instâncias do servidor DB2 em uma configuração de HADR e um cluster do WSRR com um único Deployment Manager e dois Nós Customizados.

Nota: Este tópico descreve o padrão disponível em x86. Para o padrão do IBM Power, consulte "SOA Policy Gateway Advanced Runtime External DataPower" na página 26.

O padrão requer as partes a seguir:

- Gerenciador de Implementação do WSRR
- Nós Customizados do WSRR
- HADR Primário do DB2
- HADR de Espera do DB2
- WebSphere DataPower X152 Virtual Edition
- Monitoramento SOA para DataPower (em uma parte principal do SO)

O diagrama a seguir mostra a configuração de um sistema de tempo de execução avançado.

Figura 8. Configuração do Servidor PureApplication com VMs DataPower

Scripts e Opções Avançadas

O padrão requer entrada do usuário para os seguintes scripts no momento da implementação:

Na parte do Deployment Manager do WSRR:
- SOA Policy Gateway 2.5.0.0 - Segurança
- SOA Policy Gateway 2.5.0.0 - Promoção
- SOA Policy Gateway 2.5.0.0 - Domínio do DataPower

Na parte principal do SO:
- SOA Policy Gateway 2.5.0.0 - Monitoramento do DataPower

Visualize a parte e os parâmetros de script:
- "Parte de HADR Primário do DB2 Enterprise" na página 31
- "Parte de HADR de Espera do DB2 Enterprise" na página 33
- "Parte do Gerenciador de Implementação do WSRR" na página 36
- "Parte de Nós Customizados do WSRR" na página 36
- "Script: SOA Policy Gateway 2.5.0.0 - Promoção" na página 39
- "Script: SOA Policy Gateway 2.5.0.0 - Domínio do DataPower" na página 38
- "Script: SOA Policy Gateway 2.5.0.0 - Monitoramento do DataPower (apenas x86)" na página 42

Configurando o Tempo de Execução Avançado com um Controle Principal

Quando um padrão de tempo de execução avançado estiver configurado com um padrão de Controle Principal, poderão ocorrer as ações a seguir:
- A segurança de célula cruzada é configurada
- O arquivo `promotion.xml` no Controle Principal é atualizado com os dados da implementação do tempo de execução avançado.

Para configurar a promoção, você deve escolher uma das opções de estágio a seguir:
- produção
- temporariedade

Essas opções são alinhadas com os níveis fornecidos pelo Perfil de Ativação de Controle no WSRR. Para obter informações adicionais sobre o Perfil de Ativação de Controle no WSRR, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Governance Enablement Profile.

SOA Policy Gateway Advanced Runtime External DataPower

O SOA Policy Gateway Advanced Runtime External DataPower é o mesmo que o padrão Tempo de Execução Avançado, mas requer que os dispositivos DataPower externos sejam especificados na implementação.

Nota: Essa descrição é aplicável ao padrão SOA Policy Gateway Advanced Runtime nos sistemas IBM Power.

O padrão SOA Policy Gateway Advanced Runtime External DataPower requer as partes a seguir:

- Gerenciador de Implementação do WSRR
- Nós Customizados do WSRR
- HADR Primário do DB2
- HADR de Espera do DB2
- Monitoramento SOA para DataPower (em uma parte principal do SO)

O diagrama a seguir mostra a configuração de um sistema de tempo de execução avançado.

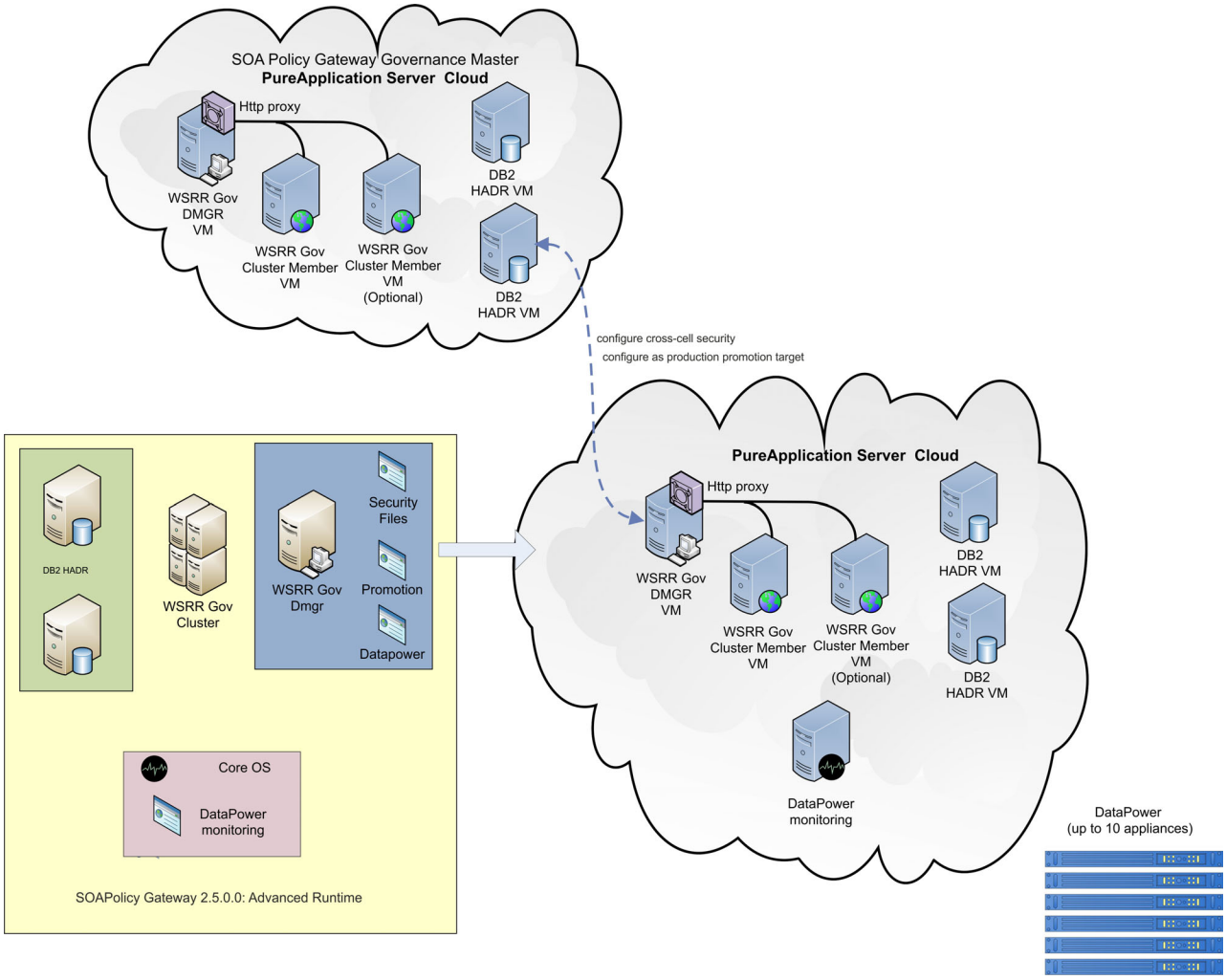


Figura 9. Configuração do Servidor PureApplication com Dispositivos DataPower

Scripts e Opções Avançadas

O padrão requer entrada do usuário para os scripts a seguir no momento da implementação.

Na parte do Deployment Manager do WSRR:

- SOA Policy Gateway 2.5.0.0 - Segurança
- SOA Policy Gateway 2.5.0.0 - Promoção

- SOA Policy Gateway 2.5.0.0 - Domínio do DataPower

Na parte principal do SO:
- SOA Policy Gateway 2.5.0.0 - Monitoramento do DataPower

Visualize a parte e os parâmetros de script:
- "Parte de HADR Primário do DB2 Enterprise" na página 31
- "Parte de HADR de Espera do DB2 Enterprise" na página 33
- "Parte do Gerenciador de Implementação do WSRR" na página 36
- "Parte de Nós Customizados do WSRR" na página 36
- "Script: SOA Policy Gateway 2.5.0.0 - Promoção" na página 39
- "Script: SOA Policy Gateway 2.5.0.0 - Domínio do DataPower" na página 38
- "Script: SOA Policy Gateway 2.5.0.0 - Monitoramento do DataPower (apenas x86)" na página 42

Configurando o Tempo de Execução Avançado com um Controle Principal

Quando um padrão de tempo de execução avançado estiver configurado com um padrão de Controle Principal, ocorrerá o seguinte:
- A segurança de célula cruzada é configurada
- O arquivo `promotion.xml` no Controle Principal é atualizado com os dados da implementação do Tempo de Execução Avançado.

Para configurar a promoção, você deve escolher uma das opções de estágio a seguir:
- produção
- temporariedade

Essas opções são alinhadas com os níveis fornecidos pelo Perfil de Ativação de Controle no WSRR. Para obter informações adicionais sobre o Perfil de Ativação de Controle no WSRR, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Governance Enablement Profile.

Serviço Compartilhado

O padrão inclui um serviço compartilhado que é usado por padrões implementados para fornecer monitoramento.

System Monitoring for SOA Policy Gateway

O serviço compartilhado System Monitoring for SOA Policy Gateway fornece os componentes de monitoramento para o SOA Policy Gateway.

O monitoramento nos padrões de tempo de execução básico e avançado é fornecido pelo serviço de monitoramento do DataPower em execução na parte principal do SO. O próprio serviço de monitoramento usa os componentes do ITCAM for SOA que estão contidos no Padrão System Monitoring for SOA Policy Gateway. O monitoramento das instâncias do WSRR também requer que o serviço compartilhado System Monitoring for WebSphere Application Server esteja em execução.

Siga o link relacionado para obter a documentação detalhada do ITCAM for SOA.

Informações relacionadas:

Documentação do ITCAM for SOA 7.2.1 (do Fix Central)

Partes

As partes a seguir constituem o IBM SOA Policy Gateway Pattern.

Parte do DB2 Enterprise

A parte do DB2 Enterprise fornece algumas opções de configuração.

Os parâmetros configuráveis da imagem do sistema virtual do DB2 Enterprise 10.1.0.2 são descritos na tabela a seguir:

Tabela 2. Parâmetros Configuráveis

Nome do parâmetro	Valor padrão	Descrição
CPUs virtuais	1	O número de processadores virtuais que estão alocados para a máquina virtual que é representada por essa parte.
Tamanho da memória (MB)	2048	A quantidade de memória que está alocada para essa máquina virtual, em megabytes.
Grupo de proprietários da instância	db2iadm1	O grupo ao qual pertence o proprietário da instância do DB2.
Proprietário da instância	db2inst1	O ID do proprietário da instância do DB2. Esse ID do usuário é usado como o proprietário da instalação da instância do DB2 e como o proprietário dos bancos de dados e dos esquemas.
Senha (Proprietário da instância)	password	A senha para o ID do usuário db2inst1 do sistema operacional.
Verificar senha	password	Verifica a senha do proprietário da instância.
Grupo de usuários protegidos	db2fadm1	O grupo ao qual pertence o proprietário protegido do DB2.
Usuário protegido	db2fenc1	O ID do usuário protegido do DB2. O ID do usuário protegido é usado para executar funções definidas pelo usuário (UDFs) e procedimentos armazenados fora do espaço de endereço que é usado pelo banco de dados DB2. O usuário protegido é um usuário sob o qual os procedimentos armazenados "protegidos" podem ser executados com autoridade reduzida do sistema operacional.
Senha (db2fenc1)		A senha para o ID do usuário protegido
Verificar senha		Verifica a senha do usuário protegido.

Tabela 2. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Valor padrão	Descrição
Grupo de usuários DAS	dasadm1	O grupo ao qual pertence o proprietário DAS do DB2.
Usuário DAS	dasusr1	O ID do usuário para o usuário do servidor de administração do DB2 que é usado para executar o servidor de administração do DB2 em seu sistema. O ID do usuário também é usado pelas ferramentas da GUI do DB2 para executar tarefas de administração com relação a bancos de dados e instâncias de bancos de dados do servidor local.
Senha (usuário DAS)	password	A senha para o usuário DAS.
Verificar senha	password	Verifica a senha do dasusr1.
Porta de Serviço do DB2	50000	A porta está bloqueada e não pode ser alterada.
Criação do banco de dados	Create-new-database	Esse valor está bloqueado e não pode ser alterado.
Nome do novo banco de dados	WSRR	Esse valor está bloqueado e não pode ser alterado.
Conjunto de códigos para o novo banco de dados	UTF-8	
Território para o novo banco de dados	US	
Ordenação para o novo banco de dados	SYSTEM	
Tamanho da página para o novo banco de dados	32768	Esse valor está bloqueado e não pode ser alterado.
Modo de compatibilidade do DB2	Padrão	Esse valor está bloqueado e não pode ser alterado.
Configurar todos os discos brutos para uso pelo DB2	NO	
Senha (raiz)		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual que é representada por essa parte no padrão.
Verificar senha		Verifica a senha raiz.
Senha (virtuser)		A senha para o ID do usuário virtuser do sistema operacional. Esse ID do usuário é usado como um ID de usuário não raiz para a máquina virtual.
Verificar senha		Verifica a senha do virtuser.
Ativar VNC	True	Esse valor está bloqueado e não pode ser alterado.

Parte de HADR Primário do DB2 Enterprise

A parte de HADR Primário do DB2 Enterprise fornece algumas opções de configuração.

Os parâmetros configuráveis da parte de HADR Primário do DB2 Enterprise são descritos na tabela a seguir:

Tabela 3. Parâmetros Configuráveis

Nome do parâmetro	Valor padrão	Descrição
CPUs virtuais	1	O número de processadores virtuais que estão alocados para a máquina virtual que é representada por essa parte.
Tamanho da memória (MB)	2048	A quantidade de memória que está alocada para essa máquina virtual, em megabytes.
Grupo de proprietários da instância	db2iadm1	O grupo ao qual pertence o proprietário da instância do DB2.
Proprietário da instância	db2inst1	O ID do proprietário da instância do DB2. Esse ID do usuário é usado como o proprietário da instalação da instância do DB2 e como o proprietário dos bancos de dados e dos esquemas.
Senha (Proprietário da instância)	password	A senha para o ID do usuário db2inst1 do sistema operacional.
Verificar senha	password	Verifica a senha do proprietário da instância.
Grupo de usuários protegidos	db2fadm1	O grupo ao qual pertence o proprietário protegido do DB2.
Usuário protegido	db2fenc1	O ID do usuário protegido do DB2. O ID do usuário protegido é usado para executar funções definidas pelo usuário (UDFs) e procedimentos armazenados fora do espaço de endereço que é usado pelo banco de dados DB2. O usuário protegido é um usuário sob o qual os procedimentos armazenados "protegidos" podem ser executados com autoridade reduzida do sistema operacional.
Senha (db2fenc1)		A senha para o ID do usuário protegido
Verificar senha		Verifica a senha do usuário protegido.
Grupo de usuários DAS	dasadm1	O grupo ao qual pertence o proprietário DAS do DB2.

Tabela 3. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Valor padrão	Descrição
Usuário DAS	dasusr1	O ID do usuário para o usuário do servidor de administração do DB2 que é usado para executar o servidor de administração do DB2 em seu sistema. O ID do usuário também é usado pelas ferramentas da GUI do DB2 para executar tarefas de administração com relação a bancos de dados e instâncias de bancos de dados do servidor local.
Senha (usuário DAS)	password	A senha para o usuário DAS.
Verificar senha	password	Verifica a senha do dasusr1.
Porta de Serviço do DB2	50000	A porta está bloqueada e não pode ser alterada.
Criação do banco de dados	Create-new-database	Esse valor está bloqueado e não pode ser alterado.
Nome do novo banco de dados	WSRR	Esse valor está bloqueado e não pode ser alterado.
Conjunto de códigos para o novo banco de dados	UTF-8	
Território para o novo banco de dados	US	
Ordenação para o novo banco de dados	SYSTEM	
Tamanho da página para o novo banco de dados	32768	Esse valor está bloqueado e não pode ser alterado.
Modo de compatibilidade do DB2	Padrão	Esse valor está bloqueado e não pode ser alterado.
Configurar todos os discos brutos para uso pelo DB2	NO	
Senha (raiz)		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual que é representada por essa parte no padrão.
Verificar senha		Verifica a senha raiz.
Senha (virtuser)		A senha para o ID do usuário virtuser do sistema operacional. Esse ID do usuário é usado como um ID de usuário não raiz para a máquina virtual.
Verificar senha		Verifica a senha do virtuser.
Ativar VNC	True	Esse valor está bloqueado e não pode ser alterado.

Outros parâmetros são herdados do padrão de sistema virtual base e são bloqueados.

Parte de HADR de Espera do DB2 Enterprise

A parte de HADR de Espera do DB2 Enterprise fornece algumas opções de configuração.

Tabela 4. Parâmetros Configuráveis

Nome do parâmetro	Valor padrão	Descrição
CPUs virtuais	1	O número de processadores virtuais que estão alocados para a máquina virtual que é representada por essa parte.
Tamanho da memória (MB)	2048	A quantidade de memória que está alocada para essa máquina virtual, em megabytes.
Grupo de proprietários da instância	db2iadm1	O grupo ao qual pertence o proprietário da instância do DB2.
Proprietário da instância	db2inst1	O ID do proprietário da instância do DB2. Esse ID do usuário é usado como o proprietário da instalação da instância do DB2 e como o proprietário dos bancos de dados e dos esquemas.
Senha (Proprietário da instância)	password	A senha para o ID do usuário db2inst1 do sistema operacional.
Verificar senha	password	Verifica a senha do proprietário da instância.
Grupo de usuários protegidos	db2fadm1	O grupo ao qual pertence o proprietário protegido do DB2.
Usuário protegido	db2fenc1	O ID do usuário protegido do DB2. O ID do usuário protegido é usado para executar funções definidas pelo usuário (UDFs) e procedimentos armazenados fora do espaço de endereço que é usado pelo banco de dados DB2. O usuário protegido é um usuário sob o qual os procedimentos armazenados "protegidos" podem ser executados com autoridade reduzida do sistema operacional.
Senha (db2fenc1)		A senha para o ID do usuário protegido
Verificar senha		Verifica a senha do usuário protegido.
Grupo de usuários DAS	dasadm1	O grupo ao qual pertence o proprietário DAS do DB2.

Tabela 4. Parâmetros Configuráveis (continuação)

Nome do parâmetro	Valor padrão	Descrição
Usuário DAS	dasusr1	O ID do usuário para o usuário do servidor de administração do DB2 que é usado para executar o servidor de administração do DB2 em seu sistema. O ID do usuário também é usado pelas ferramentas da GUI do DB2 para executar tarefas de administração com relação a bancos de dados e instâncias de bancos de dados do servidor local.
Senha (usuário DAS)	password	A senha para o usuário DAS.
Verificar senha	password	Verifica a senha do dasusr1.
Porta de Serviço do DB2	50000	A porta está bloqueada e não pode ser alterada.
Criação do banco de dados	Create-new-database	Esse valor está bloqueado e não pode ser alterado.
Nome do novo banco de dados	WSRR	Esse valor está bloqueado e não pode ser alterado.
Conjunto de códigos para o novo banco de dados	UTF-8	
Território para o novo banco de dados	US	
Ordenação para o novo banco de dados	SYSTEM	
Tamanho da página para o novo banco de dados	32768	Esse valor está bloqueado e não pode ser alterado.
Modo de compatibilidade do DB2	Padrão	Esse valor está bloqueado e não pode ser alterado.
Configurar todos os discos brutos para uso pelo DB2	NO	
Senha (raiz)		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual que é representada por essa parte no padrão.
Verificar senha		Verifica a senha raiz.
Senha (virtuser)		A senha para o ID do usuário virtuser do sistema operacional. Esse ID do usuário é usado como um ID de usuário não raiz para a máquina virtual.
Verificar senha		Verifica a senha do virtuser.
Ativar VNC	True	Esse valor está bloqueado e não pode ser alterado.

Outros parâmetros são herdados do padrão de sistema virtual base e são bloqueados.

Parte do Servidor Independente do WSRR

A parte do Servidor Independente do WSRR fornece algumas opções de configuração.

Os parâmetros configuráveis da parte do Servidor Independente do WSRR são descritos na tabela a seguir:

Tabela 5. Parâmetros Configurados

Nome do parâmetro	Valor padrão	Descrição
CPUs virtuais	1	O número de processadores virtuais que estão alocados para a máquina virtual que é representada por essa parte.
Tamanho da memória (MB)	4096	A quantidade de memória que está alocada para essa máquina virtual, em megabytes.
Nome da célula	Configure como um dos valores a seguir: • SOAPolicySampleCell (padrão de amostra de tempo de execução básico) • SOAPolicyBasicCell (padrão de tempo de execução básico) • SOAPolicyBasicCell (padrão do DataPower externo do tempo de execução básico)	
Nome do Nó	Configure como um dos valores a seguir: • SOAPolicySampleNode (padrão de amostra de tempo de execução básico) • SOAPolicyBasicNode (padrão de tempo de execução básico) • SOAPolicyBasicNode (padrão do DataPower externo do tempo de execução básico)	
Senha (raiz)		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual que é representada por essa parte no padrão.
Verificar senha		Verifica a entrada do usuário para Senha (raiz).
Nome de usuário administrativo do WebSphere	virtuser	O nome do usuário administrativo do WebSphere Application Server. Você não deve alterar esse valor.
Senha administrativa do WebSphere		A senha do usuário administrativo do WebSphere Application Server.
Verificar senha		Verifica a entrada do usuário para a senha administrativa do WebSphere Application Server.
Ativar VNC	True	Esse valor está bloqueado e não pode ser alterado.

Parte do Gerenciador de Implementação do WSRR

A parte do Gerenciador de Implementação do WSRR fornece algumas opções de configuração.

Os parâmetros configuráveis da parte do Gerenciador de Implementação do WSRR são descritos na tabela a seguir:

Tabela 6. Parâmetros Configuráveis

Nome do parâmetro	Valor padrão	Descrição
CPUs virtuais	1	O número de processadores virtuais que estão alocados para a máquina virtual que é representada por essa parte.
Tamanho da memória (MB)	2048	A quantidade de memória que está alocada para essa máquina virtual, em megabytes.
Nome da célula	SOAPolicyAdvancedCell	O nome da célula para o padrão Tempo de Execução Avançado.
Nome do Nó	SOAPolicyAdvancedNode	O nome do nó para o nó que reside na máquina virtual do Deployment Manager no padrão Tempo de Execução Avançado.
Senha (raiz)		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual que é representada por essa parte no padrão.
Verificar senha		Verifica a entrada do usuário para Senha (raiz).
Nome de usuário administrativo do WebSphere	virtuser	O nome do usuário administrador do WebSphere Application Server. Você não deve alterar esse valor.
Senha administrativa do WebSphere		A senha de usuário administrador do WebSphere Application Server.
Verificar senha		Verifica a entrada do usuário para a senha administrativa do WebSphere Application Server.
Ativar VNC	True	Esse valor está bloqueado e não pode ser alterado.

Parte de Nós Customizados do WSRR

A parte dos Nós Customizados do WSRR fornece algumas opções de configuração.

Os parâmetros configuráveis da parte dos Nós Customizados do WSRR são descritos na tabela a seguir:

Tabela 7. Parâmetros Configuráveis

Nome do parâmetro		Descrição
CPUs virtuais	2	O número de processadores virtuais que estão alocados para a máquina virtual que é representada por essa parte.

Tabela 7. Parâmetros Configuráveis (continuação)

Nome do parâmetro		Descrição
Tamanho da memória (MB)	4096	A quantidade de memória que está alocada para essa máquina virtual, em megabytes.
Nome da célula	CloudBurstCell	O valor de nome da célula na configuração da parte do Nó Customizado é ignorado.
Nome do Nó	SOAPolicyAdvancedNode	O nome do nó para o nó que reside na máquina virtual do Nó Customizado no padrão Tempo de Execução Avançado.
Senha (raiz)		A senha para o ID do usuário raiz. Essa é a senha para o sistema operacional da máquina virtual que é representada por essa parte no padrão.
Verificar senha		Verifica a entrada do usuário para Senha (raiz).
Nome de usuário administrativo do WebSphere	virtuser	O nome do usuário administrador do ambiente do WebSphere Application Server. Você não deve alterar esse valor.
Senha administrativa do WebSphere		A senha do usuário administrador do ambiente do WebSphere Application Server.
Verificar senha		Verifica a entrada do usuário para a senha administrativa do WebSphere Application Server.
Ativar VNC	True	Esse valor está bloqueado e não pode ser alterado.

Parte do DataPower

A parte do DataPower possui algumas opções de configuração.

Os parâmetros configuráveis da imagem do sistema virtual do DataPower são descritos na tabela a seguir:

Tabela 8. Parâmetros Configurados

Nome do parâmetro	Valor padrão	Descrição
CPUs virtuais	4	O número de processadores virtuais que estão alocados para a máquina virtual que é representada por essa parte.
Tamanho da memória (MB)	4096	A quantidade de memória que está alocada para essa máquina virtual, em megabytes.
senha do admin		A senha do administrador do DataPower.
Verificar senha		Verifica a entrada do usuário para a senha do admin.

Tabela 8. Parâmetros Configurados (continuação)

Nome do parâmetro	Valor padrão	Descrição
Ativar SSH	True	Ativa SSH (para utilizar a interface da linha de comandos do DataPower).
Porta SSH	22	A porta para SSH.
Ativar a interface de Gerenciamento XML	True	Ativa a interface de Gerenciamento XML. Quando ativada, essa interface permite que os administradores enviem solicitações de status e configuração para o dispositivo DataPower por meio de uma interface SOAP padrão.
Porta da Interface de Gerenciamento XML	5550	A porta para a interface de Gerenciamento XML.
Ativar Serviço de Gerenciamento da Web	True	Ativa a WebGUI para interagir com o dispositivo DataPower.
Porta do Serviço de Gerenciamento da Web	9090	A porta para a WebGUI.
Diretório RAID	raid0	O diretório no qual é possível acessar arquivos no armazenamento de dados auxiliar do DataPower.

Pacotes de Scripts

Há sete pacotes de scripts que são fornecidos com o IBM SOA Policy Gateway Pattern.

Os seguintes pacotes de scripts estão incluídos neste padrão:

- SOA Policy Gateway 2.5.0.0 - Domínio do DataPower
- SOA Policy Gateway 2.5.0.0 - Promoção
- SOA Policy Gateway 2.5.0.0 - Amostras
- SOA Policy Gateway 2.5.0.0 - Segurança
- SOA Policy Gateway 2.5.0.0 - Domínio do DataPower
- SOA Policy Gateway 2.5.0.0 - Incluir Consultas Nomeadas
- SOA Policy Gateway 2.5.0.0 - Derrubar

Os scripts Incluir Consultas Nomeadas e Derrubar não contêm parâmetros configuráveis pelo usuário.

Script: SOA Policy Gateway 2.5.0.0 - Domínio do DataPower

O script de Domínio do DataPower aprovisiona o domínio do DataPower durante a implementação. O script configura a conexão entre o tempo de execução do WSRR e até 10 dispositivos DataPower (virtuais).

Parâmetros

Tabela 9. Parâmetros Configuráveis

Nome do parâmetro	Valor padrão	Descrição
DataPower_hostname	*Esse valor está bloqueado e não pode ser alterado.*	O nome do host para a instância ou o dispositivo DataPower a ser monitorado.
DataPower_admin_id	*Esse valor está bloqueado e não pode ser alterado.*	O ID de usuário administrador para essa instância ou dispositivo.
DataPower_XML_mgmt_port	*Esse valor está bloqueado e não pode ser alterado.*	A porta para se comunicar com a interface de Gerenciamento XML na instância ou no dispositivo DataPower.
DataPower_admin_password	*Esse valor está bloqueado e não pode ser alterado.*	A senha para o ID de usuário administrador.
Verificar senha	*Esse valor está bloqueado e não pode ser alterado.*	Repita a senha para o ID de usuário administrador.
DataPower2_hostname	*Esse valor está bloqueado e não pode ser alterado.*	
DataPower2_admin_id	*Esse valor está bloqueado e não pode ser alterado.*	
DataPower2_XML_mgmt_port	*Esse valor está bloqueado e não pode ser alterado.*	
DataPower2_admin_password	*Esse valor está bloqueado e não pode ser alterado.*	
Verificar senha	*Esse valor está bloqueado e não pode ser alterado.*	
...		...
DataPower10_hostname	*Esse valor está bloqueado e não pode ser alterado.*	
DataPower10_admin_id	*Esse valor está bloqueado e não pode ser alterado.*	
DataPower10_XML_mgmt_port	*Esse valor está bloqueado e não pode ser alterado.*	
DataPower10_admin_password	*Esse valor está bloqueado e não pode ser alterado.*	
Verificar senha	*Esse valor está bloqueado e não pode ser alterado.*	
New_DataPower_domain	O valor padrão depende do tipo de padrão: • SOAPolicyAdvancedRuntime • SOAPolicyBasicRuntime	O novo nome de domínio a ser criado em cada dispositivo ou instância do DataPower. Ele não deve corresponder a nenhum domínio existente ou o pacote de scripts falhará ou sairá. O valor não pode conter espaços.
Remove_security_files	True	Para uso do suporte, é possível ignorar essa configuração.

Script: SOA Policy Gateway 2.5.0.0 - Promoção

O script Promoção permite que um padrão de Tempo de Execução Básico ou de Tempo de Execução Avançado seja integrado ao padrão de SOA Policy Gateway

Governance Master pré-implementado. Ele estabelece segurança de célula cruzada entre o padrão de Tempo de Execução e de Controle, enquanto, opcionalmente, configura a promoção de WSRR no controle principal.

Parâmetros

Tabela 10. Parâmetros Configuráveis

Nome do parâmetro	Valor padrão	Descrição
WSRR_GOV_DMGR_hostname		O nome do host do Dmgr para o Cluster do WSRR.
WSRR_GOV_DMGR_cellname	SOAPolicyGMCell	O Nome da Célula para o Cluster do WSRR.
WSRR_GOV_admin_user	virtuser	O ID de Administrador para a Célula de Controle do WSRR.
WSRR_GOV_admin_password		A senha para o ID de Administrador para a Célula de Controle do WSRR.
Verificar senha		Verifica a entrada do usuário para WSRR_GOV_admin_password.
Promotion_environment		Deve ser temporariedade, produção ou Não configurado. Esses valores fazem distinção entre maiúsculas e minúsculas e devem corresponder exatamente.
LTPA_key_password		Uma Chave LTPA é exportada e usada durante o Pacote de Scripts. A chave é do Controle Principal e é usada em todas as CÉLULAS no ambiente de promoção. Essa é a senha usada ao exportar essa chave LTPA.
Verificar senha		Verifica a entrada do usuário para LTPA_key_password.

Script: SOA Policy Gateway 2.5.0.0 - Amostra

O script de Amostra configura os parâmetros do aplicativo de amostra para serem usados com o padrão SOA Policy Gateway Basic Runtime Sample.

Parâmetros

Nenhum desses parâmetros pode ser configurado pelo usuário.

Tabela 11. Parâmetros Configuráveis

Nome do parâmetro		Descrição
SCP_host	*Esse valor está bloqueado e não pode ser alterado.*	
SCP_user	*Esse valor está bloqueado e não pode ser alterado.*	
SCP_password	*Esse valor está bloqueado e não pode ser alterado.*	
Verificar senha	*Esse valor está bloqueado e não pode ser alterado.*	

Tabela 11. Parâmetros Configuráveis (continuação)

Nome do parâmetro		**Descrição**
SCP_zip_location	*Esse valor está bloqueado e não pode ser alterado.*	
CLIENT_PUBLIC_KEY_file	*Esse valor está bloqueado e não pode ser alterado.*	
CLIENT_PUBLIC _KEY_password	*Esse valor está bloqueado e não pode ser alterado.*	
Verificar senha		
CLIENT_PRIVATE_KEY_file	*Esse valor está bloqueado e não pode ser alterado.*	
CLIENT_PRIVATE_KEY_password	*Esse valor está bloqueado e não pode ser alterado.*	
Verificar senha		
CLI_FILE_file	*Esse valor está bloqueado e não pode ser alterado.*	
Verificar senha	*Esse valor está bloqueado e não pode ser alterado.*	
DataPower_hostname	*Esse valor está bloqueado e não pode ser alterado.*	O nome do host da instância DataPower.
DataPower_XML_mgmt_port	*Esse valor está bloqueado e não pode ser alterado.*	A porta que é usada para a Interface de Gerenciamento XML do DataPower.
DataPower_admin_id	*Esse valor está bloqueado e não pode ser alterado.*	O ID de usuário administrador com permissões apropriadas para usar a Interface de Gerenciamento XML.
DataPower_admin_password	*Esse valor está bloqueado e não pode ser alterado.*	A senha para o DataPower_admin_id.
Verificar senha	*Esse valor está bloqueado e não pode ser alterado.*	Verifica a entrada do usuário para DataPower_admin_password.
SOAPolicySample_DataPower_domain	*Esse valor está bloqueado e não pode ser alterado.*	O nome de domínio da amostra. Ele não deve corresponder a nenhum domínio existente na instância DataPower.
SamplePolicySample_starting_port	*Esse valor está bloqueado e não pode ser alterado.*	O aplicativo requer 5 portas livres, que são usadas em sequência a partir desse valor. Por exemplo, se o valor for 62000, serão usadas as portas de 62000 a 62004. O script não verifica se as portas estão livres.
LDAP_hostname	*Esse valor está bloqueado e não pode ser alterado.*	O nome do host da parte independente do WSRR, em que um servidor LDAP também é hospedado.
LDAP_port	*Esse valor está bloqueado e não pode ser alterado.*	A porta para o servidor LDAP.
LDAP_password	*Esse valor está bloqueado e não pode ser alterado.*	A senha que é usada na ligação com o LDAP_DN.
Verificar senha	*Esse valor está bloqueado e não pode ser alterado.*	Verifica a entrada do usuário para LDAP_password.

Tabela 11. Parâmetros Configuráveis (continuação)

Nome do parâmetro		Descrição
LDAP_DN	*Esse valor está bloqueado e não pode ser alterado.*	O nome distinto que é usado para ligação com o LDAP.

Script: SOA Policy Gateway 2.5.0.0 - Segurança

O script Segurança copia informações de segurança (certificados etc.) entre os sistemas DataPower e WSRR no padrão.

Os parâmetros de configuração para os arquivos de script de segurança são para uso de suporte. Você deve deixá-los configurados como seus valores padrão.

Script: SOA Policy Gateway 2.5.0.0 - Monitoramento do DataPower (apenas x86)

O script Monitoramento do DataPower especifica os parâmetros de conexão para o serviço compartilhado de monitoramento doDataPower. Os coletores de dados e o agente do ITCAM DataPower são executados na parte principal do SO.

Parâmetros

O serviço de monitoramento pode monitorar até 10 dispositivos virtuais DataPower.

Tabela 12. Parâmetros Configuráveis

Nome do parâmetro	Valor padrão	Descrição
DataPower1_hostname		O nome do host para o dispositivo virtual DataPower a ser monitorado.
DataPower1_admin_id	admin	O ID de usuário administrador para esse dispositivo virtual.
DataPower1_XML_mgmt_port	5550	A porta para se comunicar com a interface de Gerenciamento XML no dispositivo virtual DataPower.
DataPower1_admin_password		A senha para o ID de usuário administrador.
Verificar senha		Repita a senha para o ID de usuário administrador.
DataPower2_hostname		
DataPower2_admin_id	admin	
DataPower2_XML_mgmt_port	5550	
DataPower2_admin_password		
Verificar senha		
...		...
DataPower10_hostname		
DataPower10_admin_id	admin	
DataPower10_XML_mgmt_port	5550	
DataPower10_admin_password		
Verificar senha		

Script: SOA Policy Gateway 2.5.0.0 - Monitoramento Externo do DataPower

O script Monitoramento do DataPower especifica os parâmetros de conexão para o serviço compartilhado de monitoramento doDataPower. Os coletores de dados e o agente do ITCAM DataPower são executados na parte principal do SO.

Parâmetros

O serviço de monitoramento pode monitorar até 10 dispositivos DataPower.

Tabela 13. Parâmetros Configuráveis

Nome do parâmetro	Valor padrão	Descrição
DataPower1_hostname		O nome do host para o dispositivo DataPower a ser monitorado.
DataPower1_admin_id	admin	O ID do usuário administrador para esse dispositivo.
DataPower1_XML_mgmt_port	5550	A porta para se comunicar com a interface de Gerenciamento XML no dispositivo DataPower.
DataPower1_admin_password		A senha para o ID de usuário administrador.
Verificar senha		Repita a senha para o ID de usuário administrador.
DataPower2_hostname		
DataPower2_admin_id	admin	
DataPower2_XML_mgmt_port	5550	
DataPower2_admin_password		
Verificar senha		
...		...
DataPower10_hostname		
DataPower10_admin_id	admin	
DataPower10_XML_mgmt_port	5550	
DataPower10_admin_password		
Verificar senha		

Capítulo 5. Trabalhando com o IBM SOA Policy Gateway Pattern

O IBM SOA Policy Gateway Pattern fornece as definições padrão para implementação repetida. Esses tópicos descrevem como implementar os padrões.

Como parte do processo de implementação, configure os parâmetros de parte. Para obter informações adicionais, consulte “Implementando Padrões” na página 47. Os padrões são descritos em Capítulo 4, “Padrões, Partes e Pacotes de Scripts”, na página 19.

Tarefas relacionadas:

Capítulo 3, “Introdução ao IBM SOA Policy Gateway Pattern”, na página 13
Este padrão usa o WebSphere DataPower para controlar mensagens usando políticas controladas e definições de serviço no WSRR. Revise os tópicos nesta seção para entender como fazer o download e instalar o padrão, como verificar o padrão após a instalação, aceitar licenças e as funções de usuário envolvidas.

Planejando a Configuração do Padrão e Pré-requisitos do Padrão

O IBM SOA Policy Gateway Pattern fornece um meio de provisionar de forma rápida e confiável um ambiente para controlar definições de serviço e políticas e aplicar essas políticas. A implementação do padrão inicia com o Controle Principal, seguido pelo padrão de tempo de execução.

Preparando e Implementando o IBM SOA Policy Gateway Pattern

- Se você estiver usando um dispositivo DataPower externo, prepare o dispositivo para administração remota. Para obter informações adicionais, consulte “Configurando um Dispositivo DataPower para os IBM SOA Policy Gateway Patterns” na página 46.

Implemente o padrão de Controle Principal:

1. Implemente um padrão do SOA Policy Gateway Governance Master. Aguarde até que a implementação seja concluída antes de implementar padrões de tempo de execução. Para obter informações adicionais, consulte “Implementando o Padrão de Controle Principal” na página 50.

Implemente os padrões de tempo de execução:

1. Decida se um padrão de tempo de execução básico com um ambiente independente ou um padrão de tempo de execução avançado com um ambiente em cluster é necessário.
2. Determine quantas instâncias ou dispositivos DataPower são necessárias para os seus padrões de tempo de execução.

   Os padrões que incluem DataPower possuem duas instâncias DataPower por padrão. É possível configurar até 10 instâncias DataPower. Para obter informações adicionais, consulte “Incluindo Instâncias do DataPower em um Padrão” na página 56.

   Os padrões com DataPower externo podem ser configurados para funcionar com até 10 dispositivos DataPower. Consulte o “Implementando os Padrões do DataPower Externo Básico e Avançado” na página 57.

Nota: Instâncias e dispositivos extras do DataPower não podem ser incluídos após a conclusão da configuração.

3. Configure o padrão de tempo de execução com as informações de padrão do Controle Principal. Para obter informações adicionais, consulte "Informações de Implementação do SOA Policy Gateway Governance Master" na página 51. É possível omitir informações do padrão do Controle Principal para implementar um sistema independente, se necessário (embora seja mostrado um erro na implementação, ele poderá ser ignorado).
4. Especifique se o sistema de tempo de execução é de temporariedade ou de produção.
5. Implemente o seu padrão. Para obter informações adicionais, consulte "Implementando um Padrão de Tempo de Execução Avançado" na página 53 ou "Implementando um Padrão de Tempo de Execução Básico" na página 52.
6. Aguarde até que esteja totalmente implementado antes de implementar outro tempo de execução.

Quando a implementação dos padrões de tempo de execução estiver concluída:

1. A segurança do WSRR e do WebSphere pode ser atualizada a partir da configuração de segurança padrão. Para obter informações adicionais, consulte "Segurança para os Padrões IBM SOA Policy Gateway Pattern".
2. O domínio do DataPower está pronto para a configuração de gateway. Se estiver usando um dispositivo virtual DataPower, você deverá primeiro aplicar o fix pack mais recente, consulte "Atualizando o DataPower na Instância Implementada" na página 54.

Configurando um Dispositivo DataPower para os IBM SOA Policy Gateway Patterns

Conclua as etapas de configuração do DataPower a seguir para que possa executar os scripts SOAPolicy.

Procedimento

1. Efetue login na WebGUI do dispositivo DataPower como um Administrador.
2. Procure `Interface de Gerenciamento XML`.
3. Certifique-se de que seu estado esteja ativado.
4. Certifique-se de que os itens a seguir estejam ativos e corretamente protegidos:
   - URI de Gerenciamento do SOAP
   - Gerenciamento de Configuração do SOAP
   - Gerenciamento de Configuração do SOAP (v2004)
   - Terminal AMP
   - Terminal SLM
   - Terminal WS-Management
   - Terminal WSDM
   - Assinatura do UDDI
   - Assinatura do WSRR

Segurança para os Padrões IBM SOA Policy Gateway Pattern

A autenticação mútua ocorre entre os aplicativos DataPower e os scripts nos Padrões Básico e Avançado. Os scripts executam a troca de certificados necessária. Observe que os certificados SSL padrão fornecidos com o padrão são atribuídos ao host que foi usado para criar o padrão.

Aumentando a Segurança

As imagens do WSRR e as imagens do WebSphere Application Server que são usadas nos padrões têm apenas a segurança padrão no local. Para produzir um ambiente mais seguro, é possível usar as técnicas de segurança padrão do WebSphere Application Server.

Consulte o Centro de Informações do WebSphere Network Deployment Versão 8.0 nos links a seguir:

- WebSphere Application Server, Network Deployment (plataformas distribuídas e Windows), Versão 8.0: Centro de Informações do IBM WebSphere Application Server, Network Deployment (Plataformas Distribuídas e Windows), Versão 8.0
- Segurança do aplicativo: Centro de Informações do IBM WebSphere Application Server, Network Deployment (Plataformas Distribuídas e Windows), Versão 8.0 - Protegendo Aplicativos e Seus Ambientes
- Caminhos de ponta a ponta para segurança: Centro de Informações do IBM WebSphere Application Server, Network Deployment (Plataformas Distribuídas e Windows), Versão 8.0 - Protegendo Aplicativos e Seus Ambientes

Implementando Padrões

A implementação de padrões com o IBM PureApplication System na nuvem fornece um ambiente de gateway de políticas SOA em execução. É possível implementar os padrões predefinidos disponíveis com as imagens do IBM SOA Policy Gateway Pattern ou implementar padrões criados por você.

Antes de Iniciar

Para implementar um padrão, você deve primeiro ter um padrão predefinido ou um novo padrão que esteja completo, com todas as partes necessárias configuradas. Você necessita de detalhes do ambiente, do grupo de nuvens e do grupo de IPs para implementá-lo a partir do seu administrador do sistema PureAS.

Sobre Esta Tarefa

Você implementa o padrão usando o Console de carga de trabalho.

Procedimento

Para implementar os IBM SOA Policy Gateway Patterns para executar em sua nuvem privada, conclua as etapas a seguir:

1. Na lista de padrões da janela Padrões de Sistema Virtual, selecione o padrão a ser implementado.
2. Clique no ícone **Implementar**.
3. Preencha os campos obrigatórios para implementar o padrão. Na janela, insira um nome para o sistema virtual e quaisquer outras informações necessárias. Uma marca de seleção ao lado de cada item indica que ele não requer configuração adicional. É possível alterar os parâmetros para partes configuradas, antes de implementar o padrão, clicando no nome da parte para abrir o editor para a parte. As máquinas virtuais são criadas na ordem necessária e, em seguida, iniciadas.

Resultados

O processo de implementação cria e inicia máquinas virtuais para as partes que são definidas e fornece links para os consoles necessários. O tempo para a implementação depende da complexidade do padrão implementado. Um padrão implementado é um sistema virtual ou um ambiente de tempo de execução do IBM SOA Policy Gateway Pattern recém-aprovisionado.

O que Fazer Depois

É possível visualizar o status de sua instância, para ver quando a implementação está concluída e começar a administrá-la, a partir da janela Instâncias do Sistema Virtual.

Informações relacionadas:

IBM PureApplication System: Gerenciando Padrões de Sistema Virtual

Implementando o Serviço Compartilhado de Monitoramento do Sistema

Implementar o serviço compartilhado do System Monitoring for SOA Policy Gateway fornece os componentes de monitoramento para o seu sistema virtual.

Antes de Iniciar

O administrador do sistema PureAS devem iniciar o serviço compartilhado do System Monitoring e avisá-lo do grupo de nuvens e do ambiente no qual eles foram iniciados. Você deve usar o mesmo grupo de nuvens e ambiente para implementar o serviço compartilhado de monitoramento do sistema do SOA Policy Gateway e os seus padrões de tempo de execução e controle.

O monitoramento de instâncias do WSRR requer também que o serviço compartilhado do System Monitoring for WebSphere Application Server esteja iniciado, de modo que você deve garantir que ele esteja presente em seu sistema PureAS.

Procedimento

Conclua as seguintes etapas no console de carga de trabalho:

1. Clique em **Instâncias** > **Serviços Compartilhados**.
2. Verifique se o serviço System Monitoring está em execução no grupo de nuvens aos quais seus padrões serão implementados. Se ele não estiver em execução, entre em contato com o administrador do PureAS para iniciá-lo.
3. Para ativar o serviço compartilhado de monitoramento do DataPower:
   a. Clique em **Nuvem** > **Tipos de Padrão**.
   b. Selecione a entrada **System Monitoring for SOA Policy Gateway Pattern 2.5.0.0** na área de janela Tipos de Padrão.
   c. Clique em **Ativar** no campo **Status** e aguarde até que o campo de status seja alterado para **Desativar**.
4. Para iniciar o serviço compartilhado de monitoramento do WebSphere Application Server:
   a. Clique em **Instâncias** > **Serviços Compartilhados**.
   b. Clique no símbolo de mais na área de janela Instâncias do Serviço Compartilhado para abrir a janela Implementar Serviço Compartilhado.

c. Selecione **System Monitoring for WebSphere Application Server** e clique em **OK**.

d. Na janela Configurar e Implementar um Serviço Compartilhado, especifique se deseja que o serviço seja iniciado nos padrões implementados anteriormente selecionando a parte inferior das duas caixas de seleção. Clique em **OK**.

e. Na janela Implementar Aplicativo Virtual, especifique o **Grupo de nuvens de destino**, **Grupo de IPs** e **Perfil** como aconselhado pelo seu administrador do sistema PureAS. Esses devem ser os mesmos que aqueles para os quais foram implementados os Sistemas Virtuais.

5. Para iniciar o serviço compartilhado de monitoramento do WebSphere DataPower:

a. Clique em **Instâncias** > **Serviços Compartilhados** na barra de menus.

b. Clique no símbolo de mais na área de janela Instâncias do Serviço Compartilhado para abrir a janela Implementar Serviço Compartilhado.

c. Selecione **System Monitoring for WebSphere DataPower** na lista e clique em **OK**.

d. Na janela Configurar e implementar um serviço compartilhado, especifique se você deseja monitorar para iniciar nos padrões implementados anteriormente selecionando a parte inferior das duas caixas de seleção. Clique em **OK**.

e. Na janela Implementar Aplicativo Virtual, especifique o **Grupo de nuvens de destino**, **Grupo de IPs** e **Perfil** como aconselhado pelo seu administrador do sistema PureAS. Esses devem ser os mesmos que aqueles para os quais foram implementados os Sistemas Virtuais.

f. Gere e salve uma Chave SSH se precisar de acesso de depuração para o serviço compartilhado de monitoramento.

g. Clique em **OK**.

Resultados

O serviço compartilhado do System Monitoring for WebSphere DataPower é mostrado como em execução. O serviço compartilhado do System Monitoring for WebSphere Application Server é mostrado como em execução.

O que Fazer Depois

Para verificar a implementação, consulte “Verificando a Implementação” na página 55.

Implementando o Padrão de Amostra de Tempo de Execução Básico

A implementação do padrão SOA Policy Gateway Basic Runtime Sample cria uma instância de sistema virtual em execução do padrão. Esse padrão está disponível apenas em sistemas x86.

Sobre Esta Tarefa

A implementação de um padrão cria uma instância de sistema virtual que está em execução na nuvem.

Procedimento

Para implementar o padrão de Amostra de Tempo de Execução Básico do SOA Policy Gateway, conclua as seguintes etapas:

1. No Console de Carga de Trabalho, clique em **Padrões** > **Sistemas Virtuais**.
2. Na lista Padrões do Sistema Virtual, selecione **SOA Policy Gateway 2.5.0.0 - Amostra de Tempo de Execução Básico**.
3. Clique no ícone **Implementar**.
4. Preencha os campos obrigatórios para implementar o padrão. Uma marca de seleção ao lado de cada item indica que ele não requer configuração adicional.
   a. Na caixa **Nome do Sistema Virtual**, insira um nome exclusivo para a instância.
   b. Expanda a seção **Escolher Ambiente** e especifique o **Perfil** aconselhado por seu administrador do sistema PureAS.
   c. Configure os padrões virtuais. Clique em **Configurar partes virtuais** e, em seguida, clique no nome da parte para abrir o editor das partes e dos scripts. Especifique o **Grupo de nuvens** e o **Grupo de IPs**, conforme aconselhado por seu administrador do sistema PureAS. Consulte os tópicos a seguir para obter detalhes dos parâmetros de configuração específicos do padrão e específicos do script.

      Nota: Todas as senhas para esse padrão são assumidas como `password`.
      - "Parte do DataPower" na página 37
      - "Parte do DB2 Enterprise" na página 29.
      - "Parte do Servidor Independente do WSRR" na página 35
      - "Script: SOA Policy Gateway 2.5.0.0 - Amostra" na página 40
5. Clique em **OK** para implementar o padrão.

O que Fazer Depois

Para verificar a implementação, consulte "Verificando a Implementação" na página 55.

Implementando o Padrão de Controle Principal

A implementação do padrão SOA Policy Gateway Governance Master cria uma instância de sistema virtual em execução do padrão.

Procedimento

Para implementar o padrão SOA Policy Gateway Governance Master, conclua as etapas a seguir:

1. No Console de Carga de Trabalho, clique em **Padrões** > **Sistemas Virtuais**.
2. Na lista Padrões de Sistema Virtual, selecione **SOA Policy Gateway 2.5.0.0 - Controle Principal**.
3. Clique no ícone **Implementar**.
4. Conclua os campos para implementar o padrão. Uma marca de seleção ao lado de cada item indica que ele não requer configuração adicional.
   a. Na caixa **Nome do Sistema Virtual**, insira um nome exclusivo para a instância.
   b. Expanda a seção **Escolher Ambiente** e especifique o **Perfil**, conforme aconselhado por seu administrador do sistema PureAS.

c. Configure os padrões virtuais. Clique em **Configurar partes virtuais** e, em seguida, clique no nome da peça para abrir o editor das partes e dos scripts. Especifique o **Grupo de nuvens** e o **Grupo de IPs**, conforme aconselhado por seu administrador do sistema PureAS. Consulte os tópicos a seguir para obter detalhes dos parâmetros de configuração específicos do padrão e específicos do script.
   - "Parte de HADR Primário do DB2 Enterprise" na página 31
   - "Parte do Gerenciador de Implementação do WSRR" na página 36
   - "Parte de Nós Customizados do WSRR" na página 36
   - "Parte de HADR de Espera do DB2 Enterprise" na página 33

5. Clique em **OK** para implementar o padrão.

O que Fazer Depois

Para verificar a implementação, consulte "Verificando a Implementação" na página 55.

Informações de Implementação do SOA Policy Gateway Governance Master

O Controle Principal deve ser implementado antes de os padrões de tempo de execução serem implementados.

Sobre Esta Tarefa

As informações de implementação a partir da instância do Controle Principal são necessárias como entrada para valores de implementação para os padrões de tempo de execução.

Procedimento

Para localizar os valores necessários da instância do Controle Principal:

1. Navegue para **Instâncias** > **Sistemas Virtuais**.
2. Selecione a instância do Controle Principal da implementação.
3. Expanda **Máquinas Virtuais**.
4. Expanda a máquina virtual denominada ***WSRRDMGR***.
5. Observe os seguintes pontos:
   - Na seção **Hardware e Rede**, anote o Nome do Host e o Endereço IP. O nome do host é o valor de **Interface de Rede 0**.
   - Na seção **Configuração do WebSphere**, anote o nome da Célula.

   O nome do host ou IP, o nome da célula e o nome de usuário administrativo e a senha do WebSphere que são usados durante a implementação da instância de Controle Principal são entradas obrigatórias para os seguintes parâmetros nos padrões de tempo de execução:
   - WSRR_GOV_DMGR_hostname
   - WSRR_GOV_DMGR_cellname
   - WSRR_GOV_admin_user
   - WSRR_GOV_admin_password

   Se você deseja implementar um padrão de tempo de execução como um sistema independente, poderá configurar esses parâmetros como "Desconfigurado". Essa configuração faz com que a implementação apareça

como **com falha** em **Sistema Virtual** > **Instâncias**, pois o pacote de scripts de promoção falha. No entanto, a implementação ainda é utilizável.

Implementando um Padrão de Tempo de Execução Básico

A implementação de um padrão de tempo de execução básico cria uma instância de sistema virtual do padrão em execução.

Antes de Iniciar

Conclua as seguintes tarefas antes de implementar o padrão de tempo de execução básico:

- Se você estiver implementando um padrão de tempo de execução básico com DataPower externo, configure seus dispositivos DataPower para o IBM SOA Policy Gateway Pattern; consulte "Configurando um Dispositivo DataPower para os IBM SOA Policy Gateway Patterns" na página 46. Nos Sistemas Power, apenas DataPower externo é suportado.
- Obtenha as informações de implementação do Controle Principal; consulte "Informações de Implementação do SOA Policy Gateway Governance Master" na página 51.

Sobre Esta Tarefa

A implementação de um padrão cria uma instância de sistema virtual que está em execução na nuvem.

Nota: Se você estiver usando o Governance Enablement Profile (GEP), não poderá implementar um ambiente de temporariedade e de produção simultaneamente nos padrões de tempo de execução. Essa limitação é porque isso pode causar conflito durante o processo de configuração das propriedades de promoção. Implemente o ambiente de temporariedade primeiro e, em seguida, o ambiente de produção.

Procedimento

Para implementar um padrão de tempo de execução básico, conclua as seguintes etapas:

1. Clique em **Padrões** > **Sistemas Virtuais**.
2. Na lista Padrões de Sistema Virtual, selecione **SOA Policy Gateway 2.5.0.0 - DataPower Externo de Tempo de Execução Básico** ou **SOA Policy Gateway 2.5.0.0 - Tempo de Execução Básico**.
3. Clique no ícone **Implementar**.
4. Preencha os campos obrigatórios para implementar o padrão. Uma marca de seleção ao lado de cada item indica que ele não requer configuração adicional.
   a. Na caixa **Nome do Sistema Virtual**, insira um nome exclusivo para a instância.
   b. Expanda a seção **Escolher Ambiente** e especifique o **Perfil** aconselhado por seu administrador do sistema PureAS.
   c. Configure os padrões virtuais. Clique em **Configurar partes virtuais** e, em seguida, clique no nome da parte para abrir o editor das partes e dos scripts. Especifique o **Grupo de nuvens** e o **Grupo de IPs**, conforme aconselhado por seu administrador do sistema PureAS. Consulte os tópicos a seguir para obter detalhes dos parâmetros de configuração específicos do padrão e específicos do script.

Nota: Se desejar implementar o padrão sem um controle principal, insira 'Desconfigurado' como o parâmetro do nome do host do controle principal. Esteja ciente de que isso resulta no pacote de scripts de promoção sendo relatado como falha na implementação, mas não há outras consequências.

- "Parte do DataPower" na página 37
- "Parte do DB2 Enterprise" na página 29
- "Parte do Servidor Independente do WSRR" na página 35
- "Script: SOA Policy Gateway 2.5.0.0 - Segurança" na página 42
- "Script: SOA Policy Gateway 2.5.0.0 - Promoção" na página 39
- "Script: SOA Policy Gateway 2.5.0.0 - Domínio do DataPower" na página 38
- "Script: SOA Policy Gateway 2.5.0.0 - Monitoramento do DataPower (apenas x86)" na página 42

5. Clique em **OK** para implementar o padrão.

O que Fazer Depois

Para verificar a implementação, consulte "Verificando a Implementação" na página 55.

Implementando um Padrão de Tempo de Execução Avançado

A implementação de um padrão de tempo de execução avançado cria uma instância de sistema virtual do padrão em execução.

Antes de Iniciar

Conclua as seguintes tarefas antes de implementar o padrão de tempo de execução avançado:

- Se você estiver implementando um padrão de tempo de execução avançado com o DataPower externo, configure seus dispositivos DataPower para conectar ao padrão. Consulte o "Configurando um Dispositivo DataPower para os IBM SOA Policy Gateway Patterns" na página 46. Nos Sistemas Power, apenas DataPower externo é suportado.
- Obtenha as informações de implementação do Controle Principal; consulte "Informações de Implementação do SOA Policy Gateway Governance Master" na página 51.

Sobre Esta Tarefa

A implementação de um padrão cria uma instância de sistema virtual que está em execução na nuvem.

Nota: Se você estiver usando o Governance Enablement Profile (GEP), não poderá implementar um ambiente de temporariedade e de produção simultaneamente nos padrões de tempo de execução. Essa limitação é porque isso pode causar conflito durante o processo de configuração das propriedades de promoção. Implemente o ambiente de temporariedade primeiro e, em seguida, o ambiente de produção.

Procedimento

Para implementar um padrão de tempo de execução avançado, conclua as seguintes etapas:

1. Clique em **Padrões** > **Sistemas Virtuais**.

2. Na lista Padrões de Sistema Virtual, selecione **SOA Policy Gateway 2.5.0.0 - DataPower Externo de Tempo de Execução Avançado** ou **SOA Policy Gateway 2.5.0.0 - Tempo de Execução Avançado**.
3. Clique no ícone **Implementar**.
4. Preencha os campos obrigatórios para implementar o padrão. Uma marca de seleção ao lado de cada item indica que ele não requer configuração adicional.
   a. Na caixa **Nome do Sistema Virtual**, insira um nome exclusivo para a instância.
   b. Expanda a seção **Escolher Ambiente** e especifique o **Perfil** aconselhado por seu administrador do sistema PureAS.
   c. Configure os padrões virtuais. Clique em **Configurar partes virtuais** e, em seguida, clique no nome da parte para abrir o editor das partes e dos scripts. Especifique o **Grupo de nuvens** e o **Grupo de IPs**, conforme aconselhado por seu administrador do sistema PureAS. Consulte os tópicos a seguir para obter detalhes dos parâmetros de configuração específicos do padrão e específicos do script.

      Nota: Se desejar implementar o padrão sem um controle principal, insira 'Desconfigurado' como o parâmetro do nome do host do controle principal. Esteja ciente de que isso resulta no pacote de scripts de promoção sendo relatado como falha na implementação, mas não há outras consequências.
      - "Parte do DataPower" na página 37
      - "Parte de HADR Primário do DB2 Enterprise" na página 31
      - "Parte do Gerenciador de Implementação do WSRR" na página 36
      - "Script: SOA Policy Gateway 2.5.0.0 - Promoção" na página 39
      - "Script: SOA Policy Gateway 2.5.0.0 - Domínio do DataPower" na página 38
      - "Parte de Nós Customizados do WSRR" na página 36
      - "Parte de HADR de Espera do DB2 Enterprise" na página 33
      - "Script: SOA Policy Gateway 2.5.0.0 - Monitoramento do DataPower (apenas x86)" na página 42
5. Clique em **OK** para implementar.

O que Fazer Depois

Para verificar a implementação, consulte "Verificando a Implementação" na página 55.

Atualizando o DataPower na Instância Implementada

Depois de implementar um padrão que inclui um componente do WebSphere DataPower, você deve atualizar o DataPower para o fix pack mais recente.

Sobre Esta Tarefa

Você atualiza o DataPower fazendo download do fix pack no Fix Central e aplicando-o na WebGUI do DataPower.

Procedimento

1. Faça o download do pacote de atualização a partir do Fix Central:
   a. No Fix Central, procure por Dispositivos do WebSphere DataPower SOA.
   b. Selecione e faça o download do pacote XI52-virtual-6.0.0.1-Firmware.

2. Conecte à WebGUI da máquina virtual do DataPower em seu padrão implementado; consulte “Conectando ao Console de um DataPower Virtual” na página 85.
3. No painel de controle, selecione **Controle do Sistema**.
4. Localize a seção **Imagem de Inicialização**.
5. Faça upload para o dispositivo DataPower do arquivo `xi6001.scrypt4` a partir do fix pack transferido por download. Use o File Manager na WebGUI do DataPower.
6. Selecione o script transferido por upload a partir da lista **Lista de Firmware**.
7. Aceite as condições de licença e clique em **Imagem de Inicialização**.
8. Siga os prompts para instalar o fix pack.

Verificando a Implementação

Depois de implementar o padrão, verifique se a implementação foi bem-sucedida.

Procedimento

1. Verifique os logs de implementação em busca de qualquer falha no histórico de implementação de sistema virtual. Para obter informações adicionais, consulte “Resolução de Problemas com a Implementação” na página 101.
2. Opcional: Se você implementou o SOA Policy Gateway Basic Runtime Sample, teste a instância implementada seguindo o tutorial para enviar algumas mensagens de amostra usando os aplicativos de amostra fornecidos. Consulte o “Executando os Casos de Teste de Amostra” na página 61.

Incluindo um Ambiente de Tempo de Execução Adicional

O Perfil de Ativação de Controle é fornecido com um sistema de classificação do ambiente predefinido que contém quatro ambientes distintos: Desenvolvimento, Teste, Temporariedade e Produção.

Sobre Esta Tarefa

Os ambientes de Temporariedade e Produção também são codificados no ciclo vida do SOA que define o ciclo de vida de Versões de Recurso, como Versões de Serviço. Há estados e transições que são específicos para os ambientes de Temporariedade e Produção, permitindo a promoção controlada nesses ambientes de tempo de execução, definindo os sistemas de destino no arquivo de configuração de promoção. Esse procedimento será apropriado se sua organização define ambientes da mesma maneira, com Temporariedade como um ambiente de Pré-produção que permite testar antes da Versão do Recurso ser aberta para uso geral. No entanto, várias organizações exigem mais ambientes, portanto, as modificações são necessárias no perfil para acomodar essas diferenças. Esta seção descreve uma maneira de como um novo ambiente de tempo de execução pode ser incluso no Perfil de Ativação de Controle do WSRR.

Para obter informações adicionais sobre o planejamento de um ambiente de implementação, consulte “Planejando a Configuração do Padrão e Pré-requisitos do Padrão” na página 45.

Procedimento

1. Implemente o SOA Policy Gateway Governance Master predefinido. Para obter informações adicionais, consulte “Implementando o Padrão de Controle Principal” na página 50.

2. Opcional: Modifique o Perfil de Ativação de Controle do WSRR. Para obter informações adicionais, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Tutorial: Customizando Ambientes de Tempo de Execução.
3. Configure os padrões de tempo de execução básico ou de tempo de execução avançado com detalhes do Controle Principal. Para obter informações adicionais, consulte "Informações de Implementação do SOA Policy Gateway Governance Master" na página 51.

   Nota: O valor do ambiente de promoção deve ser configurado como "Não Configurado".
4. Implemente os padrões de tempo de execução básico ou de tempo de execução avançado predefinidos. Para obter mais informações, consulte "Implementando um Padrão de Tempo de Execução Básico" na página 52 e "Implementando um Padrão de Tempo de Execução Avançado" na página 53.

Incluindo Instâncias do DataPower em um Padrão

Os padrões básico e avançado com instâncias internas do DataPower possuem duas instâncias por padrão. Cada padrão possui até 10 instâncias DataPower no total.

Sobre Esta Tarefa

Os padrões propriamente ditos não podem ser editados. É possível incluir mais instâncias DataPower nos padrões de tempo de execução básico ou de tempo de execução avançado fazendo uma cópia do padrão e editando-a.

Procedimento

1. Abra o padrão no Console de Carga de Trabalho.
2. Clique em **Clonar** e especifique um nome para a cópia do padrão.
3. Clique em **Editar**.
4. Arraste mais partes do DataPower da lista de partes para incluí-las no padrão.
5. Clique em **Concluir Edição**.

Excluindo Instâncias do DataPower a Partir de um Padrão

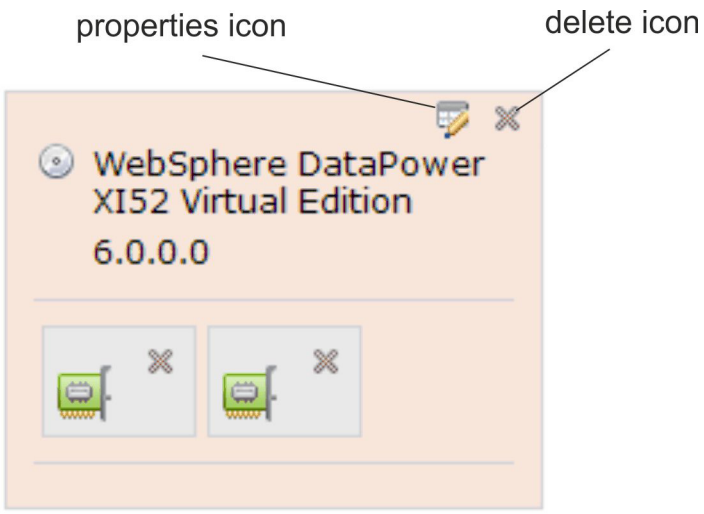
É possível excluir instâncias internas do DataPower a partir de um padrão, se necessário.

Sobre Esta Tarefa

Os padrões propriamente ditos não podem ser editados. É possível excluir instâncias do DataPower dos padrões de tempo de execução básico e de tempo de execução avançado fazendo uma cópia do padrão e editando-a.

Procedimento

1. Abra o padrão no Console de Carga de Trabalho.
2. Clique em **Clonar** e especifique um nome para a cópia do padrão.
3. Clique em **Editar**.
4. Exclua uma instância do DataPower clicando no ícone de exclusão.



Nota: As instâncias do DataPower devem ser excluídas em ordem numérica reversa. Cada instância do DataPower na tela possui um número em seu campo de nome, que é visível clicando no ícone de propriedades. O nome está no formato: 'DataPower_XI52*x*', em que *x* é o número (a primeira instância do DataPower não possui um número de qualquer modo, seu nome é: 'DataPower_XI52'). As instâncias do DataPower com numeração mais alta estão geralmente na parte superior esquerda da tela.

5. Clique em **Concluir Edição**.

Implementando os Padrões do DataPower Externo Básico e Avançado

Os padrões do SOA Policy Gateway Basic Runtime External DataPower e do SOA Policy Gateway Advanced Runtime External DataPower podem ser implementados com até 10 dispositivos DataPower.

Sobre Esta Tarefa

Para obter informações adicionais sobre como implementar padrões, consulte “Implementando um Padrão de Tempo de Execução Básico” na página 52 ou “Implementando um Padrão de Tempo de Execução Avançado” na página 53. Para obter informações adicionais sobre os parâmetros de configuração para os quais é necessário configurar valores, consulte “Parte do Servidor Independente do WSRR” na página 35, “Parte do Gerenciador de Implementação do WSRR” na página 36 e “Script: SOA Policy Gateway 2.5.0.0 - Monitoramento do DataPower (apenas x86)” na página 42.

Procedimento

1. Implemente o padrão e clique em **Configurar partes virtuais**.
2. Para a parte do gerenciador independente do WSRR ou de implementação do WSRR, insira as seguintes informações para cada dispositivo:
   - DataPower_hostname
   - DataPower_XML_mgmt_port
   - DataPower_admin_id
   - DataPower_admin_password
   - Verificar senha
   - New_DataPower_domain

O Aplicativo de Amostra

O aplicativo de amostra consiste em um Serviço da Web e uma API RESTful, ambos descritos e controlados no WSRR. Um domínio DataPower é configurado com o WSRR para ser um gateway e um Web Client de amostra é fornecido para praticar os serviços.

O cenário básico no aplicativo de amostra é o de um aplicativo de inventário para um armazenamento (Warehouse) e um serviço RESTful que duplica uma das operações para dispositivo móvel. O serviço da web Store possui três operações:

- purchase
- findInventory
- returnProduct

A última operação, findInventory, também está disponível como um serviço RESTful.

O Serviço da Web de Amostra

A definição de nível de serviço (SLD) básica possui duas políticas de mediação anexadas:

- Validação contra Store.wsdl. A amostra supõe que a Validação do DataPower esteja desligada.
- Rejeite se houver mais de 5 mensagens em 90 segundos. Esse limite é baixo para facilitar a demonstração.

O consumidor do serviço Store é o aplicativo StoreConsumer, que possui o ID do consumidor de “CEO”. Esse consumidor possui dois Acordos de Nível de Serviço (SLAs), Gold e Silver. Se uma solicitação chegar no DataPower com o ID do consumidor de “CEO” e um ID de Contexto de “Silver”, será permitida a passagem da solicitação, pois o SLA Silver está no local. Se o ID do consumidor for “CEO” e o ID do contexto for “Gold”, o SLA Gold será correspondido. Esse SLA possui uma política de novo roteamento anexada a ele, portanto a solicitação será novamente roteada para o terminal alternativo especificado na política.

Se uma solicitação chegar com um ID do consumidor diferente de “CEO”, não haverá uma Versão do Aplicativo com este ID do consumidor. Também não haverá SLAs que poderiam corresponder, portanto essa será uma solicitação de um consumidor anônimo. Dessa forma, todas as políticas anexadas ao SLA anônimo serão aplicadas. Nesse caso, isso faz com que a notificação apareça nos logs. Observe, a amostra não inclui uma maneira de enviar uma solicitação com um ID do consumidor que não seja “CEO”.

O cenário também executa a autorização para a operação findInventory, que é baseada na associação do grupo de usuários. Um servidor LDAP é fornecido com a amostra para mapear as credenciais do usuário para o grupo correto.

O diagrama do fluxo do aplicativo de amostra mostra o fluxo do aplicativo com cada caixa representando um gateway DataPower diferente.

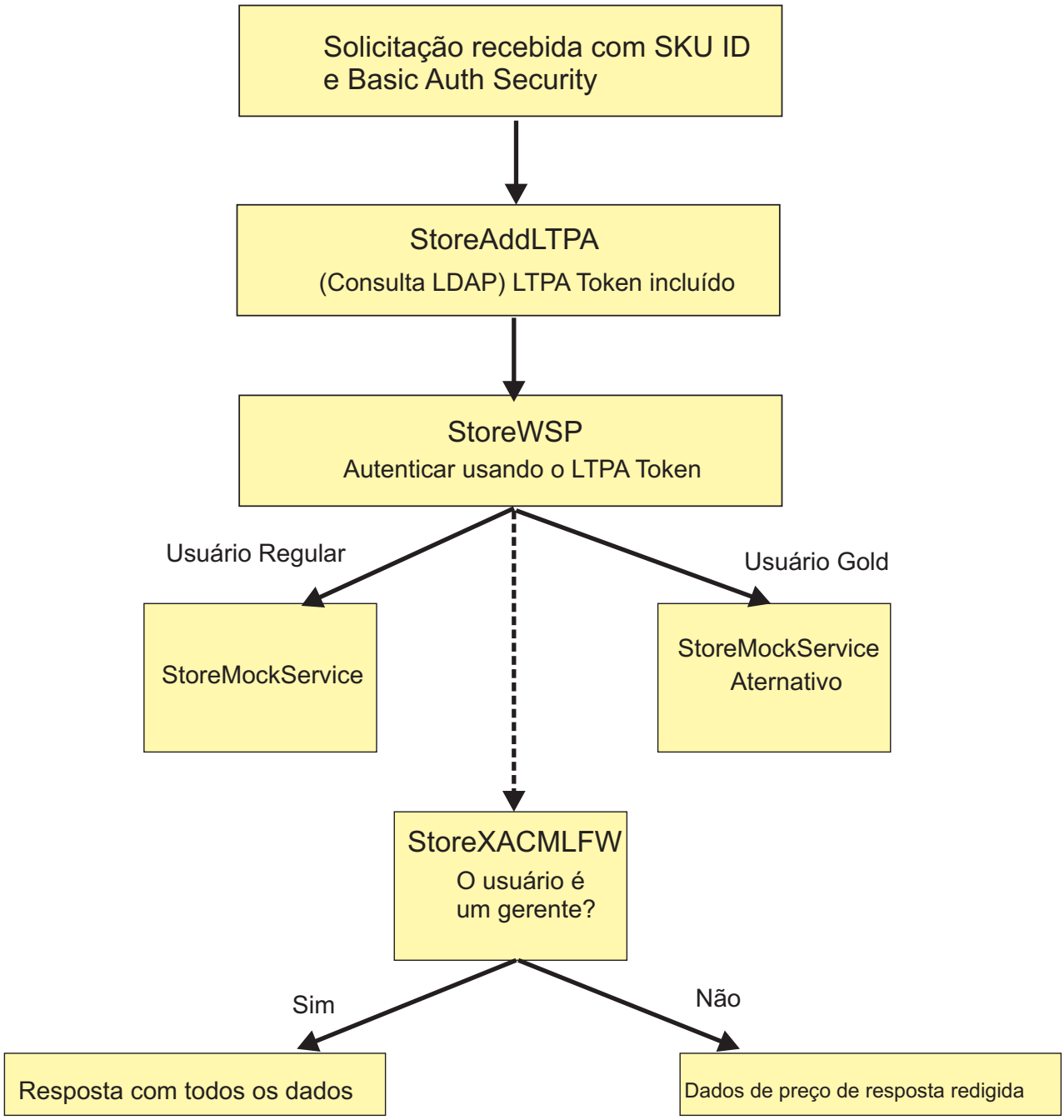


Figura 10. O Fluxograma do Aplicativo de Amostra

O Serviço RESTful de Amostra

O serviço RESTful é controlado de maneira semelhante ao serviço da web, exceto na maneira como as políticas são usadas. Como com o serviço da web, há dois SLAs: um para clientes Silver e um para clientes Gold. Para o serviço REST, no entanto, não há políticas anexadas no nível SLD (aplicado a todas as solicitações). Em vez disso, há uma política anexada a cada um dos SLAs. O SLA Gold possui uma política que rejeita mensagens após mais de 5 solicitações feitas em 90 segundos, e Silver permite 2 solicitações e 90 segundos antes de rejeitar.

Visão Geral de Artefatos do WSRR na Amostra

Os artefatos do WSRR que descrevem o Serviço Store são descritos aqui. Os artefatos para o serviço REST seguem um padrão semelhante.

O Warehouse do Bob é a organização que possui o serviço Store e o aplicativo consumidor StoreConsumer.

O serviço Warehouse Business é o objeto sob o qual todas as versões do serviço Store permanecem. A versão do serviço Store representa uma versão específica do serviço Store. Essa versão é o serviço que está sendo fornecido para reutilização. A definição de nível de serviço (SLD) Store possui duas políticas anexadas; a primeira política rejeita mensagens após 5 mensagens em 90 segundos e a segunda política executa a validação com relação ao esquema Store.wsdl. Essas políticas significam que as solicitações para o serviço Store são validadas e um máximo de 5 solicitações são permitidas através do serviço em um período de 90 segundos, independentemente da procedência da solicitação. O SLD também possui um acordo de nível de serviço (SLA) anônimo. Todas as políticas anexadas a este SLA são aplicadas quando entrarem solicitações para as quais não há SLA correspondente. Um SLA corresponderá se as seguintes condições forem atendidas:

- Houver uma Versão do Aplicativo consumidor que corresponda ao ID do consumidor na solicitação.
- Houver um SLA no local entre essa versão do aplicativo consumidor e o SLD para o serviço que está sendo consumido, que corresponda ao ID de contexto na solicitação

O aplicativo de negócios StoreConsumer representa o Aplicativo StoreConsumer, que a Versão do Aplicativo StoreConsumer é uma versão específica desse aplicativo. Esse aplicativo é o consumidor: ele está reutilizando o serviço Store. Ele tem o ID do consumidor de “CEO”. Há dois SLAs no local desse aplicativo, o qual constitui um acordo para permitir que esse aplicativo consuma o serviço Store. Um possui o ID de contexto de “Gold”, significando que corresponde solicitações do aplicativo StoreConsumer que têm o ID de contexto de “Gold” na solicitação e um corresponde a Silver. O SLA Gold possui uma política anexada às solicitações de novo roteamento, portanto todas as solicitações do aplicativo StoreConsumer que tenham o ID de contexto configurado como Gold são roteados novamente para o terminal especificado na política. O SLA Silver não possui políticas anexadas, portanto sua existência significa que as solicitações do aplicativo StoreConsumer que têm um ID de contexto de Silver têm permissão de passagem, embora nenhuma política seja aplicada.

Nessa amostra, há uma política de notificação anexada ao SLA anônimo.

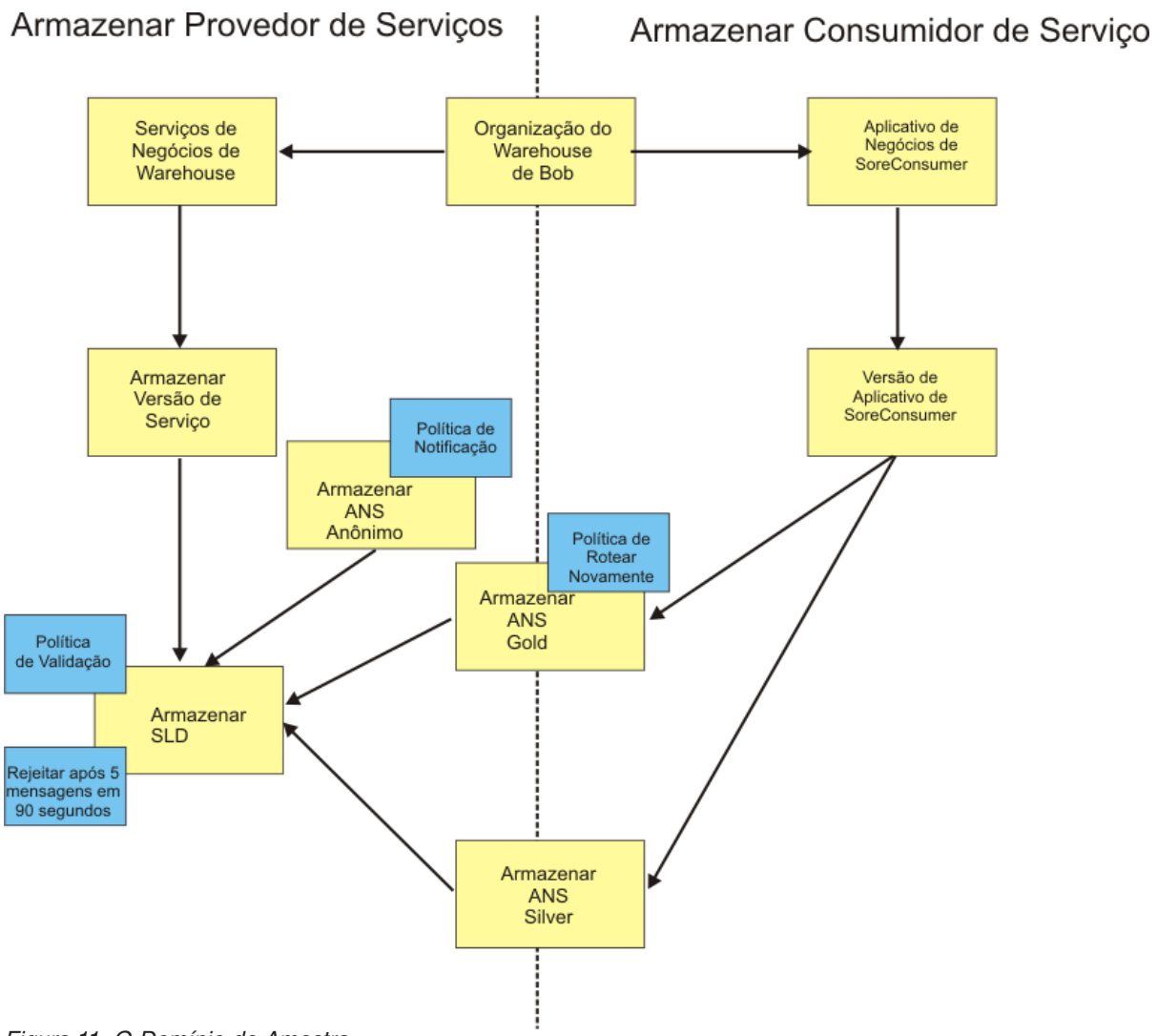


Figura 11. O Domínio de Amostra

Executando os Casos de Teste de Amostra

É possível usar o aplicativo da web de amostra ou a linha de comandos para testar o aplicativo Sample no SOA Policy Gateway Basic Runtime Sample implementado. Seis variações de teste de linha de comandos podem ser executadas no aplicativo de amostra.

Para implementar o Basic Sample Runtime, consulte "Implementando o Padrão de Amostra de Tempo de Execução Básico" na página 49.

Executando o caso de teste do aplicativo da web de amostra

Para executar o caso de teste do aplicativo da web:

1. Localize o nome do host do ambiente implementado no WSRR abrindo a Instância do Sistema Virtual implementado. Para localizar o nome do host, expanda a seção **Máquinas virtuais** e selecione a máquina virtual para o Servidor Independente WSRR para ver os detalhes da máquina virtual. Na seção **Hardware e Rede**, o nome do host é o valor **Interface de Rede 0**.

2. Abra a URL em um navegador da web: `http://<wssrHostName>:9080/SoaPolicyTester`
3. As seguintes opções estão disponíveis:
   - **Solicitação Padrão** - Envia uma solicitação findInventory para o serviço Store. O ID de contexto é Silver. O ID do consumidor é CEO. Um resultado bem-sucedido exibe o texto “Part: SKU10 Price: 401.73”.
   - **Teste da Política de Roteamento** - Igual à Solicitação Padrão, mas com ID de Contexto de Gold. A solicitação é roteada para um terminal alternativo que está executando o serviço. Um resultado bem-sucedido retorna “Part: GOLDSKU10 Price: 401.73”.
   - **Teste de Política de Validação** - Envia uma solicitação com uma carga útil inválida. A política de validação requer que o DataPower valide a solicitação e rejeite as mensagens que são inválidas. Um resultado bem-sucedido é uma mensagem de resposta do DataPower `"Erro Interno (do cliente)"`.
   - **REST Gold** - Envia solicitação ao serviço SKU RESTful com ID do Consumidor CEO e ID de Contexto Gold. As solicitações Gold estão sujeitas a uma política que permite apenas 5 mensagens em 90 segundos. Uma solicitação bem-sucedida exibe o resultado “Part: SKU33 Price: 136.43”.
   - **REST Silver** - Igual à Rest GOLD, mas com ID de Contexto Silver. As solicitações Silver são permitidas em 3 solicitações separadas em 90 segundos. Uma solicitação bem-sucedida exibe o resultado “Part: SKU33 Price: 136.43”.
   - **ID do Usuário** - A opção ID do Usuário tem dois valores possíveis; Conteúdo Integral ou Conteúdo da Edição de Dados. Cada opção resulta em solicitações que se originam de usuários diferentes. A amostra utiliza uma política XACML, que permite que apenas Gerentes vejam o preço. O valor do Preço na mensagem de resposta é editado, a menos que Conteúdo Integral esteja selecionado. Um resultado bem-sucedido para solicitações quando Conteúdo Editado estiver selecionado contém “Preço: 0.0”. O serviço RESTful não suporta edição de dados. O usuário selecionado não tem efeito.
4. Abra o console do WSRR e explore o serviço e as políticas. Para obter informações adicionais, consulte “Conectando ao WSRR - Business Space” na página 82.

A amostra também pode ser praticada usando a linha de comandos. Essa é a única maneira de enviar tráfego que usa o SLA Anônimo

Demonstrando Permitir/Negar do XACML com o Cenário de Edição de Dados Usando a Linha de Comandos

O XML de solicitação a seguir pode ser enviado ao Serviço StoreAddLTPA do DataPower:

```
<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>
```

Supondo que o XML da solicitação de exemplo esteja contido em um arquivo chamado `silver.xml`, insira o seguinte comando curl:

```
curl -k --data-bin @./silver.xml -H "Content-Type: text/xml"
-u ConsumerX:passw0rd http://<yourDataPowerHostName>:62005/Store/Store
```

Neste exemplo, ConsumerX é um Gerente, de modo que as informações completas de preço são visíveis na resposta:

```
<?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>
```

Executando o Cenário Edição de Dados Usando a Linha de Comandos

O ConsumerA não é um gerente, portanto ele vê uma resposta diferente. Insira o comando curl:

```
curl -k --data-bin @./silver.xml -H "Content-Type: text/xml"
-u ConsumerA:passw0rd http://<yourDataPowerHostName>:62005/Store/Store
```

Observe que a resposta tem o preço editado. O preço é exibido como 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>
```

Testando a Política de Roteamento Usando a Linha de Comandos

Para a política de roteamento anexada ao SLA gold a ser impingido, o ID de contexto e o ID de consumidor devem ser correspondidos. Nesse caso, o SLA para Clientes Gold possui o ID de contexto de Gold e a versão de serviço de consumo possui o ID de consumidor de CEO. Aqui está o conteúdo de uma solicitação de amostra (é possível ver que o ID de contexto e o ID de consumidor correspondem, conforme necessário):

```
<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>
```

Supondo que o XML da solicitação de exemplo esteja contido em um arquivo chamado `gold.xml`, insira o seguinte comando curl:

```
curl -k --data-bin @./gold.xml -H "Content-Type: text/xml"
-u ConsumerX:passw0rd http://<yourDataPowerHostName>:62005/Store/Store
```

A resposta é a seguinte:

```
<?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>
```

Observe que a resposta de retorno tem um `GOLDSKU` para o valor de SKU, indicando que o terminal ouro foi usado.

Testando a Validação do Esquema Usando a Linha de Comandos

A política de validação verifica o esquema da solicitação com relação ao Store.wsdl e seu Company.xsd associado.

O XML a seguir, `badvalid.xml`, mostra uma solicitação que é inválida porque o corpo contém um elemento denominado `<skubad>` quando deveria ser `<sku>`:

```
<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>
```

Se você inserir a seguinte solicitação curl:

```
curl -k --data-bin @./badvalid.xml -H "Content-Type: text/xml"
-u ConsumerX:passw0rd
http://<yourDataPowerHostName>:62005/Store/Store
```

O seguinte erro é exibido:

```
<?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>Erro interno (do cliente)</faultstring>
</env:Fault>
</env:Body>
</env:Envelope>
```

Testando a Rejeição na Política de Mediação Usando a Linha de Comandos

Umas das políticas de mediação incluídas na rejeição de testes de amostra após a contagem de mensagens é executada 5 vezes em 90 segundos. Execute o comando a seguir 6 vezes:

```
curl -k --data-bin @./silver.xml -H "Content-Type: text/xml" -u ConsumerX:passw0rd
http://<yourDataPowerHostName>:62005/Store/Store
```

A solicitação de amostra é a seguinte:

```
<?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>
```

Nesse caso, o ConsumerX é um Gerente, portanto, as informações completas de preço são exibidas para as cinco primeiras execuções:

```
<?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>
```

Na sexta execução, ocorre o seguinte erro:

```
<?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>Rejeitado (do cliente)</faultstring>
</env:Fault>
</env:Body>
</env:Envelope>
```

Nota: É possível ver esse erro mais cedo se você estiver executando outros testes dentro do intervalo de 90 segundos.

Testando a Notificação na Política de Mediação Usando a Linha de Comandos

A política de notificação é anexada ao SLA anônimo. Isso é impingido quando uma solicitação for proveniente de um consumidor que não tem um SLA no local. Nesta amostra, o único consumidor que possui SLAs no local é o CEO, de modo que uma solicitação contendo o ID do consumidor configurado como algum outro faz com que a política no SLA anônimo seja impingida. Nesse caso, ConsumerX é um Gerente, de modo que as informações completas de preço são exibidas:

Para testar essa funcionalidade usando a linha de comandos, crie um arquivo chamado `anon.xml` que contém o seguinte xml:

```
<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">ABC</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>
```

Em seguida, insira o seguinte comando:

```
curl -k --data-bin @./anon.xml -H "Content-Type: text/xml"
-u ConsumerX:passw0rd http://<yourDataPowerHostName>:62005/Store/Store
```

A mensagem a seguir é gerada no log padrão do Domínio:

```
Notificar ação acionada ('operation_38_2_sla1-1-filter_1-notify') pela política de origem ('LogEveryTime_287d0790-83d9-11e1
```

Nota: A criação de log deve estar configurada como “aviso” para ver essa mensagem. Se não estiver, clique no ícone **Resolução de Problemas** no Console da Web do DataPower. Na seção Criação de Log, altere o valor de Nível de Log para

"aviso" e clique em **Configurar Nível de Log**. Para localizar o log, retorne ao Painel de Controle e clique no ícone **Visualizar Logs**.

Testando o Serviço RESTful Usando a Linha de Comandos

Também é possível acessar a interface RESTful a partir da linha de comandos usando curl. Como com Web client, um ContextID de Gold permite 5 mensagens por 90 segundos e Silver apenas 2 mensagens.

Para testar essa funcionalidade usando a linha de comandos, crie um arquivo chamado restRequest.xml que contém o seguinte xml:

```
<?xml version="1.0" encoding="UTF-8"?>
<a:WarehouseSKUPost xmlns:a="http://company.ibm.com/">
   <postRequest>
      <sku>SKU33</sku>
      <purchaseCost>136.43</purchaseCost>
      <inventory>429</inventory>
      <msrp>272.86</msrp>
      <returns>0</returns>
   </postRequest>
</a:WarehouseSKUPost>
```

Em seguida, insira o seguinte comando para testar com o contextID Gold:

```
curl -k --data-bin @./restRequest.xml -H "Content-Type: text/xml" -H "consumerID:CEO" -H "contextID:Gold"  http://<yourDa
```

Para testar com o silver contextID use o mesmo comando, mas substitua Gold por Silver.

Uma resposta bem-sucedida é:

```
<?xml version="1.0" encoding="UTF-8"?>
<a:WarehouseSKUGet xmlns:a="http://company.ibm.com/">
<getRequest>
<sku>SKU33</sku>
<purchaseCost>136.43</purchaseCost>
<inventory>429</inventory>
<msrp>272.86</msrp>
<returns>0</returns>
<supplierID>ABB</supplierID>
<purchaseID/>
</getRequest>
</a:WarehouseSKUGet>
```

Depois que o limite foi violado, você receberá a seguinte mensagem:

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

Para praticar o SLA anônimo para o serviço RESTful, que simplesmente possui uma política de notificação anexada, use qualquer ContextID e ConsumerID diferente dos registrados. A notificação aparece no log DataPower, conforme descrito anteriormente para o exemplo de Serviços da Web.

Tarefas relacionadas:

"Implementando o Padrão de Amostra de Tempo de Execução Básico" na página 49

A implementação do padrão SOA Policy Gateway Basic Runtime Sample cria uma instância de sistema virtual em execução do padrão. Esse padrão está disponível apenas em sistemas x86.

Estendendo o Aplicativo de Amostra

O aplicativo de amostra pode ser modificado alterando a folha de estilo Ligações e as folhas de estilo XSL.

Modificações na Folha de Estilo de Ligações

A variável xacml-subjects foi inclusa na folha de estilo `apil-xacml-binding-new.xsl`. Ela inclui a criação da seção de assuntos da solicitação. Essa variável é acessada posteriormente no `sendToPDP.xsl`.

```
<xsl:variable name="xacml-subjects">
  <xacml-context:Subject
  SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<!--
**********************************************
Iniciando aqui, use o resultado do MC como assunto.
**********************************************
```

sendToPDP.xsl

Esta folha de estilo chama o StoreXACMLFW usando url-open. A chamada está na caixa para outro Firewall XML, portanto, nenhum perfil Proxy SSL é usado. Para mover o Policy Decision Point (PDP) para outra caixa do DataPower, um perfil proxy SSL poderia ser criado e usado com a chamada url-open.

```
<xsl:param name="resource" />
<!--
<xsl:variable name="incoming_resource">
<xsl:value-of select="$resource" />
</xsl:variable>
<xsl:message dp:priority="debug">
********** PRESTES A CHAMAR O PDP para RECURSO igual *************
<xsl:value-of select="$incoming_resource" />
</xsl:message>
-->
- <!--
construindo a solicitação XACML para mascaramento
-->
<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.xmlsoap.org/soap/envelop
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os" xmlns:ws="http://docs.oasis-open.org/wss/2004/01/oasis
wss-wssecurity-secext-1.0.xsd">
- <!--
copiar nos assuntos salvos do processamento de solicitação AAA
-->
<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 para que fique visível na Análise, o que é conveniente
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlRequest'" value="$customized-request" />
- <!--
Relate o XACML-REQUEST no log de depuração
-->
<xsl:message dp:priority="debug">
<XACML-REQUEST>
<xsl:copy-of select="$customized-request" />
</XACML-REQUEST>
</xsl:message>
<xsl:variable name="headers">
<header name="SOAPAction">xacml:authorization</header>
</xsl:variable>
- <!--
Chame o PDP XACML para decisão
-->
<xsl:variable name="rtss-response">
<xsl:variable name="StoreGWURL">
<xsl:value-of select="concat('http://','127.0.0.1',':',$StoreGWPort,'/rtss/authz/services/AuthzService')" />
</xsl:variable>
<dp:url-open target="{$StoreGWURL}" http-headers="$headers" response="responsecode">
<xsl:copy-of select="$customized-request" />
</dp:url-open>
</xsl:variable>
- <!--
Use set-variable para que fique visível na Análise, o que é conveniente
-->
<dp:set-variable name="'var://context/snip/xacml/BacksideXacmlResponse'" value="$rtss-response" />
- <!--
Relate o XACML-RESPONSE no log de depuração
-->
<xsl:message dp:priority="debug">
<XACML-RESPONSE>
<xsl:value-of select="$rtss-response" />
</XACML-RESPONSE>
</xsl:message>
</xsl:template>
</xsl:stylesheet>
```

Observe os seguintes pontos sobre o arquivo `sendToPDP.xsl`:

1. A folha de estilo obtém a porta para o XACMLFW do `soavars.xsl`.
2. A variável rtssResponse deve ser exatamente da forma que os Serviços de Segurança de Tempo de Execução usariam e, por sua vez, da forma que o PDP na caixa do DataPower pode processar.
3. A folha de estilo constrói uma solicitação SOAP. As informações de assunto são construídas pela folha de estilo `apil-binding.xsl` anterior e são obtidas pela solicitação de cópia de seleção a seguir:

```
<xsl:copy-of select="dp:variable('var://context/snip/xacml/xacmlSubjects')/*" />
```

4. Esta ação é simplesmente para visualizar a ação: `<xacml-context:AttributeValue>View</xacml-context:AttributeValue>`

5. O ambiente é o StorePriceData, conhecido como um objeto do aplicativo na terminologia do IBM Tivoli Security Policy Manager ou dos Serviços de Segurança de Tempo de Execução.

StorePrivateDataXACML.xml

O código a seguir mostra a folha de estilo da política para edição de dados.

```
<PolicySet PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides"
PolicySetId="RPS:StorePrivateData:policy:dc703409-d408-49b3-acc1-16c89c844fce:rolec4a9f664-a0af-451b-b80b-
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:subject-category:accesssubject"
/>
</SubjectMatch>
</Subject>
</Subjects>
</Target>
<Policy PolicyId="PPS:StorePrivateData:dc703409-d408-49b3-acc1-16c89c844fce:c4a9f664-a0af-451b-
b80b-1cafdb9fd9f0:c4a9f664-a0af-451b-b80b-1cafdb9fd9f0: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">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-a0af-451b-
b80b-1cafdb9fd9f0:c4a9f664-a0af-451b-b80b-1cafdb9fd9f0:pps:rules:0">
<Target />
</Rule>
</Policy>
</PolicySet>
</PolicySet>
```

Observe os seguintes pontos:

- A Função deve ser Gerente:

```
<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>
```

- O Recurso deve ser 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>
```

- A Ação deve ser Visualizar:

```
<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>
```

Modificando as Folhas de Estilo XSL de Amostra

É possível modificar a folha de estilo da edição de dados, `noPriceInfo.xsl`

Procedimento

Modifique a folha de estilo de Edição de Dados.
A folha de estilo `noPriceInfo.xsl` contém o código a seguir, que substituirá quaisquer valores de preços por zeros. É possível incluir outros campos na lógica de edição de dados ou incluir transformações mais complicadas que envolvem cálculo para determinar valores para os campos.

```
<!-- campos de acesso privado apenas -->
<xsl:template match="price">
<price>0.0</price>
</xsl:template>
<xsl:template match="Price">
<Price>0.0</Price>
</xsl:template>
```

Posteriormente, a folha de estilo executa uma transformação de identidade em todos os outros elementos.

Exploração Adicional da Amostra

Para saber mais sobre a amostra, você pode configurar o XACML Policy Decision Point (PDP) no DataPower e editar documentos de política.

Alterando o PDP XACML no DataPower

É possível explorar alteração no XACML usado para o Policy Decision Point (PDP) de segurança no DataPower para saber mais sobre controle de acesso com o XACML.

Procedimento

Para alterar ou incluir um PDP:

1. No Painel de Controle do DataPower, procure `PDP XACML`.
2. Clique em um PDP existente ou clique em **Incluir**.
3. Insira uma URL, por exemplo, `local:///storePrivateDataXACML.xml`.
4. Inclua quaisquer arquivos dependentes ou de diretório que sejam necessários para suportar a política.

   Nota: Se você editar um arquivo de políticas XACML diretamente no sistema de arquivos, deverá voltar para a definição de PDP e inserir novamente a URL ou qualquer coisa que você tenha alterado, ou reiniciar o domínio para que sua mudança entre em vigor.

Incluindo um Novo ou Editando Documentos sobre Políticas Existentes

Use a interface com o usuário do Business Space para incluir novos documentos sobre políticas ou edite os já existentes.

Antes de Iniciar

Configure o espaço Controle SOA. Para obter informações adicionais, consulte "Configurando o Business Space para o Primeiro Uso" na página 83.

Procedimento

1. Crie uma política de mediação com as condições e ações necessárias; por exemplo, uma condição de Contagem de Mensagens > 5 mensagens em 5 minutos e uma ação de rejeição. Para obter informações adicionais sobre como criar uma política de mediação, consulte "Criação de Novas Políticas de Mediação" na página 97.
2. Controle a política de mediação. Para obter informações adicionais sobre como controlar um documento sobre políticas, consulte "Gerenciando o Ciclo de Vida da Política" na página 100.
   a. Clique no documento sobre políticas no Navegador de Registro de Serviço ou procure por ele no widget de procura. As ações são exibidas no Editor de Documento sobre Políticas.
   b. Clique em **Propor Especificação**.
   c. Clique em **Aprovar Especificação**.

   A política é aprovada. É possível redefinir, substituir ou descontinuar a política para gerenciar o ciclo de vida ou editar uma definição existente.
3. Anexe a política. No Business Space, localize o SLD ou SLA ao qual você deseja anexar a política. Há quatro locais em que você poderia fazer isso na amostra:
   - SLD de Armazenamento - anexe sua política aqui se desejar que ela seja aplicada a qualquer uso do serviço Store.
   - SLA Ouro - anexe sua política aqui se desejar que ela seja aplicada apenas a solicitações Ouro do consumidor CEO.
   - SLA Prata - anexe sua política aqui se desejar que ela seja aplicada apenas a solicitações Prata do consumidor CEO.
   - SLA Anônimo - anexe sua política aqui se desejar que ela seja aplicada a quaisquer solicitações provenientes de consumidores que não sejam CEO.

Tarefas relacionadas:

"Criação de Novas Políticas de Mediação" na página 97
É possível criar novas políticas de mediação usando a interface com o usuário do Business Space. Quando você cria políticas de mediação, especifica as condições e as ações para a política.

"Gerenciando o Ciclo de Vida da Política" na página 100
As políticas podem ser transicionadas entre os estados de controle usando a interface com o usuário do Business Space. As políticas devem estar no estado Aprovada para serem impingidas pelo DataPower.

Informações relacionadas:

Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Using the Business Space user interface

O Domínio de Amostra do DataPower

O padrão fornece um domínio de amostra do DataPower, que permite começar a usar o padrão. Como desenvolvedor do DataPower, é possível usar os gateways existentes como um modelo para os seus próprios aplicativos. O ambiente de amostra contém cinco gateways. Há um gateway primário para o serviço Store e quatro gateways de suporte que fornecem back-ends de exemplo para chamada

pelo Gateway de Armazenamento, suporte XACML para um cenário de edição de dados e um front end para fornecer funcionalidade de segurança extra.

Store Web Service Proxy

O Store Web Service Proxy (WSP) é o gateway primário do domínio de aplicativo. Ele recebe uma solicitação com um token LTPA anexado.

Quando solicitado, a regra de processamento da solicitação conclui as ações a seguir:

1. Valida a solicitação, conforme solicitado pela política de Validação. Para obter informações adicionais, consulte "Visão Geral de Artefatos do WSRR na Amostra" na página 60.
2. Direciona a solicitação para o terminal alternativo se o acordo de nível de serviço (ANS) é "Gold".
3. Autentica, conclui a autorização e a contabilidade (AAA) na solicitação. A autenticação inclui as ações a seguir:
   a. Autentica o usuário com um token LTPA.
   b. Mapeia as credenciais com relação ao servidor LDAP, que fornece informações sobre a quais grupos o cliente pertence. Esses grupos incluem Gerente, Funcionário e Cliente.
   c. Transforma as entradas fornecidas em um objeto da solicitação que o Policy Decision Point (PDP) XACML pode entender.
   d. Conclui a autorização usando um PDP XACML na caixa DataPower, com um documento sobre políticas XACML que pode ser criado no IBM Tivoli Security Policy Manager. Os critérios da política são que o usuário deve ser um Gerente, Cliente ou Funcionário. Para a operação findInventory, os retornos requerem Gerente ou Funcionário, e as compras podem ser feitas por clientes.
4. Configura o valor ConsumerID usando um script XSL.
5. Remove o Cabeçalho de Segurança HTTP inteiro da solicitação.
6. Chama o back end do serviço Store.

Quando a solicitação é processada, a regra de processamento de resposta conclui as ações a seguir:

1. Chama o gateway StoreXACMLFW, que age como o PDP no cenário.
2. Com base na resposta, o campo de informações de preço tem os dados editados (zerado) dependendo se o usuário tem a função de Gerente ou não.

Firewalls XML na Amostra

Os firewalls XML a seguir estão definidos na amostra.

Firewall XML StoreAddLTPA

A função do firewall XML StoreAdd LTPA é fornecer um front end com uma porta que os usuários podem chamar usando apenas Autenticação básica (por exemplo, sem LTPA). A regra de processamento da solicitação:

1. Identifica com Autenticação Básica.
2. Autentica com uma consulta LDAP simples.
3. Inclui um token LTPA como parte do pós-processamento.
4. Encaminha a solicitação para a política de segurança StoreWSP com as informações de LTPA agora anexadas.

Firewall XML StoreMockService

O StoreMockService é um serviço de exemplo que usa um Firewall XML como implementação. As operações findInventory, comprar e retornar são todas suportadas. Os valores de respostas são estáticos. Esse serviço de exemplo é criado quando não é possível incluir um WebSphere Application Server no padrão. As três regras de solicitação da política usam uma ação de correspondência para determinar a operação de solicitação e são basedas em uma correspondência, respondem com uma resposta SOAP estática. As respostas SOAP estáticas são fornecidas com base na operação de solicitação em vez de uma implementação de serviço integral.

Firewall XML StoreMockServiceAlternate

O StoreMockServiceAlternate é um serviço de exemplo que usa um Firewall XML como implementação. As operações findInventory, comprar e retornar são todas suportadas. Esse serviço é usado para demonstrar o cumprimento da política de roteamento.

Firewall StoreXACMLFW

Esse cenário executa a edição de dados com base no resultado de um mecanismo de permissão/negação baseado em XACML. No DataPower, não há uma maneira de chamar uma ação AAA individual no fluxo de resposta. Um gateway separado é criado para conter o Policy Decision Point (PDP) XACML. Esse PDP foi encapsulado em uma ação AAA na regra de solicitação do StoreXACMLFW.

StoreXACMLFW é um gateway de firewall XML no DataPower. Essa implementação é usada porque é uma maneira simples de fornecer a funcionalidade. O firewall StoreXML usa a mesma interface WSDL que o servidor Tivoli Runtime Security Services. O gateway StoreWSP cria o objeto de solicitação e o envia, protegido por SSL, para o gateway StoreXMLFW.

A regra de solicitação do firewall StoreXML executa as seguintes tarefas:

1. Executa AAA usando as informações de SSL para autenticação.
2. Executa a autorização usando um PDP XACML na caixa. A política que é usada pelo PDP é criada originalmente no IBM Tivoli Security Policy Manager, mas pode ser recriada usando um editor padrão e o esquema é definido na especificação de XACML.
3. Nenhuma transformação da solicitação é necessária neste processamento de autorização.
4. Se a solicitação XACML for válida, a regra de processamento de solicitação executará uma busca de uma resposta Permit e retornará para o cliente. Caso contrário, ocorrerá uma exceção que é tratada pela regra de processamento de exceções e retorna uma resposta Negar ao cliente.

Nota: O Permitir/Negar/Indeterminado é apenas uma resposta de nível de exemplo. Informações de erro adicionais poderiam ser incluídas em um fluxo específico do cliente.

Política de Segurança XACML

Este tópico descreve como os documentos XACML são criados.

Os documentos XACML que são usados na amostra foram criados pelo editor de políticas do IBM Tivoli Security Policy Manager, mas você pode usar qualquer

texto ou editor XML para criar tais documentos. Para construir ou modificar políticas XACML existentes, consulte as especificações OASIS: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

A política de segurança XACML que é usada na amostra está contida em `storeSWPXACML.xml` e `storePrivateDataXACML.xml`. Essas políticas são usadas para avaliar a solicitação que vai para o Policy Decision Point (PDP). A solicitação é constituída de quatro elementos principais:

1. A seção Assuntos - Contém os detalhes do Nome Distinto do responsável pela chamada da solicitação, bem como os grupos aos quais pertence o responsável pela chamada.
2. A seção de recurso - Contém os documentos aos quais o responsável pela chamada deseja ter acesso. Dois tipos de recursos são usados na amostra. O primeiro tipo é a operação no serviço da web e o segundo tipo é a autorização dos dados na resposta, nesse caso, o recurso priceInfo.
3. A seção Ambiente - Contém informações sobre o ambiente da solicitação.
4. A ação - O que o usuário deseja executar com o material autorizado. No cenário de edição de dados a ação é simplesmente visualizar os dados de priceInfo.

Política de Segurança StoreWSP

A política de segurança no arquivo `storeSWPXACML.xml` mapeia grupos para Operações de Serviço da Web.

A seguir está um exemplo da política de segurança:

```
<PolicySet PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:denyoverrides"
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}findInventory</xa
```

```
cml:AttributeValue>
<ResourceAttributeDesignator AttributeId="urn:ibm:xacml:profiles:web-services:1.0:wsdl:1.1:operation"
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}StoreSOAP</xac
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</xacml:Attr
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>
```

Nota: Na seção de assuntos, ocorre uma correspondência no nome x500 ou na função do assunto do Manager. Se você examinar o arquivo de política inteiro `.xml`, poderá ver que há mapeamentos semelhantes para Cliente e Funcionário. É possível ver que a operação findInventory está autorizada para usar os três grupos enquanto as operações returnProduce e purchase estão limitadas a apenas alguns grupos.

O Gateway de Edição de Dados

Detalhes sobre a folha de estilo storeCallPDP.xsl.

Examine a folha de estilo storeCallPDP.xsl e observe os seguintes pontos:

1. A inclusão da folha de estilo storeSendToPDP.xsl. Essa folha de estilo contém a lógica para a chamada storeXAMLFW.
2. A chamada para o modelo call_PDP dentro de storeSendToPDP.
3. A extração da decisão da resposta para a chamada, por exemplo, “Permit”.
4. A configuração do valor `var:/context/response/displayfilter` para as folhas de estilo allData.xsl ou noPriceInfo.xsl.
5. A estrutura no XACML para a Reação, storePrivateDataXACML.xml, será quase idêntica à estrutura usada no cenário StoreWSP. A diferença é que apenas a função Gerente tem acesso.

storeCallPDP.xsl

```
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:dp="http://www.datapower.com/extension
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-name()='url-open']/*[localname()='response']/*[local-name()='Envelope']/*[local-name()='Body']/
    *[local-name()='Response']/*[local-name()='Result']/*[localname()='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">****** CONFIGURANDO O FILTRO PRIVADO ********</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'" />
      </xsl:otherwise>
    </xsl:choose>
  </xsl:template>
</xsl:stylesheet>
```

Artefatos do WSRR Criados no Padrão SOA Policy Gateway Basic Runtime Sample

Os artefatos do WSRR criados no padrão SOA Policy Gateway Basic Runtime Sample e como a amostra os usa.

Tabela 14. Artefatos do WSRR Criados para o Padrão SOA Policy Gateway Basic Runtime Sample

Objeto	Descrição
Organização	Warehouse de Bob. Essa é a área do negócio que possui o serviço Store
Recurso de Negócios	Warehouse. Isso representa todas as versões do serviço Store e pertence à organização Warehouse do Bob.
Versão de Serviço	Store. Isso representa a versão 1.0 do serviço Store.
WSDL	Store.wsdl
XSD	Company.xsd
Política	• Validate.xml • RouteForGold.xml • LogEveryTime.xml • RejectAfter5MsgIn90Seconds.xml
SLD	SLD do Store. Todas as políticas anexadas aqui se aplicam a qualquer solicitação para este serviço.
SLA Gold	SLA Gold. A existência deste SLA significa que as solicitações gold do CEO do consumidor não serão contadas como anônimas. Todas as políticas anexadas aqui são impingidas nas solicitações gold do CEO do consumidor.
SLA Silver	SLA Silver. A existência deste SLA significa que as solicitações silver do CEO do consumidor não serão contadas como anônimas. Sem políticas anexadas, a solicitação será permitida.
SLA Anônimo	Usuários Anônimos. As políticas anexadas aqui são impingidas em quaisquer solicitações que não tenham um SLA correspondente no local. Nesta amostra, qualquer solicitação de um consumidor diferente de CEO ou qualquer solicitação do CEO que não seja Gold ou Silver, terá políticas de SLA Anônimo impingidas a ele.

Artefatos do DataPower Criados no SOA Policy Gateway Basic Runtime Sample

Os artefatos do DataPower criados no padrão SOA Policy Gateway Basic Runtime Sample.

Tabela 15. Artefatos do DataPower Criados para o Padrão SOA Policy Gateway Basic Runtime Sample

Tipo	Nome	Objetivo
WebService Proxy	StoreWSP	O serviço principal.
Firewalls de XML	StoreAddLTPA StoreMockService StoreAlternateMockService StoreXACMLFW	Autentica e inclui o Token LTPA. O provedor de serviços para clientes não Ouro O provedor de serviços para clientes não Ouro Verifica o acesso a PriceInfo.
WSRR Server	WSRRSVR	A conexão com o WSRR.
Assinatura do WSRR	StoreSub	Fornece informações de procura para o namespace, o objeto, e assim por diante.
Política AAA	StoreAddLTPA	Autenticação básica e identificação para LDAP. Consulta a autenticação. Inclui o token LTPA na solicitação.
Política AAA	StoreWSDLAAA	Identificação e autenticação LTPA. Mapeamento de grupos para a autorização. Autorização XACML.
Política AAA	StoreXACMLFWAZ	Autorização XACML para PriceInfo.
Perfil Proxy SSL	WSRRPP	Perfil proxy SSL para o WSRR Server.
Perfil de Criptografia	WSRRCP	Perfil de criptografia para o WSRR Server.
Credenciais de Validação	WSRRVC	As credenciais de validação contêm o certificado de Criptografia WSRRCERT. Todas as outras configurações são padrão.
Certificado de Criptografia	WSRRCERT	O WSRRCERT usa o certificado de assinante. Esse certificado foi extraído do NodeDefaultKeyStore, certificado padrão para um único servidor ou do certificado padrão CMSKeyStore, no caso de um ambiente ND em que um IBM HTTP Server estava presente.

As Regras de Processamento do Web Service Proxy StoreWSP

O gateway central da amostra é StoreWSP. A Política para o gateway contém uma regra de solicitação e de resposta.

Regra de solicitação

A ação de política primária do StoreWSP_default_request-rule é chamada AAA. Na ação AAA, o Token LTPA é validado, os grupos de usuários são recuperados e uma autorização é executada para ver se o usuário está no grupo LDAP de Gerente, Funcionário ou Cliente. Essa validação é executada quando a etapa AAA

AZ chama o Policy Decision Point (PDP) StoreWSDLPDP, no dispositivo DataPower. Esse PDP usa a política XACML storeWSPXACML.xml.

Regra de resposta

Na regra de resposta, StoreWSP_default_response-rule, a transformação chama o serviço de firewall XML StoreXACMLFW.

Essa transformação determina se o usuário está autorizado a acessar as informações sobre preço com base em se o usuário é um membro do grupo Gerente. Se ele for, a variável *var:///context/response/displayFilter* será configurada para `local:///allData.xsl`. Se ele não for um membro do grupo LDAP Gerente, a variável *var:///context/response/displayFilter* será configurada para `local:///noPriceInfo.xsl`.

A transformação executa, então, as ações da folha de estilo na resposta.

Regras de Processamento StoreXAMLFW

A folha de estilo customizada storeSendToPDP.xsl faz uma chamada para o FW XML StoreXACMLFW local. Há duas regras de processamento usadas nesse firewall. A StoreXACMLFW_request contém uma única ação de política AAA que usa a transformação allData.xsl. Esta ação AAA, StoreXACMLFWAZ, chama por sua vez a ação StorePDP do PDP XACML. Usando a política XACML storePrivateDataXACML.xml, uma determinação será criada se o usuário estiver autorizado para as informações de preço.

As Folhas de Estilo XSL de Amostra

O aplicativo de amostra contém as seguintes folhas de estilo que terminam em `.xsl`, que estão localizadas no diretório local do domínio instalado.

Tabela 16. Folhas de Estilo no Aplicativo de Amostra

Folha de Estilo	Objetivo
`allData.xsl`	Uma folha de estilo de Identidade que copia todos os dados da origem para o destino. Ela é usada para a função Edição de Dados e para a chamada ao Gateway XML XACML.
`apil-xacml-binding-new.xsl`	Usa as informações de mapeamento de credenciais para criar uma solicitação SOAP que pode ser processada pelo Policy Decision Point (PDP) do dispositivo DataPower. Essa folha de estilo é uma modificação da folha de estilo tspm-xacml-binding-sample.xsl que é fornecida no diretório de armazenamento do dispositivo DataPower. Essa funcionalidade chave que é fornecida por esse script adaptado é para incluir uma variável acessível externamente que disponibiliza as informações de assunto da solicitação XACML para a folha de estilo de edição de dados.
`noPriceInfo.xsl`	Esta folha de estilo configure o elemento de preço para um valor de 0.0.

Tabela 16. Folhas de Estilo no Aplicativo de Amostra (continuação)

Folha de Estilo	Objetivo
rgxacml.xsl	Esta folha de estilo é uma customização da folha de estilo tspm-retrieve-groups.xsl no diretório de armazenamento do dispositivo DataPower. O propósito primário desta folha de estilo é fornecer o DN LDAP, nome do host, senha, porta e assim por diante, para que o usuário recebido possa ser consultado e suas informações sobre o grupo recuperadas.
soavars.xsl	Esta folha de estilo é apenas um exemplo que define as informações de LDAP em variáveis usadas pela folha de estilo rgxacml.xsl. No exemplo, a senha é decriptografada, que não é uma prática de produção.
storeCallPDP.xsl	Esta folha de estilo tem o código para chamar o Gateway XACML, manipula a decisão de permissão/negação e configura a variável de filtro para executar allData.xsl ou noPriceInfo.xsl.
storeSendToPDP.xsl	Esta folha de estilo constrói uma solicitação SOAP que é enviada ao Gateway XACML. Ela inclui informações de assunto que são obtidas na folha de estilo apil-xacml-binding-new.xsl, informações sobre o recurso, informações sobre a ação e informações sobre o ambiente.

Objetos do DataPower que Usam as Folhas de Estilo XSL

Os objetos do DataPower usam algumas das folhas de estilo XSL que são fornecidas com o aplicativo de amostra.

Tabela 17. Objetos do DataPower que Usam as Folhas de Estilo XSL

Folha de Estilo	Objetivo
allData.xsl	Usada internamente na folha de estilo storeCallPDP.xsl. A folha de estilo é usada como a transformação customizada na política AAA StoreXACMLFWAZ.
apil-xacml-binding-new.xsl	Usada como a folha de estilo customizada na etapa AZ da política AAA StoreWSDLAAA.
noPriceInfo.xsl	Usada internamente na folha de estilo storeCallPDP.xsl.
soavars.xsl	Usada internamente na folha de estilo rgxacml.xsl.
storeCallPDP.xsl	Chamada como uma transformação na regra Store_default-response.
storeSendToPDP.xsl	Usada internamente na folha de estilo storeCallPDP.xsl.

Capítulo 6. Trabalhando com a Instância Implementada

Após uma das IBM SOA Policy Gateway Patterns estar implementada, será possível visualizar a instância implementada clicando em **Instâncias** > **Sistemas Virtuais** no console de carga de trabalho.

Visualizando os Detalhes da Instância

É possível ver os detalhes de uma instância implementada selecionando-a na lista de instâncias na janela Instâncias do Sistema Virtual. Os detalhes da instância do sistema virtual são exibidos. Os detalhes incluem uma lista de máquinas virtuais que são fornecidos na infraestrutura em nuvem para essa implementação, o endereço IP e o status da máquina virtual.

Para ver o status de fornecimento e de implementação da instância, consulte o valor **Status Atual** na visualização de detalhes.

Para ver o status das máquinas virtuais e dos scripts durante o fornecimento, expanda a seção **Histórico** na visualização de detalhes.

Para ver os detalhes das máquinas virtuais e dos logs de script, expanda a seção **Máquinas Virtuais** na visualização de detalhes. O host e o endereço IP do sistema é o valor **Interface de Rede 0** na seção **Hardware e Rede**. Os logs de scripts estão acessíveis na seção **Pacotes de Scripts**. É possível conectar a quaisquer consoles disponíveis usando os links na seção **Consoles**.

Acessando Instâncias Implementadas

Depois de implementar um padrão de sistema virtual, é possível visualizar a instância de sistema virtual que foi criada para ver seu ambiente do IBM SOA Policy Gateway Pattern e acessar partes do seu componente.

Antes de Iniciar

Para visualizar uma instância de sistema virtual, você deve primeiro implementar um padrão de sistema virtual.

Sobre Esta Tarefa

A implementação de um padrão cria uma instância de sistema virtual ou um ambiente de tempo de execução do IBM SOA Policy Gateway Pattern recém-aprovisionado. Quando a implementação for concluída, a instância de sistema virtual estará em execução.

Procedimento

Para administrar as instâncias de sistema virtual do IBM SOA Policy Gateway Pattern, conclua as etapas a seguir:

1. Clique em **Instâncias** > **Sistemas Virtuais** para acessar a janela Instâncias de Sistema Virtual.
2. Na lista de instâncias da janela Instâncias de Sistema Virtual, selecione a instância que foi implementada.

3. Se a instância estiver em execução, você poderá efetuar login nos componentes do sistema virtual a partir dos links do console na visualização do sistema virtual. Os componentes que estão disponíveis dependem do padrão criado por você. Eles podem incluir:
   - Console Administrativo do WebSphere Application Server
   - UI da Web do WSRR
   - Espaço de Negócios do WSRR
   - DataPower WebGUI

Conectando ao WSRR - Business Space

Use a interface do usuário do Business Space para trabalhar com o WSRR.

Sobre Esta Tarefa

O Business Space é uma das duas interfaces gráficas que podem ser usadas para trabalhar com o WSRR. Uma descrição completa do uso do Business Space com o WSRR está no Centro de Informações do WSRR (consulte o link relacionado).

É possível conectar ao Business Space de uma instância do WSRR em seu padrão implementado clicando em um link no console de carga de trabalho ou inserindo a URL em um navegador da web.

Procedimento

1. Para conectar a partir do console de carga de trabalho:
   a. Clique em **Instâncias** > **Sistemas Virtuais** para acessar a janela Instâncias de Sistema Virtual.
   b. Na lista de instâncias da janela Instâncias do Sistema Virtual, selecione o seu sistema implementado.
   c. Clique em **Máquinas virtuais** na visualização de detalhes do sistema implementado para expandir a lista.
   d. Localize o WSRR na lista de máquinas virtuais e clique no sinal de mais para visualizar detalhes.
   e. Na seção **Consoles**, clique em **WSRR_Business_Space**.
   f. Insira o ID do usuário administrativo e a senha do WSRR.
2. Para conectar a partir de um navegador da web:
   a. Abra um navegador da web.
   b. Localize o nome do host e os números de porta do WSRR. Visualize detalhes de sua implementação, conforme descrito na etapa 1. Expanda a seção **Máquinas virtuais** e selecione a máquina virtual para o Servidor WSRR para ver os detalhes da máquina virtual. Na seção **Hardware e rede**, o nome do host é o valor **Interface de rede 0**.
   c. Insira a URL da UI da Web do WSRR: http://*hostname*:9443/BusinessSpace, em que *hostname* é o nome do host do servidor WSRR.
   d. Insira o ID do usuário administrativo e a senha do WSRR.

Resultados

O Business Space é exibido e pode ser usado para incluir, editar ou remover políticas de mediação e outros artefatos do WSRR.

O que Fazer Depois

Se você estiver usando o Business Space no sistema WSRR pela primeira vez, consulte "Configurando o Business Space para o Primeiro Uso" e siga as etapas para criar o espaço Controle SOA.

Informações relacionadas:

Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0

Configurando o Business Space para o Primeiro Uso

Antes que a interface com o usuário do Business Space possa ser usada para criar políticas, o espaço Controle SOA deve ser criado.

Antes de Iniciar

Para obter informações sobre como acessar o Business Space, consulte "Conectando ao WSRR - Business Space" na página 82.

Sobre Esta Tarefa

Para usar os widgets do Business Space, você deve criar um Espaço. Os espaços são definidos para funções específicas. A criação de política é mais adequada para trabalhar no espaço Controle SOA. Se um espaço Controle SOA ainda não existir, você deverá criá-lo. Para criar um espaço que é baseado no modelo Registro de Serviço para Controle SOA, conclua estas etapas:

Procedimento

1. Clique em **Gerenciar Espaços** na parte superior da página. O diálogo Gerenciador de Espaço é exibido.
2. Clique em **Criar Espaço**. O diálogo Criar Espaço é exibido.
3. Insira um nome no campo **Nome do espaço**; por exemplo, `Controle SOA`. Opcionalmente, insira uma descrição.
4. Selecione **Registro de Serviço para Controle SOA** na lista **Criar um novo espaço usando um modelo** e, em seguida, clique em **Salvar**.
5. O novo espaço é exibido na lista **Gerenciador de Espaço**. Clique no novo espaço para abri-lo.

Resultados

O espaço de Controle SOA é criado. Para abrir o espaço Controle SOA:

1. Clique em **Acessar Espaços** na parte superior da página. O diálogo Acessar Espaços é exibido.
2. Clique no espaço para usuários do Controle SOA. O nome específico dependerá do que foi especificado quando o espaço foi criado.

O que Fazer Depois

É possível incluir mais ações ao widget de Ações do Registro de Serviço:

1. No Business Space, clique em **Editar Página**.
2. No widget de Ações de Registro de Serviço, clique em **Editar Configurações**.
3. Selecione as ações a seguir para serem exibidas:
   - Criar uma Definição de Nível de Serviço

- Criar uma Versão de Serviço
- Criar um Acordo de Nível de Serviço
- Criar um Recurso de Negócios

4. No widget de Ações de Registro de Serviço, clique em **Salvar e Fechar**.
5. Clique em **Concluir Edição**.

Conectando ao WSRR - UI da Web do WSRR

Use a UI da Web do WSRR para trabalhar com o WSRR.

Sobre Esta Tarefa

A UI da Web do WSRR é uma das duas interfaces gráficas que podem ser usadas para trabalhar com o WSRR. Uma descrição completa do uso da UI da Web do WSRR está no Centro de Informações do WSRR (consulte o link relacionado). Na maioria dos casos, talvez você prefira usar a interface do Business Space, mas há algumas tarefas (como a criação de políticas de monitoramento) que devem ser concluídas na UI da Web do WSRR.

É possível conectar à UI da Web do WSRR de uma instância do WSRR em seu padrão implementado clicando em um link no console de carga de trabalho ou inserindo a URL em um navegador da web.

Procedimento

1. Para conectar a partir do console de carga de trabalho:
   a. Clique em **Instâncias** > **Sistemas Virtuais** para acessar a janela Instâncias de Sistema Virtual.
   b. Na lista de instâncias da janela Instâncias do Sistema Virtual, selecione o seu sistema implementado.
   c. Clique em **Máquinas virtuais** na visualização de detalhes do sistema implementado para expandir a lista.
   d. Localize o WSRR na lista de máquinas virtuais e clique no sinal de mais para visualizar detalhes.
   e. Na seção **Consoles**, clique em **WSRR_Web_UI**.
   f. Insira o ID do usuário administrativo e a senha do WSRR.
2. Para conectar a partir de um navegador da web:
   a. Abra um navegador da web.
   b. Localize o nome do host e os números de porta do WSRR. Visualize detalhes de sua implementação, conforme descrito na etapa 1. Expanda a seção **Máquinas virtuais** e selecione a máquina virtual para o Servidor WSRR para ver os detalhes da máquina virtual. Na seção **Hardware e rede**, o nome do host é o valor **Interface de rede 0**.
   c. Insira a URL da UI da Web do WSRR: http://*hostname*:9443/ServiceRegistry, em que *hostname* é o nome do host do servidor WSRR.
   d. Insira o ID do usuário administrativo e a senha do WSRR.

Informações relacionadas:

Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0

Conectando ao Console Administrativo do WebSphere Application Server

Use o console administrativo do WebSphere Application Server para ajustar as configurações de segurança e concluir outras tarefas administrativas.

Sobre Esta Tarefa

Detalhes completos do trabalho com o console administrativo do WebSphere Application Server estão no Centro de Informações. Siga o link relacionado.

É possível conectar ao console administrativo do WebSphere Application Server em seu padrão implementado clicando em um link no console de carga de trabalho ou inserindo a URL em um navegador da web.

Procedimento

1. Para conectar a partir do console de carga de trabalho:
   a. Clique em **Instâncias** > **Sistemas Virtuais** para acessar a janela Instâncias de Sistema Virtual.
   b. Na lista de instâncias da janela Instâncias do Sistema Virtual, selecione o seu sistema implementado.
   c. Clique em **Máquinas virtuais** na visualização de detalhes do sistema implementado para expandir a lista.
   d. Localize o WSRR na lista de máquinas virtuais e clique no sinal de mais para visualizar detalhes.
   e. Na seção **Consoles**, clique em **WebSphere**.
   f. Insira o ID do usuário administrativo e a senha do WSRR.
2. Para conectar a partir de um navegador da web:
   a. Abra um navegador da web.
   b. Localize o nome do host e os números de porta do WSRR. Visualize detalhes de sua implementação, conforme descrito na etapa 1. Expanda a seção **Máquinas virtuais** e selecione a máquina virtual para o Servidor WSRR para ver os detalhes da máquina virtual. Na seção **Hardware e rede**, o nome do host é o valor **Interface de rede 0**.
   c. Insira a URL da UI da Web do WSRR: http://*hostname*:9043/ibm/console, em que *hostname* é o nome do host do servidor WSRR.
   d. Insira o ID do usuário administrativo e a senha do WSRR.

Informações relacionadas:

Centro de Informações do WebSphere Application Server V8.0

Conectando ao Console de um DataPower Virtual

Use o console do DataPower para configurar o Policy Enforcement Point.

Sobre Esta Tarefa

Detalhes completos da configuração do seu gateway estão no Centro de Informações do WebSphere DataPower. Siga o link relacionado.

Você conecta ao console usando um navegador da web. Você recupera detalhes da conexão visualizando detalhes do seu padrão implementado no console de carga de trabalho.

Procedimento

1. Recupere os detalhes necessários usando o console de carga de trabalho:
   a. Clique em **Instâncias** > **Sistemas Virtuais** para acessar a janela Instâncias de Sistema Virtual.
   b. Na lista de instâncias da janela Instâncias do Sistema Virtual, selecione o seu sistema implementado.
   c. Na visualização de detalhes, expanda a seção **Máquinas virtuais** e selecione a máquina virtual do dispositivo DataPower para ver os detalhes da máquina virtual. Na seção **Hardware e rede**, o nome do host é o valor **Interface de rede 0**.
2. Abra um navegador da web e insira a URL `https://hostname:9090/dp`, em que *hostname* é o nome do host do seu dispositivo virtual.

Informações relacionadas:

Centro de Informações do WebSphere DataPower V6.0

Conectando ao Console de Monitoramento

Use o console de monitoramento para visualizar informações de monitoramento.

Sobre Esta Tarefa

Acesse o console de monitoramento a partir da janela Instâncias de Sistema Virtual.

A funcionalidade de monitoramento é fornecida por ITCAM for SOA. Faça download da documentação a partir do link relacionado para obter informações adicionais e procure por informações sobre as instalações do DataPower.

Procedimento

1. Clique em **Instâncias** > **Sistemas Virtuais** para acessar a janela Instâncias de Sistema Virtual.
2. Na lista de instâncias da janela Instâncias de Sistema Virtual, selecione a instância que foi implementada. Os detalhes da instância são exibidos.
3. Expanda a seção **Máquinas Virtuais** e selecione a máquina virtual que deseja monitorar.
4. Em **Informações gerais**, localize **Monitoramento** e clique no link **Clique para abrir**.

Informações relacionadas:

Documentação do ITCAM for SOA 7.2.1 (do Fix Central)

Parando e Iniciando a Instância Implementada

É possível parar e iniciar a instância implementada a partir do console de carga de trabalho. Também é possível parar e iniciar máquinas virtuais individuais no padrão.

Para parar a execução de uma instância implementada:

1. Selecione **Instâncias** > **Sistemas Virtuais** e selecione a instância a partir da lista **Instâncias do Sistema Virtual**.
2. Clique no ícone **Parar** na barra de título da instância.

Para iniciar uma instância implementada interrompida:

1. Selecione **Instâncias** > **Sistemas Virtuais** e selecione a instância a partir da lista **Instâncias do Sistema Virtual**.
2. Clique no ícone **Iniciar** na barra de título da instância.

Nota: Um defeito conhecido no DB2 10.1.0.2 resulta nos processos do DB2 nem sempre reiniciando quando a instância é parada e reiniciada. Nesse caso, você deve iniciar o processo do DB2 manualmente, efetuando login no nó do DB2 como db2inst1 e executando **db2start**. Talvez seja necessário também reiniciar os processos do WSRR nos nós do WSRR.

Para parar máquinas virtuais individuais.

1. Expanda a seção **Máquinas Virtuais** da visualização da instância.
2. Selecione o link **Gerenciar** para a máquina que você deseja parar.
3. Clique no ícone parar na barra de gerenciamento.

Para iniciar máquinas virtuais individuais.

1. Expanda a seção **Máquinas Virtuais** da visualização da instância.
2. Selecione o link **Gerenciar** para a máquina que você deseja parar.
3. Clique no ícone iniciar na barra de gerenciamento.

Também é possível parar e iniciar o WSRR e o DB2 a partir da linha de comandos. Clique no link de **Login** para se conectar usando o console SSH.

Você para e inicia o WSRR parando e iniciando o perfil do WebSphere Application Server. Consulte Gerenciando Perfis Usando Comandos no Centro de Informações do WebSphere Application Server.

No Padrão Avançado, após o DMGR e os Nós Customizados serem reiniciados, o cluster do WSRR precisará iniciar. Para fazer isso, abra o console administrativo do WebSphere Application Server e selecione **Servidores** > **Clusters** > **Clusters do WebSphere Application Server**. Selecione **WSRRCluster_1** e, em seguida, clique em **Iniciar**.

É possível parar e iniciar o DB2 usando comandos do sistema. Consulte Comandos do Sistema no Centro de Informações do DB2.

Configuração de Padrão de Pós-implementação

Depois de implementar os padrões, é necessário configurar a segurança e outras definições.

Configurando o Policy Enforcement Point

O dispositivo ou a instância DataPower é o Policy Enforcement Point (PEP) do IBM SOA Policy Gateway Pattern. Quando o Domínio de Aplicativo está implementado, é possível criar o conteúdo desse domínio.

Procedimento

Ao definir suas configurações, assegure-se de que nomes de domínio diferentes sejam usados em cada dispositivo DataPower; caso contrário, as áreas de trabalho de topologia do ITCAM for SOA não exibirão os dados corretos.
Crie um Web Service Proxy (WSP):

1. No Painel de Controle do DataPower, clique em **Web Service Proxy**.

2. Clique em **Incluir** e insira um nome para o Proxy.
3. Abra a guia **Assinatura do WSRR**. Na lista de Servidores WSRR, clique em **WSRRSVR**.
4. Forneça as outras informações necessárias, como o Manipulador do Lado Frontal, o namespace, o nome do objeto etc., para criar a configuração do Web Service Proxy.

Crie políticas para o WSP:

5. Abra a guia **Política** para o Editor do WSP.
6. Clique em **Regras de Processamento** no nível apropriado. É possível criar uma nova regra ou editar a regra padrão fornecida. A ação de política principal a ser inclusa é a **Ação AAA**. Isso manipula a Identificação, Autenticação e Autorização, que são a chave para o padrão.

   Dentre os itens principais que você deve especificar para a ação AAA estão a Entrada e a Saída, bem como a Política AAA. É possível criar a política durante a criação da Ação de Política AAA ou é possível criá-la antes disso usando o editor AAA.

   - Identificação é a etapa na qual o usuário é Identificado. Na amostra, há duas formas de identificação usadas. No firewal XML StoreAddLTPA, a identificação usou autenticação básica. No firewall StoreWSP, a identificação foi fornecida pelo token LTPA.
   - A autenticação é a etapa em que é comprovado que o usuário é conhecido pelo sistema. Há muitas opções para escolha. Na amostra, há dois exemplos; o primeiro, em que o usuário foi procurado usando LDAP e o segundo, que aceitou um Token LTPA válido.
   - Autorização é a etapa na qual o usuário está autorizado para o recurso, neste caso, as operações de serviço da web. Os seguintes elementos principais devem ser especificados para usar PDP na caixa de XACML:
     - O Método: **Usar Autorização XACML**.
     - A Versão do XACMLn; por exemplo, 2.0.
     - Tipo de PDP; por exemplo, PDP baseado em negação.
     - Usar PDP na caixa: **Ativado**
     - O nome do PDP, que possui o XACML especificado.
     - Configure o PDP. Para obter informações adicionais, consulte “Alterando o PDP XACML no DataPower” na página 71.
     - A folha de estilo XSL customizada para ligar o AAA e o XACML: use `apil-xacml-bindingnew.xsl` como um ponto de início.

Para configurar o gateway para usar a Edição de Dados:

7. Modifique o arquivo `.xml` do XACML para corresponder às políticas de segurança específicas que você deseja impingir para a edição de dados.
8. Crie um Firewall XML com uma ação AAA que segue a amostra de edição de dados.
9. Modifique o PDP usado pela ação AAA acima para apontar para a folha de estilo que você está usando para impingir a edição de dados.
10. Copie e modifique a folha de estilo `storeCallPDP.xsl`, que cria a carga útil SOAP para o serviço XACML. Em particular, certifique-se de que a Ação e o Recurso correspondam a seus requisitos para o documento sobre políticas XACML criado.
11. Certifique-se de que sua folha de estilo modificada chame a porta correta para seu novo Firewall XML do XACML.

Objetos do DataPower Criados nos Padrões de Tempo de Execução Básico e Tempo de Execução Avançado

Uma visão geral dos objetos do DataPower que são criados nos padrões de tempo de execução básico e tempo de execução avançado e suas funções.

Tabela 18. Objetos de Padrão do DataPower

Objeto	Descrição
Domínio	Um Domínio que pode ser usado para o aplicativo de usuários.
WSRR Server	Nomeado WSRRSVR. A URL do SOAP, o nome do usuário e a senha são configurados, bem como um Perfil Proxy SSL com Credenciais de Validação.
Perfil Proxy SSL	Nomeado WSRRPP, é um perfil de encaminhamento (cliente). Ele usa o Perfil de Criptografia WSRRCP. Todos os outros padrões são usados.
Perfil de Criptografia	WSRRCP contém um objeto de credenciais de validação WSRRVC, que contém o Certificado de Assinante que foi transferido por upload como parte dos scripts de padrão.
Credenciais de Validação	As Credenciais de Validação WSRR contêm o Certificado de Criptografia WSRRCERT. Todas as outras configurações são padrão.
Certificado de Criptografia	WSRRCERT usa o certificado de assinante. Esse certificado foi extraído do NodeDefaultKeyStore, Cert. padrão para um único servidor, ou do certificado Padrão CMSKeyStore no caso de um ambiente ND em que um IBM HTTP Server estava presente.

Exemplo de uso da Definição do WSRR Server em um Web Service Proxy:

1. No Painel de Controle do DataPower, clique em **Web Service Proxy**.
2. Clique em **Incluir** e forneça um **Nome** para o Proxy.
3. Em seguida, selecione a guia **Assinatura do WSRR**
4. Selecione WSRR Server no menu. O objeto WSRRSVR está disponível.
5. Forneça as outras informações necessárias, como o Manipulador Frontal, o namespace, o nome do objeto e assim por diante, para criar a configuração do Web Service Proxy.

Certificar Valores de DN para Certificados do DataPower

Quando SSL é usado com as IBM SOA Policy Gateway Patterns fornecidas, a verificação do host de DN é mais estrita do que a segurança padrão do WebSphere Application Server. (Este tópico é aplicável aos dispositivos DataPower externos).

A verificação do host de DN não está ativada no WebSphere Application Server por padrão. No entanto, nos pacotes de scripts que são usados pelos IBM SOA Policy Gateway Patterns, a verificação de host de DN está ativada e não pode ser desativada. Um certificado específico que funciona entre o WebSphere Application Server padrão e o DataPower pode não funcionar para o pacote de scripts “SOA Policy Gateway 2.5.0.0 - Segurança” ou o pacote de scripts “SOA Policy Gateway 2.5.0.0 - Amostra” que é usado com o IBM SOA Policy Gateway Pattern. Por exemplo, um DN de `myserver.yourcompany.com` pode ser aceito por padrões do WebSphere Application Server, mas não pelos pacotes de scripts. Para incluir ou

remover os certificados do DataPower que são usados com a implementação, consulte “Removendo ou Incluindo Certificados do DataPower no Armazenamento Confiável do WSRR”.

Removendo ou Incluindo Certificados do DataPower no Armazenamento Confiável do WSRR

Esta tarefa descreve como incluir ou remover certificados do DataPower. Este tópico é aplicável a padrões implementados com dispositivos DataPower externos.

Sobre Esta Tarefa

Os certificados DataPower são transferidos por upload para o armazenamento confiável do WSRR para simplificar a atualização síncrona entre o WSRR e o DataPower para atualizações de políticas. Se esse recurso não for necessário, será possível remover os Certificados do DataPower. É possível também incluir novos Certificados do DataPower se os certificados precisarem ser alterados.

Procedimento

1. Para remover certificados:
   a. Efetue login no console administrativo do WebSphere Application Server em `https://`*`hostname`*`:9043/ibm/console`, em que *hostname* é o nome do host do sistema WSRR. Insira o nome do usuário administrativo e a senha.
   b. Navegue para **Segurança, certificados SSL e gerenciamento de chaves**.
   c. Clique em **Armazenamentos de Chaves e Certificados**.
   d. Clique em **NodeDefaultTrustStore** se sua implementação for baseada em um padrão de tempo de execução básico ou **CellDefaultTruststore** se você implementou um padrão de tempo de execução avançado.
   e. Clique em **Certificados de Assinante**.
   f. Marque as caixas de seleção em todos os certificados que deseja remover.
   g. Clique em **Excluir**.
   h. Clique em **Salvar**.
2. Para incluir novos Certificados do DataPower, clique em **Incluir** para incluir o novo certificado.
   a. Efetue login no console administrativo do WebSphere Application Server em `https://`*`hostname`*`:9043/ibm/console`, em que *hostname* é o nome do host do sistema WSRR. Insira o nome do usuário administrativo e a senha.
   b. Navegue para **Segurança, certificados SSL e gerenciamento de chaves**.
   c. Clique em **Armazenamentos de Chaves e Certificados**.
   d. Clique em **NodeDefaultTrustStore** se sua implementação for baseada em um padrão de tempo de execução básico ou **CellDefaultTruststore** se você implementou um padrão de tempo de execução avançado.
   e. Clique em **Certificados de Assinante**.
   f. Clique em **Incluir** e especifique os novos certificados.
   g. Clique em **Salvar**.

Alterando as Chaves LTPA

Este procedimento descreve como alterar a chave LTPA. A chave LTPA é compartilhada entre todas as células nos padrões. Ela não é usada no padrão SOA

Policy Gateway Basic Runtime Sample. A Chave LTPA é exportada do Controle Principal e importada nos ambientes de tempo de execução, como temporariedade ou produção.

Sobre Esta Tarefa

Você conclui essas ações no console administrativo do WebSphere Application Server. Para obter informações adicionais, siga o link relacionado.

Procedimento

1. Exporte a nova Chave LTPA do Governance Master WSRR Dmgr.
2. Importe a Chave LTPA para as instâncias do Runtime WSRR, que são Dmgr ou Independente.
3. Se a instância Tempo de Execução for baseada em um padrão de tempo de execução avançado, conclua o seguinte em ordem:
   a. Sincronize todos os nós.
   b. Pare o Cluster do WSRR.
   c. Pare os agentes do nó.
   d. Pare o Dmgr.
4. Se o sistema WSRR for baseado em um padrão de tempo de execução avançado, ele deverá ser reiniciado em ordem reversa:
   a. Inicie o Dmgr.
   b. Inicie os agentes do nó.
   c. Inicie o Cluster do WSRR.
5. Se o WSRR for um Servidor Independente (baseado em um padrão de tempo de execução básico), ele deverá ser interrompido e reiniciado para que a mudança na Chave LTPA entre em vigor.

Informações relacionadas:

Centro de Informações do WebSphere Application Server V8.0

Criação e Controle de Serviço

Use a interface com o usuário do WSRR Business Space para criar e controlar serviços de negócios e seus objetos associados.

O espaço Controle SOA deve ser criado no Business Space para que as políticas possam ser criadas. Se o espaço Controle SOA não existir, consulte “Configurando o Business Space para o Primeiro Uso” na página 83 e siga as etapas para criar o espaço.

Para obter informações adicionais sobre como criar um serviço controlado, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Tutorial: Controlando um Novo Serviço.

Para obter informações adicionais sobre como controlar um serviço existente, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Tutorial: Controlando um Serviço Existente.

Tarefas relacionadas:

“Conectando ao WSRR - Business Space” na página 82
Use a interface do usuário do Business Space para trabalhar com o WSRR.

Políticas

Os detalhes da implementação para usar o WSRR como o Policy Authoring Point e o WebSphere DataPower como o Policy Enforcement Point ao criar políticas de mediação.

Políticas no WSRR

É possível usar o WSRR para criar todas as políticas de SOA, incluindo políticas de SLA (Acordo de Nível de Serviço), políticas de mediação, políticas de monitoramento e políticas customizadas. Usando a interface com o usuário do Business Space, é possível criar, atualizar ou excluir um documento sobre políticas no WSRR. O documento sobre políticas pode conter uma expressão de política que especifica um número de políticas para um determinado domínio de políticas. Como alternativa, é possível criar um documento sobre políticas que monta políticas existentes de outros documentos. As políticas individuais são encaminhadas para uso de identificadores de políticas, que você especifica quando inclui políticas em seu documento. Uma expressão de política representa a declaração de uma política e é equivalente a um elemento `<wsp:Policy>` em um documento WS-Policy.

Para criar uma política de mediação no Business Space, consulte "Criação de Novas Políticas de Mediação" na página 97.

Asserções de Política de Mediação

Os Acordos de Nível de Serviço (SLAs) se originam de uma necessidade de negócios de que a qualidade se serviço que é fornecida por um serviço atende a um padrão especificado. À medida que um serviço é projetado, requisitos funcionais são criados para orientar a lógica do que o serviço faz. Requisitos não funcionais são especificados em paralelo como parte da análise e do design desse serviço para designar a qualidade de serviço que se espera que o serviço forneça. Por exemplo, a empresa pode ter um serviço que fornece informações em resposta a uma consulta de Internet do cliente. O destino é para retornar a resposta em 3 segundos. Como parte da engenharia da transação de ponta a ponta, determina-se que esse serviço deve retornar suas informações em 2 segundos para atender aos requisitos não funcionais dos negócios.

É possível gravar uma política que implementa verificações de tempo de execução no desempenho do serviço e age quando os requisitos são atendidos para garantir que o serviço atenda ao seu SLA. Por exemplo, você pode ter um terminal primário de serviço que é normalmente (95% do tempo) capaz de fornecer resposta de serviço dentro de dois segundos. O arquiteto da SOA cria um terminal secundário em outro servidor que pode ser usado como uma espera a quente para indisponibilidades do terminal primário, mas está autorizado também a ser usado para tráfego de estouro quando o terminal primário não for capaz de acompanhar o carregamento da transação. É possível gravar uma política que verifica o tempo de resposta do serviço e roteia novamente o tráfego quando necessário para atender ao SLA.

Outro exemplo em que os SLAs são mantidos por meio da política de tempo de execução é uma situação em que um serviço está respondendo a transações que possuem vários consumidores, cada um com um nível diferente de prioridade. Um exemplo simples pode ter clientes "gold" e "bronze", em que os negócios garantem apenas uma qualidade de serviço específica para os clientes "gold". Nesse exemplo, é possível verificar se o cliente é "gold" e rotear novamente para o

terminal secundário, deixando o cliente “bronze” lidar com um tempo de resposta mais lento. Os negócios decidiram porque os clientes “bronze” fornecem renda incremental insuficiente para justificar a despesa de engenharia de um tempo de resposta para atender ao SLA dos clientes “gold”.

Em um terceiro exemplo, você pode ter uma situação em que um serviço faz o melhor que pode, mas quando ele determina que está com subcarregamento, enfileira ou até mesmo rejeita mensagens de serviços do consumidor de baixa prioridade. Um exemplo é quando uma rotina em lote inunda o sistema com solicitações do consumidor em um tempo inesperado. Para proteger a qualidade de serviço, é possível criar uma política de tempo de execução que esteja em efeito durante o horário comercial apenas e que rejeita todas as solicitações em lote durante esse período.

Mais genericamente, a política de mediação permite validação e transformação na mensagem recebida do cliente (consumidor) antes da apresentação ao servidor (provedor).

As políticas suportam este tipo de validação e transformação de mensagem. As políticas podem ser especificadas para um serviço de provedor apenas, para um par de consumidor/provedor específico ou para consumidores Anônimos de um serviço de provedor. As políticas para clientes Anônimos fornecem uma maneira de definir uma política padrão que se aplica apenas aos consumidores aos quais nenhum outra política se aplica. Usar esse recurso permite que políticas sejam especificadas para consumidores suspeitos que não se identificam. Tais serviços de consumidor podem, então, ter suas transações rejeitadas. Isso pode ser útil para evitar ataques de negação de serviço de hackers consumidores que tentam inundar o sistema com transações destinadas a derrubar um serviço de provedor.

Condições da Política de Mediação

Podem ser feitas asserções de mediação que permitem que a política de tempo de execução controle o SLA do serviço, a transformação de mensagens de consumidor para provedor ou valide o esquema de mensagem da mensagem do consumidor.

As condições da política SLA, um tipo especial de política de mediação, permitem efetivamente uma construção if-then-else clássica com uma condição e, em seguida, um conjunto de ações a serem executadas dependendo de como a condição é avaliada. A especificação de uma condição é opcional. Se nenhuma condição for especificada, ela será equivalente à condição lógica que avalia como Verdadeiro e nenhuma ação especificada será impingida de acordo.

A condição, se especificada, deve consistir em uma expressão booleana ou uma especificação de planejamento, ou podem ser ambas.

Planejamento

O planejamento, se especificado, identifica quando a política está em vigor. A data e hora são avaliadas pelo Policy Enforcement Point local e o fuso horário que é usado é o do Policy Enforcement Point. Se nenhum planejamento for especificado, a política será iniciada assim que for transferida por download do Policy Authoring Point para o Policy Enforcement Point, e continuará indefinidamente.

O planejamento define uma data de início opcional e uma data de parada opcional, um intervalo de tempo diário opcional e uma lista opcional de dias da semana. Por

exemplo, um planejamento pode ser definido como efetivo a partir de 1º de outubro de 2012 a 30 de outubro de 2012, das 8h às 17h, nas quarta-feiras e domingos.

Os parâmetros para o planejamento que podem ser especificados são os seguintes:

- **StartDate** - Esse atributo opcional especifica no formato xs:date a data na qual o planejamento se torna efetivo. StartDate é inclusivo e, se este atributo não estiver presente, o planejamento se tornará efetivo imediatamente hoje. (Clique no hiperlink xs:time para entender esse padrão de mercado).
- **StopDate** - Esse atributo opcional especifica no formato xs:date a data na qual o planejamento para de ser efetivo. StopDate é exclusivo e a data especificada deve ser após a data de início. Quando a data de parada for anterior ou igual à data de início, o planejamento nunca se tornará efetivo. Se esse atributo não estiver presente, o planejamento será efetivo indefinidamente.
- **Daily** - Este elemento opcional especifica o intervalo de tempo diário durante o qual o planejamento é efetivo. Se esse elemento não estiver presente, o planejamento será efetivo o dia inteiro.
  - **StartTime** – Se Daily estiver especificado, este atributo é obrigatório. Ele especifica, no formato xs:time, o horário no qual o planejamento inicia diariamente. (Clique no hiperlink xs:time para entender esse padrão de mercado).
  - **StopTime** - Se Daily estiver especificado, este atributo é obrigatório. Ele especifica, no formato xs:time, o horário no qual o agendamento para diariamente. StopTime é exclusivo e se o horário especificado for anterior ou igual ao horário de início diário, o planejamento parará no horário de parada especificado no dia seguinte.
- **Weekdays** - Este elemento opcional especifica os dias da semana inclusos no planejamento. Se este elemento não estiver presente, todos os dias da semana serão inclusos no planejamento. Esse elemento afeta apenas o intervalo de tempo diário, uma vez que a execução de planejamentos é permitida após a meia-noite. Por exemplo, se um planejamento estiver configurado para iniciar às 23h e executar por 2 horas às quartas-feiras, o planejamento efetivamente terminará na quinta-feira à 1h.
  - **Days** - Se Weekdays estiver especificado, este atributo é obrigatório. Ele lista os dias da semana inclusos no planejamento como uma lista de nomes separados com o sinal de mais ('+'), por exemplo, “Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday”.

Expressão de Condição da Política de Mediação

A expressão de condição, se especificada, é um elemento de não repetição que especifica uma expressão booleana.

A expressão compreende três parâmetros: Attribute, Operator e Value, mais parâmetros opcionais de Interval e Limit. Se o aplicativo do Operador no Attribute e no Value, além de Interval e Limit quando apropriado, avaliar como Verdadeiro, a expressão avaliará como Verdadeiro. O elemento Limit é usado apenas com os operadores HighLow e TokenBucket. Se não for especificado, o valor de Limit será 0. Se Interval não for especificado, o padrão será 60 segundos.

Os parâmetros para Expression que podem ser especificados são os seguintes:

- **Attribute** - A tabela a seguir resume os atributos definidos e seus tipos.

Tabela 19. Atributos Definidos

Atributo	Descrição e Tipo
ErrorCount	O número de falhas que são observadas durante esse intervalo de monitoramento.
MessageCount	O número de mensagens reais que são interceptadas durante o intervalo de monitoramento.
InternalLatency	A latência interna (tempo de processamento) em segundos.
BackendLatency	A latência de dispositivo-para-servidor em segundos.
TotalLatency	A soma de latência interna e de backend em segundos.

- **Operator** - A tabela a seguir resume os operadores disponíveis e seus significados:

Tabela 20. Operadores

Operador	Significado
GreaterThan	Um algoritmo numérico simples que avalia como Verdadeiro quando o Attribute é maior que o Value definido.
LessThan	Um algoritmo numérico simples que avalia como Verdadeiro quando o Attribute é menor que o Value definido.
TokenBucket	Um algoritmo baseado em taxa que permite bursting. O algoritmo consiste em um depósito com uma capacidade máxima de tokens de Limit. O depósito é preenchido a uma taxa constante de tokens de Value por Interval, enquanto um token é removido para cada unidade de Attribute. Esse algoritmo avalia como Verdadeiro quando não há tokens no depósito e avaliado como Falso caso contrário. Aqui está um exemplo para ajudar a explicar o algoritmo: Suponha Limit=100, Value=5, Interval=1 second e o Attribute=MessageCount. 1. O depósito inicia integral com uma capacidade máxima de 100 tokens 2. Quando uma mensagem chega, o algoritmo verifica se o depósito retém quaisquer tokens: a. Se sim, o algoritmo avalia como Falso e um token é removido do depósito b. Se não, o algoritmo avalia como Verdadeiro. 3. Nesse período, a cada segundo, o algoritmo inclui 5 tokens novamente no depósito conforme o espaço permite.
HighLow	Um algoritmo que avalia como Verdadeiro quando o Attribute atinge o limite alto especificado como o Valor e, em seguida, continua a avaliar como Verdadeiro até que o Attribute atinja o limite baixo especificado como o Limit.

- **Value** – Este é um elemento de número inteiro positivo. “0” é válido.
- **Interval** - Esse elemento opcional define no formato xs:duration o intervalo de tempo, usado como uma janela deslizante, para medir o wsme:Attribute ao avaliar a expressão. Se não especificado, o intervalo usado será de 60 segundos. Se especificado, um valor razoável deverá ser especificado, levando em

consideração os recursos configurados do Policy Enforcement Point. Ou seja, quanto maior esse valor, mais memória será necessária ao Policy Enforcement Point para manter o controle do atributo. (Clique no hiperlink xs:duration para entender esse padrão de mercado).

- **Limit** - Este elemento de número inteiro define o argumento Limit adicional requerido quando wsme:Operator é TokenBucket ou HighLow. A unidade depende do wsme:Operator especificado.

  Quando wsme:Operator for HighLow, ele define o limite baixo enquanto wsme:Value define o limite alto. O limite especificado deve ser inferior àquele de wsme:Value. Quando não especificado, o Limite padrão é 0.

  Quando wsme:Operator for TokenBucket, ele define o tamanho máximo do burst, ou o número máximo de tokens no depósito, enquanto Value especifica a taxa na qual o depósito é novamente preenchido, em número de tokens por Interval. Quando não especificado, o limite padrão é 0 e TokenBucket é, então, equivalente a uma operação GreaterThan.

Ações da Política de Mediação

O elemento Ação de Mediação especifica as ações a serem tomadas. Embora a sintaxe permita várias combinações, nem todas elas fazem sentido e quando ações conflitantes forem especificadas, tais como solicitar que uma mensagem seja enfileirada e rejeitada, o comportamento será rejeitado pelo Policy Authoring Point. As ações da política de mediação permissões são:

- **QueueMessage** – Essa ação especifica que as transações são enfileiradas quando a condição lógica for atendida. O processamento de mensagens não recomeça até que a condição lógica deixe de ser atendida. A metodologia da fila e quaisquer tempos limites associados são conforme definidos pelo Policy Enforcement Point, neste caso, o WebSphere DataPower. Quando várias ações são especificadas dentro de um único elemento Action, QueueMessage deverá ser a primeira ação.
- **RejectMessage** – Essa ação especifica que as transações são rejeitadas quando a condição lógica for atendida. As transações continuam a ser rejeitas até que a condição lógica deixe de ser atendida. Quando as transações são rejeitadas, uma falha de SOAP será retornada ao serviço de cliente (consumidor). Quando várias ações são especificadas dentro de um único elemento Action, RejectMessage deverá ser a primeira ação. QueueMessage e RejectMessage são mutuamente exclusivos.
- **Notify** - Esse elemento opcional especifica que uma notificação é produzida quando a condição lógica for atendida. Para DataPower, uma mensagem é gravada no log do sistema DataPower.
- **RouteMessage** - Esse elemento opcional especifica que as mensagens são roteadas para o destino especificado do terminal quando a condição lógica for atendida. As mensagens continuam a ser roteadas para o terminal especificado até que a condição lógica deixe de ser atendida.
  - **EndPoint** – Este parâmetro será necessário quando uma ação de RouteMessage for especificada. O valor de terminal suportado pode ser um endereço IP, nome do host ou host virtual; como grupo de balanceadores de carga.
- **ValidateMessage** - Esse elemento opcional especifica que as mensagens são validadas com relação às gramáticas especificadas. As mensagens são rejeitadas quando a validação falha. XSD ou WSDL deverão ser especificados como um subparâmetro se ValidateMessage for especificado. SCOPE é opcional e, se não especificado, SOAPBody será usado para a validação.

– **XSD** - Especifica que as mensagens são validadas com relação ao esquema XML identificado pelo URI que ele contém.
– **WSDL** - Especifica que as mensagens são validadas com relação à descrição de serviços da web (WSDL) identificada pelo URI que ela contém.
– **SCOPE** – Especifica qual parte da mensagem é validada. A tabela a seguir lista os valores possíveis e o que eles significam:

Tabela 21. Elementos de ValidateMessage

Valor	Descrição
SOAPBody	O conteúdo do elemento de Corpo SOAP, sem o processamento especial para falhas de SOAP. (Padrão)
SOAPBodyOrDetails	O conteúdo do elemento de detalhe para falhas de SOAP e, caso contrário, o conteúdo do Corpo.
SOAPEnvelope	A mensagem SOAP inteira, incluindo o envelope.
SOAPIgnoreFaults	Sem validação se a mensagem for uma falha de SOAP, caso contrário, o conteúdo do Corpo SOAP.

- **ExecuteXSL** - Especifica que uma conversão XSL é executada com a folha de estilo e os parâmetros especificados. As transações são rejeitadas quando a execução falha. As informações da folha de estilo devem ser especificadas, enquanto os parâmetros são opcionais, e devem ser especificados conforme necessários pela folha de estilo particular especificada.
  – **Stylesheet** - Especifica que a operação de transformação usa a folha de estilo especificada pelo URI contido. A folha de estilo DEVE ser um arquivo XSLT.
  – **Parameter** - Esse elemento de repetição opcional especifica um parâmetro de folha de estilo a ser usado para a operação ExecuteXSL.
    - **Name** – Este atributo é necessário para cada Parameter correspondente e especifica o nome do parâmetro.
    - **Value** - Este atributo é necessário para cada parâmetro Name correspondente e especifica o valor do parâmetro.

Criação de Novas Políticas de Mediação

É possível criar novas políticas de mediação usando a interface com o usuário do Business Space. Quando você cria políticas de mediação, especifica as condições e as ações para a política.

Antes de Iniciar

Para obter informações sobre como acessar o Business Space, consulte “Conectando ao WSRR - Business Space” na página 82.

O espaço Controle SOA deve ser criado para que as políticas possam ser criadas. Se o espaço de Controle SOA não existir, consulte “Configurando o Business Space para o Primeiro Uso” na página 83 e siga as etapas para criar o espaço.

Você deve também configurar o Business Space para criar políticas de mediação do WS-MediationPolicy 1.7 a partir do widget Ações. Consulte o widget Ações do Registro de Serviço

Sobre Esta Tarefa

Crie novas políticas usando o espaço Controle SOA.

Procedimento

1. Abra o espaço Controle SOA:
   a. Clique em **Acessar Espaços**. O diálogo Acessar Espaços é exibido.
   b. Clique no espaço para usuários do Controle SOA. O nome específico dependerá do que foi especificado quando o espaço foi criado.
2. Na guia Visão Geral, clique em **Criar uma Política de Mediação**.
3. Insira um nome significativo e uma descrição opcional.
4. Inclua as condições e ações, conforme necessário. Para obter informações adicionais sobre as condições e ações, consulte "Políticas" na página 92 e Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Criando uma Política de Mediação.
5. Clique em **Concluir**.

Resultados

A política é criada e armazenada no WSRR. Para visualizar o documento sobre políticas para a política criada por você, selecione o documento sobre políticas no widget Navegador do Registro de Serviço. Como alternativa, procure o nome especificado, incluindo `.xml` no final. O documento sobre políticas é exibido no widget Detalhe de Registro de Serviço à direita.

Conceitos relacionados:

"Políticas" na página 92
Os detalhes da implementação para usar o WSRR como o Policy Authoring Point e o WebSphere DataPower como o Policy Enforcement Point ao criar políticas de mediação.

Informações relacionadas:

Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Criando uma Política de Mediação

Criação de Novas Políticas de Monitoramento

É possível criar novas políticas de monitoramento usando a UI da web do WSRR. Quando você cria políticas de monitoramento, especifica as condições e ações para a política.

Antes de Iniciar

Para obter informações sobre como acessar a UI da web do WSRR, consulte "Conectando ao WSRR - UI da Web do WSRR" na página 84.

Procedimento

1. Abra a UI da web do WSRR.
2. Clique em **Visualizar** > **Documentos de Serviços** > **Documentos sobre Políticas** e, na visualização de coleção, clique em **Novo**.
3. Na lista de Estruturas de Políticas, selecione **Monitoramento**. Clique em **Avançar**. Isso cria um documento sobre políticas com uma expressão de política raiz nele.
4. Insira um nome significativo e uma descrição opcional.
5. Clique na guia Política, clique em **Editar documento sobre políticas** e inclua condições e ações, conforme necessário. Para obter informações adicionais sobre as condições e ações, siga os links relacionados.
6. Clique em **Publicar**.

Resultados

A política é criada e armazenada no WSRR. Para visualizar o documento sobre políticas no Business Space, selecione o documento sobre políticas no widget Navegador do Registro de Serviços. Como alternativa, procure o nome especificado, incluindo `.xml` no final. O documento sobre políticas é exibido no widget Detalhe de Registro de Serviço à direita.

Conceitos relacionados:

"Políticas" na página 92
Os detalhes da implementação para usar o WSRR como o Policy Authoring Point e o WebSphere DataPower como o Policy Enforcement Point ao criar políticas de mediação.

Informações relacionadas:

Tarefas de Autoria de Política

Trabalhando com a Ferramenta de Autoria de Política

Gerenciando Políticas

As políticas podem ser editadas ou removidas usando a interface com o usuário do Business Space.

Antes de Iniciar

Configure o espaço Controle SOA. Para obter informações adicionais, consulte "Configurando o Business Space para o Primeiro Uso" na página 83.

Procedimento

1. Para abrir o documento sobre políticas para a política, selecione o documento sobre políticas no Widget de Navegador do Registro de Serviço na parte inferior esquerda da tela. Como alternativa, procure o nome especificado, incluindo `.xml` no final. O documento sobre políticas é exibido no widget Detalhe de Registro de Serviço à direita.
2. Para alterar os detalhes da política:
   a. Clique no ícone Editar nesse widget para editar o documento sobre políticas. Uma janela é exibida com as opções para editar os detalhes da política.
   b. Se a política tiver quaisquer condições ou ações, elas serão exibidas. Crie e modifique as condições e ações, conforme necessário.
   c. Clique em **Concluir** para salvar e fechar o editor de políticas. O widget Detalhe de Registro de Serviço é atualizado para mostrar as mudanças feitas.
3. Para excluir a política:
   a. Faça a transição da política para um estado de controle que permita a edição ou exclusão do documento sobre políticas. Para obter informações adicionais sobre como executar a transição de uma política por meio do Ciclo de Vida de SOA Policy, consulte "Gerenciando o Ciclo de Vida da Política" na página 100.
   b. Clique em **Ação** > **Excluir**. A opção Excluir é listada no menu.
   c. Selecione **Excluir** para excluir a política.
   d. Clique em **Sim** para confirmar a exclusão.

Informações relacionadas:

Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0

Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Policies in the governance enablement profile

Gerenciando o Ciclo de Vida da Política

As políticas podem ser transicionadas entre os estados de controle usando a interface com o usuário do Business Space. As políticas devem estar no estado Aprovada para serem impingidas pelo DataPower.

Sobre Esta Tarefa

Para obter informações adicionais sobre controle, consulte “O Ciclo de Vida de SOA Policy” na página 5.

Procedimento

Para executar a transição de uma política para um estado de ciclo de vida diferente, conclua as etapas a seguir. Repita estas etapas quantas vezes forem necessárias para atingir o estado do ciclo de vida desejado:

1. No Business Space, abra o documento sobre políticas para a política, selecionando o documento sobre política no widget Navegador do Registro de Serviço. Como alternativa, procure o nome especificado, incluindo `.xml` no final. O documento sobre políticas é exibido no widget Detalhes do Registro de Serviço. A propriedade **Estado de Controle** exibe o estado de controle atual para o perfil.
2. Clique em **Ação**. Uma lista de transições de ciclo de vida possíveis é exibida juntamente com outras operações possíveis.
3. Selecione a transição de ciclo de vida necessária para mover a política para o estado requerido. A propriedade **Estado de Controle** da política é atualizada para mostrar o novo estado do ciclo de vida.

Conceitos relacionados:

“O Ciclo de Vida de SOA Policy” na página 5
As políticas são controladas pelo ciclo de vida de SOA Policy. O ciclo de vida faz com que a política seja inicialmente identificada, até ser implementada na produção e, finalmente, ser descontinuada quando não for mais necessária.

Informações relacionadas:

Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - SOA policy lifecycle

Políticas Anexadas a um Serviço

Políticas podem ser anexadas a um serviço usando o WSRR.

Para obter informações adicionais, consulte Centro de Informações do IBM WebSphere Service Registry and Repository Versão 8.0 - Tarefas de Anexo sobre a Política.

Capítulo 7. Resolução de Problemas

Obtenha assistência ao diagnosticar problemas que você possa ter antes, durante e após a implementação do padrão.

Use os links para localizar os tópicos relevantes para um problema com os padrões.

Resolução de Problemas com a Implementação

É possível solucionar problemas comuns que você encontra ao implementar os padrões no IBM SOA Policy Gateway Pattern.

Falha ao Conectar ao Dispositivo DataPower Externo Durante a Implementação

Tente as soluções a seguir:

- Verifique com o Administrador do DataPower se o usuário e a senha são válidos:
  - No DataPower, a GUI da Web valida que o usuário existe acessando o **Painel de Controle** > **Gerenciar Contas do Usuário**.
  - Verifique se a conta existe.
  - Verifique se o usuário é privilegiado para usar a Interface de Gerenciamento XML; por exemplo, o administrador do sistema.
  - O Administrador do DataPower pode precisar verificar se a conta do usuário está ativa nas configurações do agente do usuário; por exemplo, as Configurações de Autenticação Básica.
- Verifique se o nome do host do DataPower está correto
- Verifique se a Interface de Gerenciamento XML do DataPower está ativada.

Resolvendo problemas de um erro para o domínio já existente

Tente a solução a seguir:

- No Painel de Controle do DataPower, abra os Domínios do Aplicativo. Verifique se o Domínio já existe.

Resolvendo problemas de erro de sobreposição de porta para o aplicativo de amostra

Se um dos serviços de amostra estiver indisponível, verifique se as portas em seu domínio estão em conflito com outros domínios.

Tente as soluções a seguir:

- Efetue login no DataPower e alterne para o domínio de amostra. Em seguida, abra o Painel de Controle e clique no ícone Firewall XML. Verifique se os Firewalls XML estão todos no estado Ativo.
- Procure o Manipulador Frontal HTTP. Verifique se o único manipulador Frontal HTTP está no estado Ativo.

Resolução de Problemas de Falha de Promoção

Vários problemas podem surgir durante a promoção, inclusive falha ao conectar ao Controle Principal durante a implementação.

Tente as soluções a seguir:

- Verifique os parâmetros:
  - Verifique o usuário do WSRRCELL do Controle Principal.
  - Verifique a senha do usuário da Célula WSRR do Controle Principal.
  - Verifique o nome do host da Célula WSRR do Controle Principal.
  - Verifique o nome de CÉLULA da Célula WSRR do Controle Principal.
- Verifique a troca do certificado de assinante:
  - Acesse o Armazenamento Confiável Padrão da Célula da célula do Controle Principal e se certifique de que haja uma entrada de certificado para o Dmgr ou o Servidor independente do ambiente de tempo de execução.
  - Acesse cada Ambiente de Tempo de Execução e verifique o armazenamento CellDefaultTrust (para o caso do ambiente ND) ou o NodeDefaultTrustStore (para servidores Independentes do WSRR) para ter certeza de que existe um certificado para o Dmgr do Controle Principal.
  - Exporte as chaves LTPA de ambas as células usando a mesma senha e verifique se elas são iguais (por exemplo, os bytes).
- Certifique-se de que o arquivo de propriedades de promoção contenha seções de servidor com o host e a porta apropriados e as informações do usuário e senha. Essas informações podem ser encontradas no console ServiceRegistry para o Controle Principal:
  - Acesse o GovernanceMasterDMgrHost ou ServiceRegistry e alterne para a perspectiva Configurações. Na seção Ações, localize **Promoção** e abra o arquivo de propriedades de promoção. Para cada ambiente, deve haver elementos XML para cada servidor no nó ou cluster do WSRR de temporariedade. Se existir um cluster ou nó de produção, deverá haver entradas server:port para cada um e, além disso, deverá haver informações do usuário e senha.
- Verifique se a Versão de Serviço e o Terminal SOAP possuem ambos a Classificação para temporariedade e Produção.
  - No Console de Registro de Serviço, selecione a perspectiva Controle SOA. Abra a Versão de Serviço e selecione a guia Classificações. A Temporariedade e a Produção devem estar ativadas.

Resolução de Problemas de Falhas de CLI Customizada

Tente as soluções a seguir:

- Verifique as mensagens de erro no defaultLog no Domínio do DataPower.
- Ative a depuração de CLI e verifique esses logs antes de quaisquer execuções adicionais da CLI.

Resolução de Problemas na Instância Implementada

É possível solucionar problemas comuns na instância implementada.

Conexões com Falha com o Servidor LDAP ou com a Porta StoreWSP do DataPower

Você pode ter um problema com as configurações de Domínio se os logs do DataPower mostrarem um erro de conexão com o LDAP ou o gateway StoreWSP e se você estiver usando o nome do alias do host; por exemplo, `xyz`, em vez do nome completo do host `xyz.company.com` para um dos parâmetros a seguir no pacote de scripts:

- O nome do host do DataPower
- O nome do host do LDAP

Tente a solução a seguir:

1. No Console de Administração do DataPower, alterne para o domínio padrão.
2. Procure `Configurar Definições de DNS`.
3. Clique na guia Procurar Domínios.
4. Certifique-se de que seu domínio, por exemplo, `company.com`, esteja na lista. Se não estiver, clique em `Incluir` e inclua-o na lista.

Problemas com Monitoramento

Se o monitoramento não estiver disponível nos nós implementados, você deverá verificar se os serviços compartilhados necessários estão em execução. Navegue para **Instâncias** > **Serviços Compartilhados**

Verifique se o System Monitoring e o System Monitoring for WebSphere DataPower estão em execução no mesmo grupo de nuvens que o das instâncias implementadas. Para monitoramento do WSRR, verifique também se o System Monitoring for WebSphere Application Server está em execução em seu grupo de nuvens.

Coletando Informações sobre Diagnóstico

É possível usar os logs para ajudar a localizar e resolver problemas. Os logs são armazenados no dispositivo e podem ser visualizados a partir da interface com o usuário ou podem ser transferidos por download para seu sistema de arquivos local.

Procedimento

Para coletar informações de diagnóstico, conclua as etapas a seguir:

1. Visualize as instâncias virtuais:
   a. Clique em **Instâncias** > **Sistema Virtual**.
   b. Selecione a instância na lista de instâncias na janela Instâncias do Sistema Virtual.
2. Para a máquina virtual do WSRR:
   a. Na seção **Máquinas Virtuais**, expanda a máquina virtual do WSRR e verifique se existem erros na seção **Pacotes de Scripts**. Se alguns dos pacotes de scripts contiverem erros, clique nos links de log para **remote_std_out.log** e **remote_std_err.log** ao lado dos nomes de pacotes de scripts.
   b. Efetue login na instância do WSRR e verifique os erros do servidor.

c. Consulte os guias de resolução de problemas do WSRR: http://pic.dhe.ibm.com/infocenter/sr/v8r0/topic/com.ibm.sr.doc/cwsr_troubleshootingandsupport.html

3. Para o DataPower:
   a. Recupere o arquivo **default.log** para o domínio que é criado pelo padrão.
   b. Recupere o arquivo **default.log** para o domínio padrão.
4. Para problemas de monitoramento, colete esses logs do SO Base e dos nós do WSRR (excluindo Nós Customizados do WSRR):
   - `/0config/0config.log`
   - `/opt/IBM/maestro/ITCAMSOADP/lx8266/d4/KD4/logs/*` (x86)
   - `/opt/IBM/maestro/ITCAMSOADP/aix523/d4/KD4/logs/*` (Power)

Capítulo 8. Manutenção e Suporte

É possível executar funções de manutenção, como aplicar correções temporárias.

Incluindo uma Correção Emergencial no Catálogo

As correções temporárias e os fix packs são aplicados a instâncias de sistema virtual como correções emergenciais. É possível incluir correções emergenciais em seu catálogo para serem aplicadas às suas imagens virtuais.

Antes de Iniciar

Você deve ser designado à permissão *Criar novo conteúdo de catálogo* ou à função *Administrador* do Dispositivo IBM Workload Deployer com permissões integrais para executar estas etapas.

Sobre Esta Tarefa

As correções são fornecidas pela IBM ou um provedor de imagem e devem ser transferidas por download. As correções novas são transferidas por download a partir do IBM Fix Central. As correções são então transferidas por upload para o catálogo e podem ser aplicadas a todas as instâncias de sistema virtual aplicáveis.

Procedimento

Conclua as etapas a seguir para incluir uma correção emergencial em seu catálogo.

1. Localize e faça download da correção emergencial (ou correções) a partir do Fix Central.
2. Opcional: É possível incluir diversas correções temporárias de uma vez. Para incluir várias correções de uma vez, faça download dos arquivos compactados a partir do Fix Central e empacote-os em um único arquivo compactado.
3. No menu, selecione **Catálogo** > **Correções de Emergência**.
4. Clique no ícone de inclusão no painel esquerdo.
5. Insira um nome para a correção a ser inclusa. Opcionalmente, também é possível incluir uma descrição da correção que você está incluindo. A correção é mostrada no painel esquerdo da janela Correções Emergenciais e as informações para a correção são mostradas no painel direito.
6. Navegue até o local no qual você armazenou a correção e clique em **Fazer Upload**. Por segurança, apenas os arquivos.zip, .tgz e .pak podem ser transferidos por upload. O Red Hat RPM também é suportado.
7. Preencha as informações sobre a correção. É possível conceder acesso aos usuários e fornecer uma classificação de severidade. Use o campo **Aplicável a** para especificar a imagem virtual ou imagens virtuais às quais essa correção se aplica.

Resultados

A correção emergencial está no catálogo e disponível para ser aplicada às imagens de sistema virtual.

Aplicando uma Correção Emergencial

As correções temporárias e os fix packs são aplicados a instâncias de sistema virtual como correções emergenciais. É possível aplicar correções emergenciais às suas imagens de sistema virtual.

Antes de Iniciar

Você deve ser designado ao acesso Todos para a instância de sistema virtual ou ser designado à função de administração de Dispositivo com permissões integrais para concluir estas etapas. A instância de sistema virtual deve ser iniciada para que o serviço seja planejado ou aplicado. A correção emergencial deve ser inclusa no catálogo para que possa ser aplicada a um sistema virtual.

Sobre Esta Tarefa

Ao incluir uma correção emergencial, você define as imagens virtuais para as quais a correção é aplicável. A lista de correções disponíveis quando você planeja uma solicitação de serviço é construída usando todas as correções aplicáveis à imagem virtual usada para criar sua instância do sistema virtual. Se uma correção já tiver sido aplicada ao sistema virtual, será possível vê-la na listagem **Histórico** e ela não será inclusa na lista de correções disponíveis.

Nota: Você deve encerrar todos os processos do WSRR e WAS antes de instalar uma correção emergencial. Efetue login usando SSH para todos os nós do WSRR e encerre os processos com os comandos **`stopServer.sh`** e **`stopNode.sh`** (Nós Customizados apenas).

Procedimento

Conclua as etapas a seguir para aplicar uma correção temporária.

1. Selecione uma instância de sistema virtual à qual aplicar a correção a partir da janela Instâncias de Sistema Virtual.
2. Clique no ícone **Aplicar Serviço**.
3. Opcional: Planeje uma solicitação de serviço. Por padrão, a correção é aplicada imediatamente. Para planejá-la para ser aplicada posteriormente, clique em **Planejar Serviço** e forneça as informações necessárias.
4. Clique em **Selecionar nível de serviço ou correções**.
5. Clique em **Aplicar Correções Emergenciais** para ver e selecionar a correção a ser aplicada. A correção emergencial é aplicada a todas as máquinas virtuais na instância de sistema virtual. O status da instância de sistema virtual mostra que o serviço foi aplicado no sistema virtual.
6. Verifique os erros. Verifique os arquivos a seguir para assegurar que nenhum erro tenha ocorrido durante o processo de aplicação das correções emergenciais:
   - Remote_std_out.log
   - Remote_std_err.log

   É possível acessar os arquivos de log a partir da janela Instâncias de Sistema Virtual.

Capítulo 9. Appendices

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM ou outros direitos legalmente protegidos, poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não garante ao Cliente direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240.

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

IBM World Trade Asia Corporation
Licensing 2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA" SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a websites que não sejam da IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a estes websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Licenciados deste programa que desejam obter informações sobre este assunto com objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) a utilização mútua das informações trocadas, devem entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nestas informações e todo o material licenciado disponível para ele são fornecidos pela IBM sob os termos do IBM Customer Agreement, Contrato de Licença do Programa Internacional IBM ou qualquer contrato equivalente.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão do desempenho, da compatibilidade ou de qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores.

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações ou cancelamento sem aviso prévio e representam apenas metas e objetivos.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos podem incluir nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com nomes e endereços utilizados por uma empresa real é mera coincidência.

LICENÇA DE COPYRIGHT:

Estas informações contêm programas de aplicativos de amostra na linguagem fonte, ilustrando as técnicas de programação em diversas plataformas operacionais. O Cliente pode copiar, modificar e distribuir estes programas de amostra sem a necessidade de pagar à IBM, com objetivos de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo para a plataforma operacional para a qual os programas de amostra são criados. Esses exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou implicar a confiabilidade, manutenção ou função destes programas.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

Informações sobre a Interface de Programação

As informações sobre interface de programação destinam-se a facilitar a criação de software aplicativo utilizando este programa.

No entanto, estas informações também podem conter informações sobre diagnósticos, modificações e ajustes. As informações sobre diagnósticos, modificações e ajustes são fornecidas para ajudá-lo a depurar seu software aplicativo.

Important: Não utilize estas informações sobre diagnósticos, modificações e ajustes como uma interface de programação, pois elas estão sujeitas a alterações.

Marcas Comerciais

IBM, o logotipo IBM e ibm.com são marcas comerciais ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se estes e outros termos de marca comercial da IBM estiverem marcados em sua primeira ocorrência nestas informações com um símbolo de marca comercial (® ou ™), estes símbolos indicarão marcas comerciais dos Estados Unidos ou de direito consuetudinário de propriedade da IBM no momento em que estas informações forem publicadas. Estas marcas comerciais também podem ser marcas registradas ou de direito consuetudinário em outros países. Uma lista atual de marcas comerciais IBM está disponível na web, na seção Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Enviando seus comentários para a IBM

Se você tiver elogios ou reclamações específicos sobre algo neste manual, utilize um dos métodos listados abaixo para enviar os seus comentários para a IBM.

Sinta-se livre para comentar sobre o que considerar erros ou omissões específicos, e sobre a precisão, a organização, o assunto ou a integralidade desse manual.

Limite os seus comentários às informações contidas neste manual e à forma na qual as informações são apresentadas.

Para fazer comentários sobre as funções de produtos ou sistemas IBM, fale com seu representante IBM ou o revendedor autorizado IBM.

Quando o Cliente envia seus comentários, concede direitos não exclusivos à IBM para usá-los ou distribuí-los da maneira que ela julgar conveniente, sem que isso implique qualquer obrigação para com o Cliente.

É possível enviar comentários para IBM de uma das maneiras a seguir:

- Pelo correio, para este endereço:

  IBM Brasil - Centro de Traduções
  Rodovia Francisco Aguirre Proença (SP 101) Km 09
  Chácaras Assay
  CEP 13186-900
  Hortolândia, SP
- Por fax:
  - De fora do Reino Unido, após seu código de acesso internacional, use 44-1962-816151
  - De dentro do Reino Unido, use 01962-816151
- Eletronicamente, use o ID de rede apropriado:
  - IBM Mail Exchange: GBIBM2Q9 at IBMMAIL
  - IBMLink: HURSLEY(IDRCF)
  - Internet: idrcf@hursley.ibm.com

Qualquer que seja o método usado, assegure-se de incluir:

- O título e o número da ordem da publicação
- O tópico ao qual seus comentários se aplicam
- Seu nome e endereço/número de telefone/número de fax/ID de rede.